NetScaler 10.0

2015-05-18 10:53:30 UTC

Release Notes

Release notes describe the enhancements, changes, bug fixes, and known issues for a particular release or build of the Citrix® NetScaler® 10 software. The release notes are categorized into:

- Main Release
- Maintenance Release
- Enhancement Release

Main Release

These topics describe enhancements in NetScaler® 10 nCore™ and NetScaler® 10 nCore™ VPX™ releases. The nCore NetScaler uses multiple CPU cores for packet handling, which greatly improves the performance of many NetScaler features.

Note: Beginning with this release, NetScaler® Classic™ is no longer available.

You can determine your NetScaler build type by looking at the build information on the banner of the NetScaler Graphical User Interface (GUI), or by issuing the `show version` command at the command line. The file extension indicates the build type. In the GUI, an nCore NetScaler has a `.nc` extension. On the command line, the tar file name for an nCore NetScaler contains `_nc`.

Main Release

These topics describe enhancements in NetScaler® 10 nCore™ and NetScaler® 10 nCore™ VPX™ releases. The nCore NetScaler uses multiple CPU cores for packet handling, which greatly improves the performance of many NetScaler features.

Note: Beginning with this release, NetScaler® Classic™ is no longer available.

You can determine your NetScaler build type by looking at the build information on the banner of the NetScaler Graphical User Interface (GUI), or by issuing the `show version` command at the command line. The file extension indicates the build type. In the GUI, an nCore NetScaler has a `.nc` extension. On the command line, the tar file name for an nCore NetScaler contains `_nc`.

Enhancements

The Citrix NetScaler 10 release provides enhancements for the following NetScaler features.

AAA-TM

The following AAA-TM feature enhancements are available in this release.

127-Character User Name and Password Support

The AAA-TM feature now supports user names and passwords up to 127 characters in length.

127-Character Support for RADIUS NAS ID

The AAA-TM feature now supports RADIUS NAS IDs (`radNASid`) up to 127 characters in length.

SAML 2.0 Consumer Support

The AAA-TM feature now accepts tokens in the Security Assertion Markup Language (SAML), version 2.0. This feature enables you to configure single sign-on (SSO) on your NetScaler appliance for users who log on through a third party authentication server that supports SAML.

To configure this feature, at the NetScaler command line, type the following command:

add authentication samlAction <*name*> [-samlIdPCertName <*string*>] [-samlSigningCertName <*string*>][-samlRedirectUrl <*string*>][-samlUserField<*string*>][-samlRejectUnsignedAssertion (ON | OFF)] [-samlIssuerName <*string*>]

Enhanced NTLMv2 Support

AAA-TM now fully supports NTLMv2 for its single sign-on (SSO) feature. The NetScaler appliance attempts to connect by using NTLMv2 first, and only if that fails does it then attempt to fall back to NTLMv1. This support resolves outstanding issues with accessing Microsoft Share point servers that are part of a private network behind a AAA-TM SSO configuration.

LDAP Referral Support

When AAA-TM receives an LDAP_REFERRAL response to a credential modify request, AAA-TM follows the referral to the indicated domain administration server, authenticates to that server, and performs the password change on that server.

Three caveats apply:

1. AAA-TM assumes that the domain administration server in the referral accepts the same bind credentials as the original server.

2. AAA-TM only follows LDAP referrals for password change operations. In other cases AAA-TM refuses to follow the referral.

3. AAA-TM only follows one level of LDAP referrals. If the second LDAP server also returns a referral, AAA-TM refuses to follow the second referral.

Support for Password Changes on Novell NDS

AAA-TM now fully supports password changes on Novell NDS. When a user responds to a Novell NDS password change prompt, AAA-TM no longer displays an error, but simply changes the password and authenticates the user.

Support for Password Changes on Microsoft RADIUS via MSCHAP

AAA-TM now supports password changes on Microsoft RADIUS by using MSCHAP. When a user authenticates with an expired password, AAA-TM parses the RADIUS authentication rejection message for the MSCHAP vendor identification string and the password-change-required error. If it finds these strings, it initiates the required password change and passes the changed password to the RADIUS server. It then authenticates the user.

Logging out AAA-TM Sessions

You can now configure a traffic management action on the NetScaler appliance to log out a AAA-TM session. At the NetScaler command line, type one of the following commands to add the action or modify an existing action:

add tm trafficAction <name> -initiateLogout (yes|no)
set tm trafficAction <name> -initiateLogout (yes|no)

To put the logout action into effect, associate it with a policy and bind the policy to Global or an appropriate bind point.

AGEE

The following AGEE enhancements are available in this release.

Apply the Citrix Receiver theme to the logon page

You can use the command line to overwrite the original Access Gateway logon page with the Citrix Receiver theme.

Enabling Access Interface Bookmarks

Access Gateway supports the following four services to enable bookmarks to appear in the Access Interface when users log on with Citrix Receiver: Enumeration, Check Protection, Ticketing, and Access.

AppExpert

The following AppExpert feature enhancements are available in this release.

Load Balancing Virtual Server Template Enhancements

In this release, the following enhancements are available for load balancing virtual server templates:

- Deployment files.
- Variables for non-string parameters.

Deployment Files

In NetScaler release 10, when you export a load balancing virtual server, a deployment file is created along with the template file. Both files are created in XML format. The template file contains configuration-specific information (load balancing configuration parameters, information on bound policies, and variable definitions) and the deployment file contains deployment-specific information (services, service groups, and the name-value pairs of variables). You can specify the deployment file when you import the template file to create an entity, or you can manually specify all the deployment information. If you specify the deployment file, the template import wizard prompts you for only the entity name, and uses the deployment information in the deployment file.

You can store the files either on the NetScaler appliance or in any directory/folder on your local drive. If you choose to save the files on the appliance, you can save the template file only to the `/nsconfig/nstemplates/entities/lb vserver/` directory. The deployment file is stored in the /nsconfig/nstemplates/entities/lb vserver/deployment_files directory. The string `_deployment` is automatically appended to the name of the template file to create the name of the deployment file.

Variables for Non-String Parameters

You can now create variables for non-string parameters such as IP addresses and ports. For more information about configuring variables in load balancing virtual server templates, see Configuring Variables in Load Balancing Virtual Server Templates.

SQL OK and SQL Error Response Types Options Added to GUI

You can now use the configuration utility to configure the Responder feature to send an SQL OK or SQL ERROR response. To do this, after enabling the responder feature, you configure a responder action with one of the following action types:

- **Respond with SQL OK**. Sends the designated SQL OK response defined by the Target expression. Use this type of action to send an SQL OK response to an SQL query.
- **Respond with SQL Error**. Sends the designated SQL Error response defined by the Target expression. Use this type of action to send an SQL Error response to an SQL query.

For more information, see Configuring a Responder Action.

Responder HTML Page Imports

The Responder feature can now respond to designated requests by sending the client an HTML-based web page that you upload to the NetScaler appliance. This is a new option. You still have the option of redirecting the request or responding with a response code and answer configured on the NetScaler itself.

To use this feature, first upload an HTML-based web page to the NetScaler by using either the NetScaler command line or the configuration utility. Next, configure a responder action with type set to `RespondWithHTMLPage` and the name of the HTML page. Finally, create a responder policy and bind it to the action.

To upload an HTML page to the Responder feature, at the NetScaler command prompt, type the following commands:

import responder htmlpage [<*src*>] <*name*> [-comment <*comment*>] [-overwrite]

show responder htmlpage f<*name*>]

For more information on configuring a responder action to use an imported HTML page, see Configuring a Responder Action.

Responder Action for Timeouts

You can now invoke a Responder action when an HTTP request times out. To configure this feature, first create the Responder action that you want to invoke. Then, configure the global HTTP timeout action.

To configure the global HTTP timeout action to invoke a Responder action by using the NetScaler command line, type the following command:

set ns httpProfile -reqTimeoutAction <responder action name>

Binding URL Transformation Policies

The URL transformation Global Bindings dialog box has been replaced by the URL Transformation Policy Manager dialog box. This dialog box provides access to the full range of bind points available for application firewall profiles. In addition to Global, you can now bind URL transformation policies to load balancing virtual servers, content switching virtual servers, and policy labels.

For more information, see Globally Binding URL Transformation Policies.

Expressions for Identifying the Protocol in an Incoming IP Packet

The following table lists the expressions that you can use to identify the protocol in an incoming packet.

Expression	Description
CLIENT.IP.PROTOCOL	Identifies the protocol in IPv4 packets sent by clients.
CLIENT.IPV6.PROTOCOL	Identifies the protocol in IPv6 packets sent by clients.
SERVER.IP.PROTOCOL	Identifies the protocol in IPv4 packets sent by servers.
SERVER.IPV6.PROTOCOL	Identifies the protocol in IPv6 packets sent by servers.

Arguments to the PROTOCOL() function

You can pass the Internet Assigned Numbers Authority (IANA) protocol number to the PROTOCOL() function. For example, if you want to determine whether the protocol in an incoming packet is TCP, you can use CLIENT.IP.PROTOCOL.EQ(6), where 6 is the IANA-assigned protocol number for TCP. For some protocols, you can pass an enumeration value instead of the protocol number. For example, instead of CLIENT.IP.PROTOCOL.EQ(6), you can use CLIENT.IP.PROTOCOL.EQ(TCP). The following table lists the protocols for which you can use enumeration values, and the corresponding enumeration values for use with the PROTOCOL() function.

Protocol	Enumeration value
Transmission Control Protocol (TCP)	TCP
User Datagram Protocol (UDP)	UDP
Internet Control Message Protocol (ICMP)	ICMP
IP Authentication Header (AH), for providing authentication services in IPv4 and IPv6	AH
Encapsulating Security Payload (ESP) protocol	ESP
General Routing Encapsulation (GRE)	GRE
IP-within-IP Encapsulation Protocol	IPIP
Internet Control Message Protocol for IPv6 (ICMPv6)	ICMPv6
Fragment Header for IPv6	FRAGMENT

Use Case Scenarios

The protocol expressions can be used in both request-based and response-based policies. You can use the expressions in various NetScaler features, such as load balancing, WAN optimization, content switching, rewrite, and listen policies. You can use the expressions with functions such as EQ() and NE(), to identify the protocol in a policy and perform an action.

Following are some use cases for the expressions:

- In Branch Repeater load balancing configurations, you can use the expressions in a listen policy for the wildcard virtual server. For example, you can configure the wildcard virtual server with the listen policy `CLIENT.IP.PROTOCOL.EQ(TCP)` so that the virtual server processes only TCP traffic and simply bridges all non-TCP traffic. Even though you can use an Access Control List instead of the listen policy, the listen policy provides better control over what traffic is processed.
- For content switching virtual servers of type `ANY`, you can configure content switching policies that switch requests on the basis of the protocol in incoming packets. For example, you can configure content switching policies to direct all TCP traffic to one load balancing virtual server and all non-TCP traffic to another load balancing virtual server.
- You can use the client-based expressions to configure persistence based on the protocol. For example, you can use `CLIENT.IP.PROTOCOL` to configure persistence on the basis of the protocols in incoming IPv4 packets.

HTML5 Parsing and Expression Support

The NetScaler expressions language contains new XPath expressions that parse HTML web pages and allow you to extract specific content from the HTML headers and body.

For more information, see XPath and HTML, XML, or JSON Expressions.

Packet Expression Support

The NetScaler default expressions language now contains expressions that perform any task that could be performed by using the NetScaler classic expressions language. In particular, the following new expressions have been added:

- **PACKET.SRCPORT**. Returns the TCP/UDP source port, as a `num_at` number.
- **PACKET.DSTPORT**. Returns the TCP/UDP destination port, as a `num_at` number.
- **PACKET.PORT**. Returns the packet port. Supports only `EQ` and `NE`.
- **PACKET.SRCIP**. Returns the IPv4 source IP.
- **PACKET.DSTIP**. Returns the IPv4 destination IP.
- **PACKET.IP**. Returns the packet IP. Supports only `EQ` and `NE`.
- **PACKET.VLANID**. Returns the Vlan ID, as a `num_at` number.
- **PACKET.INTF**. Returns the packet interface ID, as a `text_t` string.
- **PACKET.PPEID**. Returns the packet core ID, as a `num_at` number.
- **PACKET.CONNID**. Returns the packet connection ID, as a `num_at` number.
- **PACKET.SVCNAME**. Returns the packet service name, as a `text_t` string.

- **PACKET.SRCIPv6**. Returns the IPv6 source IP.
- **PACKET.DSTIPv6**. Returns the IPv6 destination IP.
- **PACKET.IPv6** Returns the packet IPv6 IP. Supports only `EQ` and `NE`.

SIP Expression Support

The NetScaler expressions language now contains a number of new expressions for Session Initiation Protocol (SIP) connections. These expressions are intended for use in policies for any supported protocol that operates on a request/response basis, such as application firewall, content switching, rate limiting, and responder policies. The header format used by the SIP protocol is similar to that used by the HTTP protocol, so many of the new expressions look and function much like their HTTP analogs. The NetScaler operating system currently supports only SIP over UDP, so the new expressions conform to that.

For more information, see SIP Expressions.

String Comparison Functions

You can now use the functions `NE()`, `GT()`, `GE()`, `LT()`, and `LE()` to compare a string to the string returned by an expression prefix. If the prefix returns a non-string value, the function argument is compared to the string representation of the value returned by the prefix. You can use the functions with `SET_TEXT_MODE(IGNORECASE)` or `SET_TEXT_MODE(NOIGNORECASE)`, and with both ASCII and UTF-8 character sets.

MOD() Function for Data of Type Integer and Unsigned Long

You can use the `MOD()` function with data of type integer and unsigned long. The function divides the value returned by the preceding function by its argument and returns the remainder. The argument must be a non-zero value.

APPEND() String Function

You can use the `APPEND()` function to append the string representation of the argument to the string representation of the value returned by the preceding function. The preceding function can be one that returns a number, unsigned long, double, time value, IPv4 address, or IPv6 address. The argument can be a text string, number, unsigned long, double, time value, IPv4 address, or IPv6 address. The resulting string value is the same string value that is obtained by using the `+` operator.

NE() Function for Time Values

You can now use the `NE()` function for time values. The argument to the `NE()` function is compared with the value returned by the preceding function.

Command-Line Interface Support for Importing and Exporting AppExpert Applications

You can use the NetScaler command line interface (CLI) to export and import application configuration information to and from an AppExpert application template file. The template files are exported to and imported from the `/nsconfig/nstemplates/applications/` directory on the appliance. Deployment files are exported to and imported from the `/nsconfig/nstemplates/applications/deployment_files` directory. You cannot change the source and target directories.

When you use the command-line interface to import a template, you can configure deployment information only by specifying a deployment file in the import application command. If you do not specify a deployment file when importing a template, after you import a template, you must use the configuration utility to provide the deployment information.

To import an AppExpert application by using the NetScaler command line

At the NetScaler command line, type the following command to import an AppExpert application to the NetScaler appliance:

import application <apptemplateFilename> [-appname <string>] [-deploymentFilename <input_filename>]

To export an AppExpert application by using the NetScaler command line

At the NetScaler command line, type the following command to export an AppExpert application to the NetScaler appliance:

export application <appname> [-apptemplateFilename <input_filename>] [-deploymentFilename <input_filename>]

Application Firewall

The following Application Firewall feature enhancements are available in this release.

Variable Support for Application Firewall Configuration

Instead of using static values, to configure the application firewall's security checks and settings, you can now use standard NetScaler named variables. By creating variables, you can more easily export and then import configurations to new NetScaler appliances, or update existing NetScaler appliances from a single set of configuration files. This simplifies updates when you use a testbed setup to develop a complex application firewall configuration that is tuned for your local network and servers and then transfer that configuration to your production NetScaler appliances.

For more information, see Configuration Variable Support.

Support for CEF Format Logs

The application firewall can be configured to maintain logs in either the proprietary NetScaler log format or the Common Event Format (CEF), an open standard used by other security appliances and network devices. The use of CEF makes it possible to analyze application firewall logs along with logs produced by other security appliances and network devices.

CEF logs consist of three sections: the syslog prefix, the CEF header, and the CEF extension. An application firewall log in CEF format contains the following information:

Mon Day hh:mm:sss <hostname> CEF:<version>|<device vendor>|<device product>|<device version>|<module>|<event-type>|<severity>|<CEF extension>

Source Port and HTTP Method Added to Logs

The application firewall logs now contain the source port and the HTTP method used for the connection that generated the logged event.

For more information, see Logs, Statistics, and Reports.

Importing and Exporting Application Firewall Profiles

You can now import and export application firewall profiles from a local file. This allows you to configure the application firewall on one NetScaler appliance, and then duplicate that configuration on other NetScaler appliances. This permits use of a testbed setup to develop your application firewall configuration. You can then transfer the configuration to your production NetScaler appliances.

Resetting Learning Thresholds

You can now reset the learning thresholds to zero (0) for any profile, to force the application firewall to restart the learning process. This is helpful when you import a profile to a new NetScaler appliance or standalone Application Firewall appliance that is intended to protect different web sites.

To remove all learned data, in the Configure Application Firewall Profile dialog box, Learning tab, click Remove All Learned Data.

For more information, see Manual Configuration By Using the Configuration Utility.

Binding Application Firewall Policies

The application firewall Global Bindings dialog box has been replaced by the Application Firewall Policy Manager dialog box. This dialog box provides access to the full range of bind points available for application firewall profiles. In addition to Global, you can now bind application firewall policies to load balancing virtual servers, content switching virtual servers, and policy labels.

For more information, see Manual Configuration By Using the Configuration Utility.

Response-Side Signatures Check

The application firewall now supports signatures for response-side patterns as well as request-side patterns. This functionality allows the following types of checks:

- **Credit cards.** You can specify specific types of credit card numbers for signature checking, just as you currently do for the Credit Card security check.
- **Safe objects.** You can specify a pattern matching any type of sensitive private information that you want to prevent from being included in responses, such as social security numbers, or driver's license numbers.

For more information, see Signatures.

Sessionless URL Closure

The application firewall sessionless URL Closure feature supports a new type of URL closure. From the client's point of view, this type of URL closure functions in exactly the same way as standard, session-aware URL Closure. However, instead of using a cookie to track the user's session, it embeds the necessary information as a token in the response URL.

For more information, see Start URL Check.

CSRF Learning

Application firewall learning is now supported for the CSRF Form Tagging security check. If you enable learning for CSRF form tagging, the application firewall generates a list of URLs that violate this security check for your review.

Learning for the CSRF Form Tagging feature is enabled in exactly the same way as learning for the other features. You can enable learning by checking the Learn check box on either the Security Checks tab of the main Configure Application Firewall Profile dialog box or the General tab of the Modify Cross-Site Request Forgery dialog box. You can configure the Learning thresholds on the Learning tab of the Configure Application Firewall Profile dialog box, by selecting CSRF form tagging and then typing the appropriate values in the Learning Thresholds area.

For more information on application firewall learning, see Manual Configuration By Using the Configuration Utility. For more information on the CSRF Form Tagging check, see CSRF Form Tagging Check.

The Web Interface AppExpert Template

The Citrix Web Interface AppExpert template provides an alternative method to configure the application firewall feature on a new NetScaler appliance. It provides a simple configuration that is suitable for protecting most web site content. You can modify that configuration later to provide additional protection for more complex features.

For an overview of the application firewall-specific features of the Web Interface AppExpert template, see Configuring the Application Firewall. For information on installing and using an AppExpert template, see the AppExpert Applications and Templates.

Qualys Support

The QualysGuard(r) vulnerability scanner has been added to the list of vulnerability scanners whose scan results can be imported into the Application Firewall and then used to create signature rules. This allows users to use the QualysGuard scanner to detect exploitable vulnerabilities on their web sites and then feed the results into the application firewall to create signature rules tailored to protect their web sites.

For more information about application firewall support for external vulernability scanners and instructions on how to use this feature, see Updating a Signatures Object from a Supported Vulnerability Scanning Tool.

Application Firewall Support for Chunked POST Requests

The application firewall now supports HTTP 1.1 chunked POST requests. When the NetScaler appliance receives a chunked POST request, it calculates and adds an appropriate Content-Length header, removes the Transfer-Encoding header, and then performs the appropriate checks. The workarounds that were used in previous releases are no longer necessary.

Cache Redirection

The following Cache Redirection enhancement is available in this release.

Support for Fully Transparent Cache Redirection

The NetScaler appliance now supports transparent cache redirection with the Use Source IP (USIP) option enabled and Use Proxy Port option disabled. The NetScaler appliance preserves the client's IP address and port when forwarding a request to the cache server or origin server.

Cloud Bridge

The following Cloud Bridge enhancements are available in this release.

Cloud Bridge Set Up for SoftLayer Enterprise Cloud

The configuration utility now includes a wizard that helps you to easily configure a cloud bridge between a NetScaler appliance or a virtual appliance (VPX), on any network, and NetScaler VPX instances on the SOFTLAYER enterprise cloud.

For more information, see CloudBridge.

IKEv2 Liveliness Check for IPSEC Tunnels

For an IPSEC tunnel, the NetScaler appliance now performs the standard IKEv2 liveliness check on the peer at a regular interval, which is user configurable. As determined by the check, the NetScaler appliance displays the status of the tunnel as UP or DOWN.

Statistical Counters for IPSEC Tunnels

The following statistical counters have been introduced for IPSEC tunnels:

Bytes Received.

Total number of bytes received by the NetScaler appliance through all the configured IPSEC tunnels since the appliance was last started. Does not include bytes received during the following phases:

- Internet Key Exchange (IKE) authentication (pre-shared key or digital certificates) phase on any configured IPSEC tunnel.
- IKE Security Association (SA) establishment phase on any configured IPSEC tunnel.

Bytes Sent.

Total number of bytes sent by the NetScaler appliance through all the configured IPSEC tunnels since the appliance was last started. Does not include bytes sent during the following phases:

- Internet Key Exchange (IKE) authentication (pre-shared key or digital certificates) phase on any configured IPSEC tunnel.
- IKE Security Association (SA) establishment phase on any configured IPSEC tunnel.

Packets Received.

Total number of packets received by the NetScaler appliance through all the configured IPSEC tunnels since the appliance was last started. Does not include packets received during the following phases:

- Internet Key Exchange (IKE) authentication (pre-shared key or digital certificates) phase on any configured IPSEC tunnel.
- IKE Security Association (SA) establishment phase on any configured IPSEC tunnel.

Packets Sent.

Total number of packets sent by the NetScaler appliance through all the configured IPSEC tunnels since the appliance was last started. Does not include packets sent during the following phases:

- Internet Key Exchange (IKE) authentication (pre-shared key or digital certificates) phase on any configured IPSEC tunnel.
- IKE Security Association (SA) establishment phase on any configured IPSEC tunnel.

Clustering of NetScaler Appliances

You can now create a cluster of nCore NetScaler appliances and make them work together as a single system image. The traffic is distributed among the cluster nodes to provide high availability, high throughput, and scalability. A NetScaler cluster can include as few as 2 or as many as 32 NetScaler nCore hardware or virtual appliances.

Each NetScaler appliance that you intend to add to the cluster must satisfy the following criteria:

- Must be of the same platform type (physical appliance or VPX instance).
- Must be of the same hardware type (for physical appliances).
- Must have the same licenses (Standard, Enterprise, Platinum, or any add-on license).
- Must be on the same subnet.
- Must be of the same software version.

For more information, see Clustering.

Compression

The following compression enhancement is available in this release.

Renaming and Getting Compression Statistics

You can perform the rename and get statistics operations on the compression policy and the compression policy label by using the following commands:

- `rename cmp policy <name> <newName>`
- `rename cmp policylabel <labelName> <newLabelName>`
- `stat cmp policy <name>`
- `stat cmp policylabel <labelName>`

Configuration Utility

The following configuration utility enhancements are available in this release.

HTML Dashboard

The monitoring page is enhanced and renamed to “Dashboard.” The new Dashboard is HTML-based and replaces the Java-based Dashboard. The Dashboard displays critical performance statistics and provides real-time data. The data displayed is for approximately the last 5 minutes of operation and is updated every 7 seconds. This data is displayed in the form of graphs—linear and tabular.

Windows Gadget to Monitor NetScaler

A Windows gadget is available to monitor multiple NetScaler appliances from your desktop. The gadget is supported on Windows 7 and Windows XP operating systems. You can download the gadget from the Downloads page in the NetScaler configuration utility. The gadget displays the aggregate interface throughput, CPU usage, memory usage, rate of HTTP requests, and events (for example, a virtual server going down).

Pagination Support in Dashboard

Pagination is introduced for all entities, such as virtual servers and services, displayed in the Dashboard. The default is 25 entries per page.

SCOM Management Pack

You can now download the SCOM Management pack from the Downloads page in the NetScaler configuration utility.

The pack contains the Citrix NetScaler Operation Manager and The Citrix NetScaler Performance and Resource Optimization (PRO) Management Pack (MP).

The Citrix NetScaler Operation Manager pack provides monitors and rules for monitoring the NetScaler appliances deployed in your network. The Citrix NetScaler Performance and Resource Optimization (PRO) Management Pack (MP) provides monitors and rules for monitoring the health of the virtual servers configured on the managed NetScaler appliances. The MP uses the PRO feature of SCVMM to initiate corrective actions if the virtual servers become unhealthy.

Content Switching

The following content switching enhancements are available in this release.

Priority Based Sorting of Bound Policies

When you run the show cs vserver command, you can now view the associated content switching policies in the order of the priority of the policies instead of by the chronological order in which they are bound.

This enhancement can help you know the order in which the content switching polices are applied and, therefore, understand how client requests are routed. The configuration utility also shows the content switching policies in the order of their priority.

For more information, see Viewing the Properties of Content Switching Virtual Servers.

Identifying Connections with the 4-tuple and Layer 2 Parameters

You can now set the L2Conn option for a content switching virtual server. With the L2Conn option set, connections to the content switching virtual server are identified by the combination of the 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>) and Layer 2 connection parameters. The Layer 2 connection parameters are the MAC address, VLAN ID, and channel ID. For more information, see Identifying Connections with the 4-tuple and Layer 2 Connection Parameters.

Enhanced Set of Counters for Virtual Servers

The following table lists the statistical counters that are now available for a content switching virtual server on the dashboard, on the Statistics page, and in the output of the stat cs vserver CLI command:

Table 1. New Counters Available for a Content Switching Virtual Server

Counter name	Description
Vserver hits	The total number of hits for the virtual server.
Total Packets rcvd	The total number of client-side packets received by the content switching virtual server.
Total Packets sent	The total number of packets sent by the content switching virtual server to clients.
Current client connections	The total number of client-side connections.
Current Client Est connections	The total number of connections that are in ESTABLISHED state.
Current server connections	The total number of server-side connections.

DataStream Enhancements

The following DataStream enhancements are available in this release.

Configuring Token Method of Load Balancing

You can configure the token method of load balancing for DataStream to base the selection of database servers on the value of the token extracted from the client (application or Web servers) requests. These tokens are defined by using SQL expressions. For subsequent requests with the same token, the NetScaler sends the requests to the same database server that handled the initial request. Requests with the same token are sent to the same database server until the maximum connection limit is reached or till the session entry has aged out. For more information, see Configuring the Token Method of Load Balancing for DataStream.

Responder Policy Support

You can now configure responder policies for DataStream. You can configure responder policies by using default syntax expressions that are provided for evaluating MYSQL/MSSQL client and query properties. You can then bind the policies to global bind points provided specifically for DataStream. You can also bind the policies to policy labels of type MYSQL or MSSQL.

Before creating a responder policy for DataStream, you create a responder action. In the policy, you define the rule by using one or more default syntax expressions for MYSQL or MSSQL, and you assign the action to the policy. Then, you bind the policy globally or to a

policy label. To apply the policies that you have bound to a policy label, you must call the policy label from another policy. For more information, see Responder.

Audit Log Message Support

You can now configure the NetScaler appliance to generate audit log messages for the DataStream feature. Audit log messages are generated when client-side and server-side connections are established, closed, or dropped. The categories of messages that you can log and view are ERROR and INFO. For more information, see Audit Log Message Support.

Configuring Content Switching Based on RPC for MS SQL Databases

You can use the following expressions to configure content switching based on remote procedure call (RPC) names or IDs:

MSSQL.REQ.RPC.NAME.

Returns the name of the procedure that is being called in a remote procedure call (RPC) request. The name is returned as a string.

MSSQL.REQ.RPC.IS_PROCID.

Returns a Boolean value that indicates whether the remote procedure call (RPC) request contains a process ID or an RPC name. A return value of TRUE indicates that the request contains a process ID and a return value of FALSE indicates that the request contains an RPC name.

MSSQL.REQ.RPC.PROCID.

Returns the process ID of the remote procedure call (RPC) request as an integer.

AppFlow Support

Appflow records can now export database information (such as database protocol, database request type, and database request string) to the AppFlow collectors. Following is an example of configuring the AppFlow action and policies for MS SQL:

```
> enable feature appflow
> add db user sa password freebsd
> add lb vserver lb0 MSSQL 10.102.147.97 1433 -appflowLog ENABLED
> add service sv0 10.103.24.132 MSSQL 1433 -appflowLog ENABLED
> bind lb vserver lb0 sv0
> add appflow collector col0 -IPAddress 10.102.147.90
> add appflow action act0 -collectors col0
> add appflow policy pol0 "mssql.req.query.text.contains(\"select\")" act0
> bind lb vserver lb0 -policyName pol0 -priority 10
```

When the NetScaler appliance receives a database request, the appliance evaluates the request against the configured policies. If a match is found, the details are sent to the AppFlow collector configured in the policy.

Microsoft SQL Server Version Setting

You can specify the version of Microsoft® SQL Server® for a load balancing or content switching virtual server that is of type MSSQL. The version setting is recommended if you expect some clients not to run the same version as your Microsoft SQL Server product. The version setting provides compatibility between the client-side and server-side connections by ensuring that all communication conforms to the server's version. For more information about configuring the server version setting for a load balancing virtual server, see Configuring the Microsoft SQL Server Version Setting. For more information about configuring the server version setting for a content switching virtual server, see Configuring the Microsoft SQL Server Version Setting.

SNMP Support for DataStream Rate Limiting

A new SNMP alarm, DATASTREAM-RATE-LIMIT-HIT, can generate a trap when the DataStream request rate exceeds the limit defined for the NetScaler appliance.

If you configure this SNMP alarm, the NetScaler appliance checks the DataStream request rate every second. When the DataStream request rate exceeds the limit defined, the NetScaler generates the following SNMP trap message:

- DataStreamRateLimitHit

Domain Name System

The following Domain Name System enhancements are available in this release.

Text (TXT) Record Support

Domain hosts store TXT records for informative purposes. A TXT record's RDATA component, which consists of one or more character strings of variable length, can store practically any information that a recipient might need to know about the domain, including information about the service provider, contact person, email addresses, and associated details. Sender Policy Framework (SPF) protection has been the most prominent use case for the TXT record. For more information, see Creating TXT Records for Holding Descriptive Text.

Rewriting NXDOMAIN Responses

You can evaluate a DNS response against certain predefined criteria, and then rewrite the A records and AAAA records in the response before forwarding it to the client. For rewrite to occur, queries must be of type A or AAAA. Other types of queries cannot be rewritten. They raise an `UNDEF` condition if they meet your defined criteria.

To rewrite the A or AAAA records in a DNS response that matches your criteria, do the following:

- Configure a DNS action with the `Rewrite_Response` action type. Provide the IPv4 and/or IPv6 addresses that you want to be sent to the client. If necessary, configure the time to live value for the rewritten records.
- Configure a DNS policy with criteria that must be met by a DNS response before it can be rewritten. Define the criteria in the policy rule. For example, to determine whether

the status of a DNS response is set to NXDOMAIN, use the DNS.RES.HEADER.RCODE.EQ(NXDOMAIN) expression. In this expression, the RCODE function returns the response code in the DNS response.

- Bind the policy to the global request bind point.

Note: If the appliance finds in its DNS cache an NXDOMAIN record for the domain in a query, the appliance does not send the query to the name server. The appliance sends the client the cached NXDOMAIN record. Consequently, the DNS policy that you configure for evaluating responses for the NXDOMAIN response code is not evaluated. To prevent NXDOMAIN records from being served from the appliance's DNS cache, after you bind the DNS policy to a bind point, flush the DNS cache by using the flush dns proxyRecords command.

Following is a sample configuration for rewriting DNS responses whose response code is NXDOMAIN. Policy mydnspolicy determines whether a DNS response is an NXDOMAIN response. Action mydnsaction rewrites the response to include the IP addresses that you want to send to the client. The policy is bound globally.

```
> add dns action mydnsaction Rewrite_Response -IPAddress 192.0.2.77 2001:DB8:: -TTL 36000
Done
> add dns policy mydnspolicy 'DNS.RES.HEADER.RCODE.EQ(NXDOMAIN)' mydnsaction
Done
> bind dns global mydnspolicy 10
Done
>
```

For more information about configuring a DNS action, configuring a DNS policy, and binding a DNS policy, see Configuring DNS Actions, Configuring DNS Policies, and Binding DNS Policies, respectively.

EdgeSight Monitoring

The following EdgeSight monitoring enhancement is available in this release.

Exporting EdgeSight Information to AppFlow Collector

You can now export web page monitoring information collected through EdgeSight Monitoring to AppFlow collectors so that you get an in-depth analysis of the web page monitoring data. To export web page monitoring statistics to AppFlow collectors, you have to associate an AppFlow action with the EdgeSight Monitoring responder policy.

You can also configure load balancing and content switching virtual servers to export EdgeSight Monitoring statistics to AppFlow collectors by associating an AppFlow action with the virtual servers.

Global Server Load Balancing

The following global server load balancing enhancements are available in this release.

Overriding Static Proximity Behavior by Configuring Preferred Locations

You might want to direct traffic from a local DNS (LDNS) server or network to a GSLB service other than the GSLB service that the static proximity method selects for that traffic. That is, you have a *preferred location* for that traffic. To override the static proximity method with preferred locations, you can do the following:

1. Configure a DNS action that consists of a list of preferred locations.
2. Configure a DNS policy to identify the traffic arriving from the LDNS server or network and apply the action in the policy.
3. Bind the policy to the global request bind point.

For more information, see Overriding Static Proximity Behavior by Configuring Preferred Locations.

Confirmation Prompt before Synchronization of Global Server Load Balancing Sites

Unlike in earlier releases, when you use the sync gslb config command or its alias, the sync config command, the NetScaler appliance displays a warning that the synchronization of GSLB sites can result in loss of configuration on remote sites and prompts you to confirm that you want to synchronize the sites. The prompt helps prevent unintentional synchronization that might result from accidental use of the command.

Option to Save the Configuration on All Nodes after Synchronization

If you specify the saveConfig option in the sync gslb config command, all the nodes that participate in the GSLB configuration synchronization process save their configuration automatically after synchronization completes. The master saves its configuration immediately before synchronization begins. Slave nodes save their configuration after the process of synchronization is complete. A slave node saves its configuration only if the configuration difference was applied successfully on it. The option is mutually exclusive with the preview option.

Integrated Caching

The following Integrated Caching enhancements are available in this release.

Seek Streaming of Large Content

The integrated cache can now serve partial content for byte-range requests greater than 9 MB, such as byte-range requests of PDF documents or HTML5 videos. For example, you can jump to any location within a video, and integrated caching fetches the video content from that location.

Multi-part Byte Range Requests Handling from Cache

The integrated cache can now serve partial content from the cache in response to multi-part byte-range requests. Therefore, you can now specify multiple ranges of content to be served. For example, you can specify that, within 1024 bytes of content, the content of bytes 50-100 and bytes 450-700 is to be served in one request.

Viewing Cache Objects

You can now view cache objects on the basis of HTTP status code by using the command `show cache object -httpStatus <status code>`.

Enabling Persistence based on ETag Header

The ETag header now includes information about the server that served the content. You can enable this feature by using the command `set ns httpprofile <profilename>-persistentETag enabled`. When persistent ETag is enabled, the cache validation conditional requests or browser requests, for that content, always hit the same server.

If the cache validation request hits another server that has the same content, the content is re-fetched from the other server, because the ETags would be different. For example, with load balancing, the integrated cache might cache the content from say, Server S1, with S1-ETag. For the next request for this content, the cache serves the content with the S1-ETag. When the S1-ETag must be revalidated in the cache, the NetScaler sends a request with the S1-ETag to a server that is determined by the load balancing virtual server. This means that the validation request can be received by any of the other servers available. If the request goes to a server besides S1, the server would serve the full response with S2-ETag, by virtue of the fact that the ETags are different (even though the content is the same).

The integrated cache removes the old content and replaces it with the new content, which results in serving the FULL content to the client.

For more information, see Configuring Connection Options with HTTP Profiles.

Caching of SQL Protocols

You can now cache responses of SQL protocol types such as MYSQL and MSSQL. When adding a cache content group, you must specify the response type, HTTP, MYSQL, or MSSQL, to be cached. By default, the content group is HTTP. Request based policies for SQL caching support actions CACHE and INVAL, while response based policies support only the NOCACHE action.

For more information about Caching of Database protocols, see Caching Support for Database Protocols.

Load Balancing

The following load balancing enhancements are available in this release.

Firewall Load Balancing

In a firewall load balancing setup in which a set of firewalls is configured on both sides (upstream and downstream) of the NetScaler appliance, if traffic is coming though one set of firewalls (for example, upstream), you can now perform load balancing on the other set of firewalls (for example, downstream). At the command line, type:

set lb parameter -vServerSpecificMac ENABLED

This parameter is DISABLED by default.

Connection Mirroring Support for Layer 2 Connection Parameters

The NetScaler appliance supports connection mirroring for Layer 2 connection parameters. When a failover occurs, the secondary appliance in the high availability (HA) pair picks up and manages the TCP connections that clients had established with the former primary appliance. Connection mirroring for Layer 2 connection parameters is required for resuming TCP connections in deployments that depend on those parameters for proper functioning. An example of such a deployment is the load balancing of Branch Repeater appliances.

To enable the secondary appliance in the HA pair to pick up and resume the TCP connections that the failed primary was handling, information associated with the following two pairs of connections must be synchronized with the secondary:

- The connection between the client and the NetScaler appliance and the connection between the NetScaler appliance and the Branch Repeater appliance.
- The connection between the Branch Repeater appliance and the NetScaler appliance and the connection between the NetScaler appliance and the server.

The first pair of connections is associated with the wildcard load balancing virtual server. Therefore, to synchronize the information associated with those connections, you must configure connection mirroring for the load balancing virtual server. Layer 2 connection parameters are also synchronized. For more information about configuring connection mirroring for a load balancing virtual server, see Configuring Connection Failover.

The second pair of connections is associated with the forwarding session. To synchronize the information associated with those connections, you must configure connection mirroring for the forwarding sessions. The connfailover parameter is applicable to all the connections that are associated with the forwarding session.

Note: Connection mirroring is available for both ACL based forwarding sessions (forwarding sessions for which the aclname parameter is set) and network based forwarding sessions (forwarding sessions for which the network parameter is set). Additionally, all bypassed traffic that meets the requirements of the ACL's are synchronized with the secondary appliance, even though that traffic does not match the wildcard virtual server.

For more information about configuring connection mirroring for forwarding sessions, see Configuring Forwarding Session Rules.

Finally, on the primary appliance, you must create a virtual router ID (VRID) and bind the VRID to the interface that communicates with the Branch Repeater appliances. For more

information about configuring a VRID and binding the VRID to an interface, see Configuring Virtual MAC Addresses.

Using a String as the Server ID for a Service

While adding or setting a service, you can now specify a string as a server ID. The string can have up to 47 characters and contain alphanumeric characters and dashes.

Use -customServerId <*string*> instead of the earlier option -serverId <*positive integer*>. The -serverId option will be deprecated.

Example

```
set service SE_WEB_SVR1 -customServerId 4324-7658-fer9-4324
```

For more information, see Custom Server ID Persistence.

Rule Based Persistence for a Virtual Server Group of Type ANY

You can configure rule-based persistence for a load balancing virtual server group to which virtual servers that use the ANY protocol are bound. For more information about rule based persistence, see Configuring Persistence Based on User-Defined Rules.

Virtual Server-Level Slow Start

You can configure the NetScaler appliance to gradually increase the load on a service (the number of requests that the service receives per second) immediately after the service is either added to a load balancing configuration or has a state change from DOWN to UP. You can either increase the load manually with load values and intervals of your choice (manual slow start) or configure the appliance to increase the load at a specified interval (automated slow start) until the service is receiving as many requests as the other services in the configuration. During the ramp-up period for the new service, the appliance uses the configured load balancing method.

This functionality is not available globally. It has to be configured for each virtual server. The functionality is available only for virtual servers that use one of the following load balancing methods:

- Round robin
- Least connection
- Least response time
- Least bandwidth
- Least packets
- LRTM (Least Response Time Method)

- Custom load

For more information, see Gradually Stepping Up the Load on a New Service with Virtual Server–Level Slow Start.

Automatic Domain Based Service Group Scaling

A domain based service group consists of members whose IP addresses are obtained by resolving the domain names of servers that are bound to the service group. The domain names are resolved by a name server whose details you configure on the appliance. A domain based service group can also include IP-address based members.

The process of name resolution for a domain based server might return more than one IP address. The number of IP addresses in the DNS response is determined by the number of address (A) records configured for the domain name, on the name server. Even if the name resolution process returns multiple IP addresses, only one IP address is bound to the service group. To scale up or scale down a service group, you need to manually bind and unbind additional domain based servers to and from the service group, respectively.

However, you can configure a domain based service group to scale automatically on the basis of the complete set of IP addresses returned by a DNS name server for a domain based server. To configure automatic scaling, when binding a domain based server to a service group, enable the automatic scaling option.

For more information, see Configuring Automatic Domain Based Service Group Scaling.

Increased Limits on the Number of Virtual Servers, Services, and Servers

The NetScaler appliance now supports a larger number of virtual servers, services, and servers. The following table shows the previous and current limits for each of these entities:

	Previous limit	Current limit
Virtual servers	8192	60000*
Services	30720	60000*
Servers	30720	60000
Bindings between virtual servers and services	46080	150000
Monitor bindings	61440	150000

* The sum total of virtual servers and services cannot exceed 60,000. For example, if you configure 4000 virtual servers, you cannot configure more than 56,000 services.

Rule Based Persistence for Load Balancing Virtual Servers of Type TCP and SSL_TCP

You can now configure a rule to define persistence criteria for load balancing virtual servers of type TCP and SSL_TCP. The persistence criteria can be based on TCP/IP protocol data, Layer 2 data, TCP options, and TCP payloads (even if the protocol that is encapsulated in the TCP payload is not HTTP).

In the add lb vserver or set lb vserver CLI command, set the `persistenceType` parameter to RULE, and then configure a rule for the rule parameter. You can define rules to configure persistence based on source and destination ports, source and destination IP addresses and IP octets, source and destination MAC addresses, VLAN IDs, payload content, and so on. Following are examples of expressions that you can use to define persistence criteria:

- `CLIENT.TCP.PAYLOAD(500).TYPECAST_NVLIST_T('=',';').VALUE("field1")`. The value of `field1`, obtained after casting the first 500 bytes of the TCP payload to a name-value list that consists of name-value pairs in the format `<name>=<value>;`.
- `CLIENT.TCP.SRCPORT`. The source port in the client request.
- `CLIENT.IP.DST`. The destination IP address in the client request.
- `CLIENT.IP.SRC.GET4`. The fourth octet (rightmost octet) of the source IP address in the client request.
- `CLIENT.ETHER.DSTMAC.GET5`. The fifth octet of the destination MAC address in the client request.
- `CLIENT.VLAN.ID`. The ID of the VLAN through which the request arrived.

Following is an example of a command that you can use to configure rule based persistence based on the destination IP address in the client request:

add lb vserver mylbvserver SSL_TCP 192.0.2.0 443 -persistenceType RULE -rule CLIENT.IP.DST

You cannot set the resRule parameter for load balancing virtual servers of type TCP or SSL_TCP.

For more information, see Configuring Persistence Based on User-Defined Rules. For a use case based on configuring rule based persistence based on a name-value pair in a TCP byte stream, see Configuring Rule Based Persistence Based on a Name-Value Pair in a TCP Byte Stream.

Wizard for Setting Up Branch Repeater Load Balancing

The NetScaler configuration utility now includes a wizard that you can use to set up a load balancing configuration for Branch Repeater appliances. You can use the Load Balancing Wizard for Citrix Branch Repeater to configure static mapping, where requests from specific clients are always forwarded to the same Branch Repeater appliance.

Note: Load balancing of Branch Repeater appliances is not supported in cluster deployments in this release.

To configure load balancing of Branch Repeater appliance by using the NetScaler configuration utility

1. In the navigation pane, click Load Balancing.
2. In the details pane, click Load Balancing wizard for Branch Repeater.
3. Follow the instructions on the screen.

NetScaler Online Help

The following enhancements are made to the NetScaler Online Help (OLH) engine:

- The search results now also display Citrix Blogs as one of the categories.
- Web search functionality is added to the search pane, which lets you perform a web search on the keywords from the OLH Window.
- Scrolling the search results pane now does not impact the position of the Search text box. The text box is made stationary.
- Functionality to collapse different categories of the search result is added to the search pane.

NetScaler SDX Appliance

The following NetScaler SDX appliance enhancements are available in this release.

Assign Multiple Cores to an Instance

When provisioning a NetScaler instance on an SDX appliance, you can now assign multiple cores to an instance. To do so, from the CPU list in the Resource Allocation page of the Provision NetScaler wizard or Modify NetScaler wizard, select the number of cores that you want to assign to the instance. You can assign a maximum of five cores to an instance. For each additional core that you assign to the instance, assign an additional 2048 MB of memory. If you modify the number of cores assigned to an existing instance, the instance implicitly stops and restarts to bring this parameter into effect.

Configuring Clock Synchronization

You can now configure your NetScaler SDX appliance to synchronize its local clock with a Network Time Protocol (NTP) server. As a result, the clock on the SDX appliance has the same date and time settings as the other servers on your network. The clock synchronization configuration does not change if the appliance is restarted, upgraded, or downgraded. However, the configuration does not get propagated to the secondary NetScaler instance in a high availability setup.

For more information, see Configuring Clock Synchronization.

New Wizards for Provisioning and Modifying a NetScaler Instance

Provisioning and modifying a NetScaler instance on the NetScaler SDX appliance is now made simple with the addition of two new wizards: the Provision NetScaler Wizard and the Modify NetScaler Wizard.

Installing an SSL Certificate on the SDX Appliance

You can now replace the default certificate that is shipped with the NetScaler SDX appliance with your own certificate. Installing an SSL certificate terminates all current client connections with the Management Service, so you have to log back on to the Management Service for any additional configuration tasks.

For more information, see Installing an SSL Certificate on the SDX Appliance.

Upgrading the XenServer Software

You can now upgrade to a later version of the XenServer software to enable functionality of some features, such as VLAN filtering, L2 mode, and VMAC support. The process of upgrading the XenServer software involves uploading the build file of the target build to the Management Service, and then upgrading the XenServer software. For more information, see Upgrading the XenServer Software.

Polling for SSL Certificates on the NetScaler Instances

You can now poll all of the NetScaler instances to check for new SSL certificates. You need to poll all of the instances if you add a new SSL certificate directly on a NetScaler instance after logging on to that instance because the Management Service is not aware of the new certificate. You can specify a polling interval or perform an immediate poll.

For more information, see Polling for SSL Certificates on the NetScaler Instances.

Allowing L2 Mode on a NetScaler Instance

A supplemental software pack supports L2 mode on NetScaler SDX appliances running XenServer 6.0. To upgrade to XenServer 6.0, see Upgrading the XenServer Software. To install the supplemental software pack, see http://support.citrix.com/article/ctx132877.

In Layer 2 (L2) mode, a NetScaler instance acts as a learning bridge and forwards all packets for which it is not the destination. Some features, such as Cloud Bridge, require that L2 mode be enabled on the NetScaler instance. With L2 mode enabled, the instance can receive and forward packets for MAC addresses other than its own MAC address. However, if a user wants to enable L2 mode on a NetScaler instance running on an SDX appliance, the administrator must first allow L2 mode on that instance. If you allow L2 mode, you must take precautions to avoid bridging loops. For more information about these precautions, see Allowing L2 Mode on a NetScaler Instance.

Configuring VMACs on an Interface

You can now configure VMACs on an interface assigned to an instance on the NetScaler SDX appliance. A NetScaler instance uses Virtual MACs (VMACs) for high availability (active-active or active-standby) configurations. A Virtual MAC address (VMAC) is a floating entity shared by the primary and the secondary nodes in a high availability setup. You must be careful when configuring VMACs. For more information, see Allowing L2 Mode on a NetScaler Instance.

Single Sign-On to the Management Service and the NetScaler Instances

Logging on to the Management Service gives you direct access to the NetScaler instances that are provisioned on the appliance, if you upgrade the Management Service and the NetScaler instances to this build. If you log on to the Management Service by using your user credentials, you do not have to provide the user credentials again for logging on to an instance. By default, the Timeout value is set to 30 minutes and the configuration tab is opened in a new browser window.

For more information, see Single Sign-On to the Management Service and the NetScaler Instances.

Backing Up and Restoring the Configuration Data of the SDX Appliance

The backup policy runs a backup at 00:30 A.M. every day, but you can create a backup file at any time if, for example, you want to immediately back up changes to the configuration.

You can use the backup file to restore the configuration data on the appliance. You can restore the configuration data of the XenServer, Management Service, and all of the NetScaler instances. Alternatively, you can restore only the NetScaler instances or selected NetScaler instances.

For more information, see Backing Up and Restoring the Configuration Data of the SDX Appliance.

Performing a Factory Reset

You can now reset the appliance to the factory default. Performing a factory reset terminates all current client sessions with the Management Service, so you have to log back on to the Management Service for any additional configuration tasks. When you are ready to restore the appliance, import the backup files by using the Management Service.

For more information, see Performing a Factory Reset.

Generating a Certificate Signing Request

You can now generate a certificate signing request (CSR) for a certificate on the NetScaler SDX appliance. A CSR is a collection of information, including the domain name, other important company details, and the private key to be used to create a certificate. To renew an existing certificate or obtain a new SSL certificate from an authorized certificate authority (CA), you must generate a CSR and submit the CSR to the CA. To generate a CSR, navigate to the NetScaler>SSL Certificates pane, select a certificate, and then click Generate CSR. Copy and paste the text directly in the order form that you send to the CA or save as a text file and send the file to the CA.

Viewing the SSL Certificates for the Management Service and the NetScaler Instances

The Management Service and the NetScaler instances use SSL certificates for secure client connections. You can now view certificate details, such as validity status, issuer, subject, days to expiration, valid from and to dates, version, and serial number. To view the SSL certificate for the Management Service, in System, under Setup Appliance, click View SSL Certificate. To view the SSL certificate for a NetScaler instance, navigate to NetScaler>SSL Certificates, select a certificate, and then click Details. You can also double-click a certificate to view the certificate details.

Monitoring CPU Core Usage on the NetScaler SDX Appliance

The CPU core usage page in the Monitoring tab of the Management Service user interface now provides the following details:

- Mapping of a core to a physical CPU.
- Hyper threads for each physical core.
- Instances running on each core.
- Average CPU usage for each core.

Initial Configuration through the Serial Console

A networkconfig utility has been added to simplify initial configuration of the SDX appliance through the serial console. For more information, see the *Citrix NetScaler SDX Quick Start Guide* for the related hardware platform.

Networking

The following Networking enhancements are available in this release.

Unsetting Parameters for any RPC Node by Using the Node IP Address

The IP address parameter of the unset rpcNode command is now a required parameter. This parameter specifies the RPC node for which you want to unset one or more of the optional parameters. Following is the synopsis of the unset rpcNode command:

unset ns rpcNode <*IPAddress*> [-password] [-srcIP] [-secure]

IS-IS Dynamic Routing Protocol

The NetScaler appliance supports the Intermediate System-to-Intermediate System (IS-IS or ISIS) dynamic routing protocol. This protocol supports IPv4 as well as IPv6 route exchanges. IS▫IS is a link state protocol and is therefore less prone to routing loops. With the advantages of faster convergence and the ability to support larger networks, ISIS can be very useful in Internet Service Provider (ISP) networks.

For more information, see Configuring ISIS.

IPv6 Support for Link Load Balancing

The NetScaler Link Load balancing (LLB) feature now supports IPv6 addresses. This support is required when Internet service providers (ISPs) assign IPv6 addresses to customers. Configuring an LLB setup with IPv6 addresses is similar to configuring a setup with IPv4 addresses, except that you now create an IPv6 service to represent your router or the next hop. Three new CLI commands (add lb route6 , show lb route6 , and rm lb route6) have been added for configuring an IPv6 route. The configuration utility has a new LLBv6 tab in the Network > Routes pane.

For more information, see Configuring an LLB Route.

Specifying IP Addresses for Backend Communication

You can specify an IP address that should be used by the NetScaler appliance as the source IP address for communication with the physical servers and peer devices. You can create IP sets, which are sets of IP addresses. You can create net profiles, which have an IP address or an IP Set, and bind a net profile to a service, service group, load balancing virtual server, or monitor. The NetScaler appliance uses the IP address specified in the net profile as the source IP address. For more information about configuring network profiles, see Using a Specified Source IP for Backend Communication.

Forwarding all Fragments of an ICMP Packet

In L3 mode, by default, the NetScaler appliance forwards only the first fragment of an ICMP request or response and drops the rest. In this mode, you can configure the appliance to forward all the ICMP fragments of an ICMP echo request that is destined for a network device. With this option enabled, the appliance also forwards all the ICMP fragments of the corresponding echo response.

One example of a situation in which this enhancement is useful is slow-link detection by a Windows 2000 Server. The Windows 2000 server sends out ICMP requests of size 2048 for

slow link detection. The NetScaler appliance can forward the fragments of the ICMP request to the destination network device and the fragments of the ICMP response from the network device to the Windows 2000 server.

IPv6 Extension Header Traversing

For simple ACL6s and ACL6s rules, the NetScaler appliance now supports traversing the extension headers (if present) of all the incoming IPv6 packets to identify the layer 4 protocol and take a specified action.

For more information on ACLs, see Access Control Lists.

ARP Response Suppression for Virtual IP Addresses (VIPs)

You can configure the NetScaler appliance to respond or not respond to ARP requests for a Virtual IP (VIP) address on the basis of the state of the virtual servers associated with that VIP.

For example, if virtual servers V1, of type HTTP, and V2, of type HTTPS, share VIP address 10.102.29.45 on a NetScaler appliance, you can configure the appliance to not respond to any ARP request for VIP 10.102.29.45 if both V1 and V2 are in DOWN state.

The following three options are available for configuring ARP-response suppression for a virtual IP address.

- NONE. The NetScaler appliance responds to any ARP request for the VIP address, regardless of the state of the virtual servers associated with the address
- ONE VSERVER. The NetScaler appliance responds to any ARP request for the VIP address if at least one of the associated virtual servers is in UP state
- ALL VSERVER. The NetScaler appliance responds to any ARP request for the VIP address if all of the associated virtual servers are in UP state.

For more information, see Configuring ARP response Suppression for Virtual IP addresses (VIPs).

SNIP Address Binding to Interfaces

You can now bind a NetScaler owned SNIP address to an interface without using Layer 3 VLANs. With this configuration, any packets related to the SNIP address go only through the bound interface.

This enhancement is useful in a scenario including a NetScaler appliance and an upstream L2 switch where the upstream switch does not support Link Aggregation channels and you want the NetScaler appliance to load balance traffic, originating from a server, across the four links to the upstream switch.

Route Monitors in High Availability in Non-INC

You can now add route monitors in a High Availability (HA) configuration in non-INC mode.

Route monitors are propagated and get synchronized only in the non-INC mode. Route monitors are useful in a non-INC mode HA configuration where you want the non-reachability of a gateway from a primary node to be one of the conditions for HA failover.

For more information, see Configuring Route Monitors.

Command Propagation changes in High Availability

In an HA configuration, when command propagation fails on the secondary node, the command still executes on the primary node.

VLAN as Gateway in the IPv6 Routes

You can now specify a VLAN instead of a gateway while adding IPv6 static routes. This option is required for adding directly connected IPv6 routes.

Also, the NetScaler appliance now supports adding directly connected routes, discovered by the dynamic routing protocols, that include a VLAN ID instead of a gateway.

Policy Based Routes for IPv6 Traffic

You can now add Policy based routes for outgoing IPv6 packets. Policy-based routing bases routing decisions on criteria that you specify. An IPv6 policy-based route (PBR6) specifies criteria for selecting IPv6 packets and, typically, a next hop to which to send the selected packets. For example, you can configure the NetScaler appliance to route outgoing IPv6 packets from a specific IPv6 address or range to a particular next hop router. Each packet is matched against each configured PBR6, in the order determined by the specified priorities, until a match is found. If no match is found, or if the matching PBR6 specifies a DENY action, the NetScaler applies the routing table for normal destination-based routing.

For more information, see Configuring a Policy-Based Routes (PBR6) for IPv6 Traffic.

Source IP selection based on a PBR

When an outgoing packet matches the rule in a PBR, the source IP selection for the packet is now based on the next hop selected. This helps in avoiding asymmetric routing.

For more information on PBRs, see Configuring Policy-Based Routes.

Load Balancing in DSR Mode for IPv6 Networks

The NetScaler now supports Load Balancing in Direct Server Return (DSR) mode for IPv6 networks by using the Type of Service (TOS) field when the NetScaler appliance and the servers are in different networks.

In this mode, when a client sends a request to a VIP6 address on a NetScaler appliance, the appliance forwards this request to the server by changing the destination IPv6 address of the packet to the IPv6 address of the server and setting an encoded value of the VIP6 address in the TOS (also called traffic class) field of the IPv6 header. You can configure the server to use the information in the TOS field to derive the VIP6 address from the encoded value, which is then used as a source IP address in response packets. Response traffic goes

directly to the client, bypassing the NetScaler.

For more information, see Configuring Load Balancing in DSR Mode for IPv6 Networks by Using the TOS Field.

Load Balancing in DSR Mode for IPv6 Networks by Using IP Tunnels

The NetScaler now supports Load Balancing in Direct Server Return (DSR) mode for IPv6 networks by using IP tunnels when the NetScaler appliance and the servers are in different networks.

The NetScaler appliance implements IP tunneling by encapsulating data packets that it receives. The encapsulation adds header information. The appliance then forwards the encapsulated data packets to the router, or appropriate server, using tunnels. The NetScaler can also act as a decapsulator if placed in front of the load balanced server.

Terminating Established Connections that Match Simple ACLs

For a simple ACL, the NetScaler appliance blocks any new connections that match the conditions specified in the ACL. The appliance does not block any packets related to existing connections that were established before the ACL was created.

However, you can immediately terminate the established connections by running a flush operation from the command line interface or the configuration utility.

Flush can be useful in the following cases:

- You receive a list of blacklisted IP addresses and want to completely block those IP addresses from accessing your servers. In this case, you create simple ACLs to block any new connections from those IP addresses, and then run flush to terminate any existing connections.
- You want to terminate a large number of connections from a particular network without taking the time to terminate them one by one.

For more information, see Terminating Established Connections.

Enable or Disable Established Parameter

You can now enable or disable the established parameter for previously configured extended ACLs or ACL6s from the command line interface by using the set and unset commands, respectively. (The parameter specifies that the ACL or ACL6 is for TCP response traffic only.)

Renaming Extended ACLs and ACL6s

You can now rename extended ACLs and ACL6s configured on the appliance.

Reverse Network Address Translation for IPv6 Traffic

You can now add Reverse Network Address Translation (RNAT) rules for IPv6 packets. These RNAT rules are called RNAT6s. When an IPv6 packet generated by the server matches the conditions specified in the RNAT6 rule, the appliance replaces the source IPv6 address of the IPv6 packet with a configured NAT IPv6 address before forwarding it to the destination. The NAT IPv6 address must be one of the NetScaler owned SNIP6 or VIP6 addresses.

When configuring an RNA6 rule, you can specify either an IPv6 prefix or an ACL6 as the condition:

IPv6 Prefix.

When you use an IPv6 prefix, the appliance performs RNAT processing on those IPv6 packets whose IPv6 address matches the prefix.

ACL6.

When you use an ACL6, the appliance performs RNAT processing on those IPv6 packets that match the conditions specified in the ACL6.

For more information, see Configuring RNAT for IPv6 Traffic.

Support for IPv4 Addresses with /31 Subnet Mask

The NetScaler now supports adding of IP addresses with /31 subnet mask compliant with RFC 3021. These IP addresses are useful on a point to point link. A /31 subnet has only two IP addresses, one can be assigned to the NetScaler appliance and the other to the peer node of a point-to-point link.

Note: The peer node of a point-to-point link should be compliant with RFC 3021.

NITRO API

The following NITRO API enhancements are available in this release.

Cluster APIs

You can use NITRO APIs to perform cluster operations such as adding cluster instances, adding cluster nodes, configuring the cluster IP address, and configuring linksets.

Display Warnings in Execution of APIs

You can now configure NITRO to display warnings that are thrown during API execution. Warnings are captured in the NITRO exception object with severity set as WARNING.

Display Paginated Statistics

You can now view statistics in a paginated manner. For example, if a query results in a large number of entries, you can display the results in multiple pages, where each page displays a specific number of entries.

Exception Handling in Bulk Operations

You can specify how exceptions are handled in bulk operations:

Exit.

Execution stops when the first error is encountered. The commands that were executed before the error are committed.

Rollback.

Execution stops when the first error is encountered. The commands that were executed before the error are rolled back. This option is supported for only the add and bind commands.

Continue.

All the commands in the list are executed even if some commands fail.

REST API Enhancements

The REST API has been enhanced for the following:

- Content-type/Accept are provided in the request header to identify object type.
- Authorization headers are provided in accordance with HTTP rules.
- Consistent use of the same URL across different methods (operations) on an object. This is applicable only if the new content-type/Accept header is used.
- Error codes and error messages are not returned in successful responses. Unsuccessful responses include the error codes and error messages. This is applicable only if the new content-type/Accept header is used.
- The HTTP status code indicates the status of the operation. It is returned in the response header.
- The cookie is now set in the request header.

Support for SDX Bulk Operations

You can now perform bulk operations on SDX appliances by using NITRO APIs. For example, when you want to provision multiple NetScaler instances on an SDX appliance, you can invoke a bulk add operation to add the NetScaler instances in a single operation.

Policy

The following Policy enhancement is available in this release.

Non-Blocking HTTP Callout

A new non-blocking version of the HTTP Callout feature is now available. Like standard HTTP Callout, the non-blocking version sends a request to the HTTP server. Unlike standard HTTP Callout, the initiator does not wait for the response. Any response is eventually dropped, although the response will be cached if cache policies are set up appropriately.

The syntax is exactly the same as the `http_callout()` function, except that the name of the function is `non_blocking_http_callout()`.

Since the initiator does not wait for the response message, non-blocking HTTP callout return a fixed response depending on the result type of the HTTP Callout. Possible responses are:

- Boolean true, for boolean results
- 0 (zero), for numeric results
- A zero-length string, for text results

Example:

```
HTTP.REQ.URL.PATH.GET_REVERSE(0) == "special" &&
SYS.NON_BLOCKING_HTTP_CALLOUT(myCallout)
```

Secure Sockets Layer (SSL)

The following Secure Sockets Layer enhancements are available in this release.

Default Syntax Policies Support for SSL

Default syntax policies are now supported for SSL. There are two types of SSL policies:

Control policy.

A control policy uses a control action. Built-in control actions:

- CLIENTAUTH-Perform client authentication.
- NOCLIENTAUTH-No client authentication.

Data policy.

A data policy uses a data action, such as inserting some data in the request or the response. An action defines the response of the NetScaler when a policy is hit. An action can be user-created or built-in. Built-in data actions are:

- RESET-Close the connection by sending a RST packet to the client.
- DROP-Drop all packets from the client. The connection remains open until the client closes it.
- NOOP-No operation is performed and the packet is forwarded.

You can add policies to a policy label and then invoke the policy label from another policy. There are two types of policy labels:

- Control policy label-holder for control policies.
- Data policy label-holder for data policies.

For more information, see Configuring SSL Actions and Policies.

Denying Nonsecure SSL Renegotiation

SSL and TLS renegotiations are vulnerable to an MITM attack that injects its own content as a prefix to a TLS connection. A new option addresses this vulnerability. If you specify `NONSECURE` as the value of the denySSLReneg parameter in the set ssl parameter command, any nonsecure renegotiations are denied. For more information about this attack, see RFC 5746. For more information about setting this parameter, see Configuring Advanced SSL Settings.

New SNMP Alarms in SSL

The following, new, SNMP alarms are added to indicate the rate of 1024, 2048, and 4096-bit key operations during SSL transactions and the number of current SSL sessions in use.

- 1024KEY-EXCHANGE-RATE
- 2048KEY-EXCHANGE-RATE
- 4096KEY-EXCHANGE-RATE
- SSL-CUR-SESSION-INUSE

SNMP

The following SNMP enhancements are available in this release.

IPv6 Based SNMP Managers

You can now add IPv6 based SNMP managers on the NetScaler appliance. You can set either of the following values for the IP Address parameter when adding IPv6 based SNMP managers.

IPv6 address of the SNMP manager.

The NetScaler appliance accepts and responds to SNMP queries from the device that is assigned this IPv6 address.

IPv6 network prefix.

The NetScaler appliance accepts and responds to SNMP queries from any device if its IPv6 address prefix matches this prefix.

Note: The NetScaler appliance does not support use of host names for SNMP managers that have IPv6 addresses. You must specify the IPv6 address.

For more information, see Specifying an SNMP Manager.

Logging SNMP Traps

You can now enable the NetScaler appliance to log any SNMP trap messages (for those SNMP alarms in which logging is enabled) even when no trap listeners are specified on the appliance. By default, the appliance logs any SNMP trap messages when at least one trap listener is specified.

For more information, see Enabling Unconditional SNMP Trap Logging.

SNMP Alarm for HA License Mismatch

A new SNMP alarm, HA-LICENSE-MISMATCH, has been introduced for detecting any mismatch between the two lists of licenses present in the two nodes of a High availability configuration.

This SNMP alarm, when configured, can generate the following SNMP trap message:

- `haLicenseCheck`

New SNMP Alarms for SSL

The following new SNMP alarms indicate the rate of 1024, 2048, and 4096-bit key operations during SSL transactions and the number of current SSL sessions in use.

- 1024KEY-EXCHANGE-RATE
- 2048KEY-EXCHANGE-RATE
- 4096KEY-EXCHANGE-RATE
- SSL-CUR-SESSION-INUSE

SNMP OID for Model number

A new SNMP OID, sysModelId (1.3.6.1.4.1.5951.4.1.1.16), returns the model number of the NetScaler appliance.

Stream Analytics

The performance of your web site or application depends on how well you optimize the delivery of the most frequently requested content. Techniques such as caching and compression help accelerate the delivery of services to clients, but you need to be able to identify the resources that are requested most frequently, and then cache or compress those resources. You can identify the most frequently used resources by aggregating real-time statistics about web site or application traffic. Statistics such as how frequently a resource is accessed relative to other resources and how much bandwidth is consumed by those resources help you determine whether those resources need to be cached or compressed to improve server performance and network utilization. Statistics such as response times and the number of concurrent connections to the application help you determine whether you must enhance server-side resources.

If the web site or application does not change frequently, you can use products that collect statistical data, and then manually analyze the statistics and optimize the delivery of content. However, if you do not want to perform manual optimizations, or if your web site or application is dynamic in nature, you need infrastructure that can not only collect statistical data but can also automatically optimize the delivery of resources on the basis of the statistics. On the NetScaler appliance, this functionality is provided by the Stream Analytics feature. The feature operates on a single NetScaler appliance and collects run-time statistics on the basis of criteria that you define. When used with NetScaler policies, the feature also provides you with the infrastructure that you need for automatic, real-time traffic optimization.

For more information, see Stream Analytics.

Surge Protection

The following Surge Protection enhancements are available in this release.

Flushing a Surge Queue without Having to Disable a Service

If you want to flush the surge queue of a service, service group, or a load balancing or content switching virtual server, now you do not need to disable the NetScaler entity. With this enhancement, you can manage the traffic in surge conditions without affecting the existing traffic.

Options are added to the command line interface and configuration utility to flush a surge queue. Flushing a surge queue does not affect the existing connections. Only the requests present in the surge queue get deleted. To get responses to those requests, the client has to send fresh requests.

When you flush the surge queue of a virtual server, the surge queues of all the services and service groups bound to it are flushed. When you flush the surge queue of a service group, the surge queues of all its members are flushed. You can flush the surge queue of one or more members of a service group without flushing the surge queues of all its members. You can flush the surge queue of a specific service.

In the configuration utility, when you select an entity, the Flush Surge Queue option is available in the action pane. In the command line interface, the flush ns surgeQ option is added with necessary options.

For more information, see Flushing the Surge Queue.

Virtual Server - Options of Response to PING

You can now configure the NetScaler not to respond to a ping message if the virtual server is DOWN. This is possible on load balancing, content switching, cache redirection, and VPN virtual servers. By default, the NetScaler responds to a ping message even if one or more virtual servers are DOWN. The option can be set at an IP address level or virtual server level. The option functions are described below.

Table 2. On an IP address:

Option	Effect
NONE	Always responds
ONE_VSERVER	Responds if at least one virtual server on this IP address is UP
ALL_VSERVER	Responds only if all the virtual servers on this IP address are UP
VSVR_CNTRLD	Responds according to the setting on the virtual servers

Table 3. On a virtual server:

Option	Effect
PASSIVE on all virtual servers	Always responds
ACTIVE on all virtual servers	Responds even if one virtual server is UP
ACTIVE on some and PASSIVE on others	Responds even if one virtual server set to ACTIVE is UP

This option can be set on an IP address only if it is a VIP.

CLI commands:

set ip <IPAddress> -icmpresponse (NONE | ONE_VSERVER | ALL_VSERVERS | VSVR_CNTRLD)

set lb vserver <name> -icmpVsrResponse (PASSIVE | ACTIVE)

You can replace lb with cs, cr, or vpn. You can configure this feature by using the configuration utility also.

System

The following System enhancements are available in this release.

TCP Westwood

The NetScaler appliance now supports TCP Westwood congestion avoidance algorithm. You can enable this algorithm by setting the Westwood option for the Flavor parameter while configuring TCP profiles.

For more information, see Configuring TCP Profiles.

Call Home

The new Call Home feature monitors the NetScaler appliance for common error conditions. If your appliance is registered with the Citrix Technical Support server, Call Home automatically uploads system data to that server in the event that one of the conditions occurs. The Appliance keeps a full log of all upload events so that you can review them. If you then contact the Citrix Technical Support team and open a case, the team can analyze the uploaded system logs and recommend possible solutions.

For more information, see Configuring Call Home.

Idle CLI Session Timeout for a System User

You can now specify a time-out value for inactive CLI sessions for a system user. If a user's CLI session is idle for a time that exceeds the time-out value, the NetScaler appliance terminates the connection.

The timeout can be defined in a user’s configuration, in a user-group configuration, and in the global configuration. The time-out for inactive CLI sessions for a user is determined by the following order of precedence:

1. Time-out value as defined in the user's configuration.
2. Time-out value as defined in the group configuration for the user’s group.
3. Time-out value as defined in the system global configuration.

For more information, see Configuring Users and Groups.

WebSocket Connection Support

The NetScaler appliance can now interpret WebSocket handshakes when the HTTP profile that is bound to the virtual server is configured to allow WebSocket connections.

For more information, see Configuring WebSocket Connections.

Web Interface

The following Web Interface enhancements are available in this release.

Customized Login Page Title for a Web Interface Site

You can now customize the Login page title for a Web Interface site. The custom title can consist of from 1 to 127 characters including letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

For more information, see Configuring the Web Interface.

Option for Activating Web Interface in Receiver Platforms

The "Enable access through mobile receiver" option has been introduced in the Web Interface GUI wizard for activating web interface sites for mobile and other receiver platforms. The option, which works with most mobile platforms, is known to work with the following:

- iPhone Receiver
- iPad Receiver
- Android Receiver
- Blackberry Receiver
- Mac Receiver
- iPad web browser
- Wyse Terminals

For more information, see Configuring the Web Interface.

Web Interface Tech Support

The show techsupport command is updated to collect the WebInterface.conf files from the NetScaler appliance.

Using the WebInterface.conf Dialog Box

The configuration utility now includes a dialog box that displays the content of the webinterface.conf file for a Web Interface site.

You can do the following from this dialog box:

- Search the WebInterface.conf file’s content for instances of a text string.
- Edit the WebInterface.conf file and save the changes.
- Easily save the WebInterface.conf file to your local computer.

For more information, see Using the WebInterface.conf Dialog Box.

Using the config.xml Dialog Box

The configuration utility now includes a dialog box that displays the content of the config.xml file for a Web Interface site of type XenApp/XenDesktop Services site.

You can do the following from this dialog box:

- Search the file’s content for instances of a text string.
- Edit the config.xml file and save the changes.

- Easily save the config.xml file to your local computer.

For more information, see Using the config.xml Dialog Box.

New Access Modes for Configuring Web Interface

The Web Interface on a NetScaler appliance now supports the following access modes:

- Direct Mode: Actual address of a XenApp or XenDesktop server is sent to the clients.
- Alternate Mode: Alternate address of a XenApp or XenDesktop server is sent to the clients.
- Translated Mode: Translated address, from the defined internal addresses to external addresses and ports mapping table, is sent to the clients from a specified network.
- Gateway Direct: Actual address of a XenApp or XenDesktop server is sent to Access Gateway.
- Gateway Alternate: Alternate address of a XenApp server is sent to Access Gateway. You cannot use this mode to access XenDesktop servers.
- Gateway Translated: Translated address, from the defined internal addresses to external addresses and ports mapping table, is sent to Access Gateway.

Note: Before you configure access method based on the client IP address, you must enable USIP mode on the web interface service to make the client's IP address available with the web interface.

For more information, see Configuring the Web Interface.

Idle Session Timeout for a Web Interface Client

You can now modify the time-out of idle Web Interface browser sessions for a client. If a client's session is idle for a time that exceeds the time-out value, the NetScaler appliance terminates the connection.

For more information, see Configuring the Web Interface.

Web Logging

The following Web Logging enhancements are available in this release.

Web Logging for an HTTP Profile

You can now log HTTP data for an HTTP profile and bind the profile to a virtual server. In the NetScaler command line, in the add ns httpprofile -name or set ns httpprofile -name command, specify the -webLog ENABLED option. In the configuration utility, navigate to System > Profiles. On the HTTP Profiles pane, add or open a profile and select **"Enable Weblogging."**

Support for Logging Source IP address in the Custom Header of a Given HTTP Request

The NSWL client can now log the originating source IP address from the custom header of a given HTTP request. You can use a new parameter in the HTTP profile where you specify an expression for extracting the custom header information from a particular HTTP request. The appliance then extracts the source IP address and sends it to the NSWL client.

A new custom log format specifier, %c, has been introduced in the NSWL client for logging the source IP address sent by the NetScaler appliance.

Logging Set-Cookie Headers

In a NetScaler Web Logging (NSWL) client, the custom log format specifier %{Foobar}o now supports the logging of information from the set cookie headers of HTTP responses.

Changes

The following changes are available in the Citrix NetScaler 10 release.

AppExpert

The following AppExpert feature changes are available in this release.

Entity Templates Feature Deprecated

In this release, the entity templates feature is deprecated. However, you can continue to create and use load balancing virtual server templates and AppExpert application templates. The documentation for this feature will be updated to reflect this change.

Limit Selector Commands are Deprecated

The limit selector commands are deprecated in this release. The autocomplete functionality of the NetScaler CLI does not work for limit selector commands, and if you use a command, the CLI displays a warning. However, the NetScaler appliance creates the limit selector so that there is no loss in functionality. Any limit selectors that are present in your configuration when you upgrade to the current release continue to function as expected after the upgrade.

Stream selectors are identical to rate limiting selectors. Therefore, you are recommended to use stream selectors in a rate limiting configuration. To configure rate limiting, do the following:

1. Create a stream selector.
2. Create a limit identifier that uses the stream selector.
3. Configure a policy that calls the limit identifier.

The following table maps each deprecated limit selector command to the stream selector command that you are recommended to use.

Deprecated limit selector command	Corresponding stream selector command
add ns limitSelector	add stream selector
rm ns limitSelector	rm stream selector
set ns limitSelector	set stream selector
show ns limitSelector	show stream selector

In the configuration utility, you can configure a selector in either of the following locations:

- **AppExpert** > **Rate Limiting** > **Selectors**
- **AppExpert** > **Stream Analytics** > **Selectors**

Compression

The following compression feature change is available in this release.

Compliance of “show cmp global” with Other “show” Commands

The output of the “show cmp global” command is now similar to the output of the “show” commands that you use for viewing global bindings for other types of default syntax policies. The “show cmp global” command continues to display all the globally bound classic policies along with their priority values. But, for default syntax policies, the command displays only those global bind points to which policies are bound, along with a count of the number of policies that are bound to each of them.

To view the details for a given global bind point, you can specify the bind point as the argument to the “type” parameter. When you specify a global bind point, the command displays all the policies that are bound to the bind point, along with their priorities and Goto expressions. Classic policy bindings are not displayed if you specify a global bind point.

Global Server Load Balancing

The following global server load balancing change is available in this release.

Backup Session Timeout Parameter is Deprecated

The global server load balancing (GSLB) parameter backupSessionTimeout is deprecated in this release. To achieve the functionality that the backupSessionTimeout parameter provided, you can use the spillover persistence parameter soPersistenceTimeout.

Load Balancing

The following load balancing changes are available in this release.

Work Load Manager Feature is Deprecated

As NetScaler Classic is no longer supported, the Work Load Manager (WLM) feature is deprecated.

Generic vserver Commands Deprecated

The set, unset, enable, disable, and rm vserver commands are deprecated on a standalone appliance and are not supported on a cluster. The show vserver command is supported.

Policies

The following policies change is available in this release.

Order of Evaluation of Operators and Operator Associativity

The order of evaluation of operators in the NetScaler policy infrastructure has been aligned with the standards set by other languages, including the C programming language and JavaScript. The following table summarizes the order of evaluation of operators and their associativity in NetScaler 10. The operators are listed in the ascending order of precedence (lowest to highest). When in doubt about the order of precedence, use parentheses to guarantee the order of evaluation that you want.

Table 1. Order of Evaluation of Operators and Their Associativity in NetScaler 10

Operator	Operator Symbol	Associativity
Logical OR	||	Left to right
Logical AND	&&	Left to right
Bitwise OR	|	Left to right
Bitwise XOR	^	Left to right
Bitwise AND	&	Left to right
Not equal to Equal to	!= ==	Non-associative
Less than Less than or equal to Greater than Greater than or equal to	< <= > >=	Non-associative
Bitwise left shift Bitwise right shift	<< >>	Left to right
Addition Subtraction	+ -	Left to right
Modulus Multiplication Division	% * /	Left to right
Logical NOT (negation) Logical bitwise NOT	! ~	Right to left
NetScaler ALT operator	ALT	Left to right

System

The following system change is available in this release.

Changes to the set ns config command

The parameters that were set with the set ns config command are now split across two commands: set ns config and set ns param. When executed on a cluster, the set ns param command is propagated to the cluster nodes. The set ns config command is not propagated to the cluster nodes.

Bug Fixes

The following issues have been fixed in this release.

Note: Unless stated otherwise, the bug fixes apply to Citrix® NetScaler® 10 nCore™ and NetScaler® 10 nCore™ VPX™.

AGEE Issues

Issue ID 0306678

If Access Gateway license is bound to any host name other than "ns" or "ANY", the license is considered to be inapplicable on Access Gateway.

System Issues

Issue ID 0290271 (nCore)

If a 1G e1k interface is reset, the hardware controller RX logic might write to the data area of a NetScaler packet buffer (NSB) after it has been returned to the NSB free pool. This can result in NSB corruption. An interface reset can be triggered by an event, such as changing the flow control settings by using the set interfacecommand.

Known Issues and Workarounds

The following known issues have been identified in this release. Workarounds are included where applicable.

AAA Issues

Issue IDs 0303465 and 0303507

The NetScaler 10 release contains an upgrade of the Likewise software, used to provide Kerberos support, from version 5.4 to version 6.1. Because of this upgrade, after upgrading a NetScaler appliance that uses Kerberos authentication to NetScaler 10, or when installing a new NetScaler appliance and configuring it to use Kerberos authentication, the NetScaler appliance does not rejoin the domain automatically. For Kerberos authentication to function properly, you must manually join your NetScaler appliance to the domain.

1. Before upgrading the Likewise server, log on to the windows active domain controller and do the following steps:

   a. In the Active Directory Users and Computers [file/dialog box/what?], remove the NetScaler appliance from the computer list.

   b. From the domain controller shell, type the following command to create the kerbtabfile.txt file:

   ```
   >ktpass –princ HTTP/kerberos.crete.example.com@crete.example.com
     -ptype KRB5_NT_PRINCIPAL -mapuser kerberos@crete.example.com
     -mapop set -pass Citrix1 -out C:\kerbtabfile.txt
   ```

   Note: Type the preceding command on a single line, although the display wraps to multiple lines.

2. After upgrading to Likewise 6.1, log onto the NetScaler appliance, open a shell, and do the following steps:

   a. Import the kerbtabfile.txt file from the domain controller to the /etc directory on the NetScaler appliance.

   b. At the shell prompt, run the necessary programs to rejoin the domain, as shown below.

   ```
   # cd /opt/likewise/bin/
   # ktutil
   # rkt /etc/kerbtabfile.txt
   # wkt /etc/krb5.keytab
   # list
   # domainjoin-cli join <EXAMPLE.COM> <DOMAINUSERNAME>
   ```

AGEE Issues

Issue ID 0251110

When you enable ICA proxy on Access Gateway and when users connect to XenDesktop, if users attempt to open a published application, the Secure Ticket Authority (STA) issues a session ticket with an invalid format and the connection fails.

Issue ID 0251596

After you configure Access Gateway to provide user connections through Citrix Receiver, when users right-click the Receiver icon in the notification area, the Log On option does not appear. Users must connect by using the Web browser or they must right-click the Receiver icon, click Preferences, and then click Plug-in status. You can also enable the Log Option to appear when users right-click the Receiver icon by adding the following settings in the registry:

1. Add the Receiver key (if the key doesn't already exist) under HKEY_CURRENT_USER\Software\Citrix\ as well as under HKEY_LOCAL_MACHINE\Software\Citrix\

2. Add the Inventory key under HKEY_CURRENT_USER\Software\Citrix\Receiver as well as under HKEY_LOCAL_MACHINE\Software\Citrix\Receiver

3. Configure following REG_SZ values under the Inventory key:

   - VPNAddress. Provide the value as the Web address for the server running Access Gateway; for example, `https://<AGEE-server-fqdn>/`.

   - VPNPrompt1. Provide the value as "UserName".

   - VPNPrompt3. Provide the value as "*Password".

Issue ID 0261547

When you enable Access Gateway as a reverse proxy and you enable basic preauthentication and post- authentication scans, as well as encryption and client choices, when users log on with the Access Gateway Plug-in, the preauthentication scan passes, but the post-authentication scan fails.

Issue ID 0285995

If you configure Access Gateway to assign an Intranet IP address to user devices that connect to Access Gateway, when users log on with the Access Gateway Plug-in, the secure DNS dynamic update does not occur and the Intranet IP address is not registered with the DNS Server.

Issue ID 0288469

After you configure a virtual server to use the Java client, when users log on with the Access Gateway Plug-in by using a browser that has a 64-bit Java Runtime Environment (JRE) installed, the Java client fails to establish a connection.

Issue ID 0290976

When you configure a post authentication policy on Access Gateway and configure the policy to redirect the connection to the Web Interface if the endpoint analysis fails, when users log on with the Access Gateway Plug-in, if the user device fails the endpoint analysis scan, users receive the Access Gateway logon page instead of the Web Interface.

Issue ID 0291264

If you create a Web Interface 5.4 site and enable authentication through Access Gateway, and you enable single sign-on with a smart card to the Web Interface that enables smart card pass-through, when users log on with the Access Gateway Plug-in, the users' desktops are not listed on the Web Interface.

Issue ID 0291821

If you create a Web Interface 5.4 site and enable authentication with a smart card through Access Gateway, and you configure the **Single Sign-on Domain** on the **Published Applications** tab using the format domainname.com instead of domainname, when users start a published application or desktop, authentication fails.

Issue ID 0291822

If you create a Web Interface 5.4 site and enable single sign-on with a smart card to the Web Interface that prompts user for a PIN, and if you do not configure the **Single Sign-on Domain** on the **Published Applications** tab, when users log on with the Access Gateway Plug-in and start a published application or desktop, authentication (directly or through single sign-on) fails. You must configure Single Sign-on Domain.

Issue ID 0292005

When users connect with clientless access and try to download a file larger than 1 gigabyte (GB) from the file share on the home page, as the file is downloading, if an upload is attempted, the download process fails but the upload continues.

Issue ID 0298971

When users log on with the Access Gateway Plug-in for Java and the Web Interface opens in Internet Explorer 9, if users do not turn on Compatibility View in Internet Explorer, when they click a published application, the following error appears: Resource shortcuts are not available.

Issue ID 0299515

If you configure an intranet IP address on Access Gateway, when users connect with the Access Gateway Plug-in on a computer running Windows XP SP3 and try to access a CIFS share hosted on a computer in the secure network, users receive an error that the share is inaccessible.

Issue ID 0300511

When users log on using clientless access and click a bookmark from the home page to open a Distributed File Share (DFS), if the target folder resides on a different computer than the computer where the domain DFS server resides, the share does not open.

Issue ID 0301060

When you configure IP pooling, enable intranet IP addresses, and disable spillover, when users log on with the Access Gateway Plug-in and then try to log on from a second user device, the Transfer Login page appears. However, the message appears incorrectly as text only on a blank page.

Issue ID 0301338

If a user password is longer than 31 characters, when users try to log on through the Access Gateway Plug-in logon dialog box rather than through a Web browser, logon fails. A message appears stating that the user name and password are invalid.

Application Firewall Issues

Issue ID 0291389

Logs sent to a remote auditlog server have missing and incorrect information.

Issue IDs 0299940, 0300223, 0302044, 0302053, 0302055, and 0302077

The UI display of the Type field for application firewall profile and some parameter settings may appear inaccurate but the underlying functionality works as expected.

Workaround: Click Refresh to display an updated profiles list or the UI display.

Issue ID 0300465

If you upgrade from NetScaler 9.3 to NetScaler 10, any existing user-created signature objects are not upgraded to the new schema format.

Workaround: After upgrading to NetScaler 10, open each signature object and click OK. The signature objects will be upgraded to the new version.

Issue ID 0300827

Regular Expressions are not supported in NetScaler expressions that are used in application firewall signatures.

Issue ID 0283780

To enable sessionless URL closure, you must first enable URL closure. If you do not, in the configuration utility the Sessionless URL Closure check box is selected, but the feature is not enabled.

Issue ID 0284009

If the sessionless URL closure option in the Start URL check is enabled, and blocking is not enabled for the Start URL check, then occasional Referer-Check violations might occur. This is harmless, and is consistent with the design of this feature. If you want to prevent any Referer-Check violations from appearing in the logs, set the Referer-Check option to none.

Issue IDs 0282932, 0301817, 0302748, 03022820, and 302295

Users must keep the following points in mind when configuring response-side Credit Card and Safe Object signature rules:

- Credit Card and Safe Object rules should be configured either as signature rules or as security check profile protections, but not both. If you configure both types of protection in the same profile, only the signature rules are applied. The security check profile protections are skipped.
- Every response-side signature rule must be associated with a request-side rule.
- Every response-side signature rule must contain at least one literal pattern.
- Although the configuration utility allows other choices, signature rules do not work unless the user sets the location to HTTP_RESP_BODY.
- Although the Max Length parameter is found under "optional parameters", Max Length must be specified.
- In Response Pattern, do not use the Expression pattern type.

Issue IDs 0302368 and 0302294

Certain learned rules that contain specific special characters and sequences cannot be skipped or removed, and may not be deleted from the learned rules list after being deployed.

Issue ID 0303049

When using the configuration utility, you can import application firewall profiles from your desktop, a local hard disk on your computer, or a remote location accessible by HTTP. You can also export profiles to your desktop or a local hard disk. When using the NetScaler command line, you can import and export profiles only to and from a hard drive or device on the NetScaler appliance.

To import a profile directly from your computer in one step, use the configuration utility. To store exported profiles on a remote server, you must use ftp or another utility to transfer them to that server.

Issue IDs 0303057 and 0301813

If the user enables transformation of SQL Injection and Cross-Site Scripting special characters, common event format (CEF) logs of violations of the HTML SQL Injection and HTML Cross-Site Scripting checks cannot be click-deployed as exemptions (relaxations) from the log viewer. The same issue affects logs of many Cross-Site Request Forgery (CSRF) violations.

Issue ID 0303044

Only QualysGuard WAS 1.0 scan reports are supported when importing signature rules. WAS 2.0 scan reports are not supported.

Cluster Issues

Issue ID 0269773

On some switches like Extreme, PTP multicast packets are processed by the CPU and are dropped if the switch does not understand the packet.

Workaround: There is an option on Extreme switch where you can disable multicast packets reaching CPU: ipmcforwarding to-cpu off ports 41-48 (specify the backplane interfaces)

Issue ID 0276162

Cluster commands are not propagated from the configuration coordinator to other nodes, when you log on to the cluster IP address using the Password Authentication mechanism. However, the commands are propagated when you log on to the cluster IP address using the Keyboard Interactive mechanism.

Issue ID 0290504

You cannot form a cluster of NetScaler appliances by using the configuration utility if you are accessing the configuration utility over a secure channel (https instead of http).

Issue ID 0302924 (nCore)

In the configuration utility, the NetScaler appliances that are added to the cluster by using the 'Discover NetScalers' option, are not automatically saved and rebooted.

Workaround: You must manually save the configuration and then warm reboot the appliances that are added.

Command-Line Interface Issues

Issue ID 0262838

The CLI man page for the `set dns parameter` command has the following errors:

- It displays ENABLED as the default value for the cacheRecords parameter. The possible values are only YES and NO, and the default value is YES.
- It displays NS_FOUR as the default value for the resolutionOrder parameter. The only possible values are OnlyAQuery, OnlyAAAAQuery, AThenAAAAQuery, and AAAAThenAQuery. The default value is OnlyAQuery.

Issue ID 0299716

In a cluster setup, the 'bind vlan' command throws an error when interface and IP address are specified together.

Workaround: Bind the interface and IP address individually, by using separate 'bind vlan' commands.

Configuration Utility Issues

Issue ID 0251463

When you click the Applications node in AppExpert, the configuration utility throws a null pointer exception. The issue occurs sporadically.

Issue ID 0278097

In the configuration utility, when a user clicks **Application Firewall** in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node are not visible. The user has to manually scroll down to view the subnodes.

Issue ID 0298686 (nCore)

If the number of records displayed exceeds the details pane area, the header row is not visible if you scroll down.

Issue ID 0300506

On the MPX 17000 platform, if you use the configuration utility to upgrade from release 9.2 build 55.5 to release 10, the appliance does not restart automatically after the upgrade.

Workaround: Restart the appliance manually by using the command line or the configuration utility.

Issue ID 0302742

If you use the configuration utility to bind a compression policy (for example, app_cmp) to an AppExpert application, the following error message appears: `Policy "app_cmp" cannot be inserted. It does not have expression with advanced syntax.`

Issue ID 0303279

In the configuration utility, in the Rewrite Policies pane, when the user clicks Add, the Create Rewrite Policy dialog box is not displayed, but the main configuration utility window is disabled.

Issue ID 0438216

In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation Issues

Issue ID 0277923

The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server, and the policy's Goto expression specifies END if it evaluates to TRUE, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated.

Domain Name System Issues

Issue ID 0291053

Under the following sequence of events, the NetScaler appliance sends the client a cached NXDOMAIN response instead of the IP addresses that are configured in the DNS action for response rewrite:

1. A security-aware name server sends the appliance a DNSSEC-enabled NXDOMAIN response for a non-existent domain. The appliance, which is designed to not rewrite DNSSEC-enabled responses, relays the negative response to the client without modifying it. The appliance also caches the response.

2. A client sends the appliance a request for the same domain, but it does not set the DNSSEC OK EDNS header bit.

This behavior is expected, and ensures that security-aware and security-oblivious clients receive the same response.

Issue ID 0301348

Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

Global Server Load Balancing Issues

Issue IDs 0287825 and 0287827

If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

Integrated Caching Issues

Issue ID 0278377 (nCore)

Cache policy labels cannot be bound to MYSQL or MSSQL virtual servers.

Issue ID 0288716

In a cluster setup, when there is a delay in processing the cache invalidation request originating from other cluster nodes, if the client sends a request before the cache invalidation request is processed on the node, the cache will serve old content.

Load Balancing Issues

Issue ID 89129/0248646

For non-HTTP load balancing virtual servers for which rule based persistence has been configured, the appliance does not automatically refresh the session time-out setting during a file download. Therefore, if the download is not completed before the session times out (and another request does not arrive before the session times out), the time-out setting is not refreshed, and requests that arrive during what would otherwise have been the extended time-out interval are forwarded to whatever server is selected by the configured load balancing method.

A consequence of this behavior is failure to accelerate some Repeater Plug-in connections in a WAN optimization configuration. If a persistence session that was created for a request from a Repeater Plug-in expires before the complete response is sent to the client, the next request from the Repeater Plug-in is sent to a different Branch Repeater appliance and is therefore not accelerated. When that happens, the Branch Repeater graphical user interface indicates that the reason for the connection not being accelerated is "Not enough room left in the TCP packet header to append unit specific options (5)."

Issue ID 90395/0249705

If the rule that is used for creating rule based persistence sessions is a compound expression, the `show lb persistentSessions` CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.

Issue ID 90875/0250110

On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

Issue ID 91711/0250846

If the string (or "token") that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR("string2").AFTER_STR("string1") if the string that is enclosed by "string1" and "string2" is not larger than 64 KB.

Issue ID 0285672

When using load balancing of Branch Repeaters in a cluster setup, there is no response from the server and the request hangs.

Issue ID 0289339

Service group members that that are configured to scale automatically are not synchronized correctly with the secondary appliance in a high availability pair. The issue can lead to appliance failure during a failover event.

Issue ID 0351632

A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

NetScaler SDX Appliance Issues

Issue ID 0261232

If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type : `#/etc/rc.d/svmd restart`

NetScaler VPX Virtual Appliance Issues

Issue ID 0302377

If you install a NetScaler VPX virtual appliance on Microsoft Server 2008 R2 by using Hyper-V Manager, or if you install a NetScaler VPX virtual appliance on VMware ESX 3.5 or 4.0, you are not prompted to specify the IP address, subnet mask, and gateway. The appliance starts with the default IP address of 192.168.100.1.

Networking Issues

Issue ID 0276933

When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.

System Issues

Issue ID 0290271 (nCore)

If a 1G e1k interface is reset, the hardware controller RX logic might write to the data area of a NetScaler packet buffer (NSB) after it has been returned to the NSB free pool. This can result in NSB corruption. An interface reset can be triggered by an event, such as changing the flow control settings by using the set interface command.

Web Interface Issues

Issue ID 86463/0246466

The new option **Make Site Path Case Insensitive** on the **Web Interface** wizard does not work as expected.

This option is expected to enable the NetScaler appliance to ignore case sensitivity in the site name part of the URL request for a Web Interface site configured on the NetScaler appliance.

Issue ID 86538/0246528

The following dialog boxes under **Upload Plugins** available in the **Web Interface** pane of the configuration utility do not work as expected:

- Windows Client
- Linux Client
- Macintosh Client

These dialog boxes are added to enable you to upload XenApp plugins for the Windows, Linux, and Macintosh platforms, respectively, to the NetScaler appliance. The plugins appear as downloadable links on the specified Web Interface sites.

Maintenance Release

This section describes the enhancements, changes, fixed issues, and known issues provided in the maintenance releases of the Citrix NetScaler, Citrix NetScaler SDX, and Citrix Access Gateway software.

Build 78.6

Release version: Citrix NetScaler, version 10 build 78.6

Replaces build: None

Release date: October 2013

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Changes and Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler.

Changes and Fixes

Application Firewall

- Issue ID 0303060: Application firewall statistics are not supported for NetScaler classic policies. If you need to see numbers of policy hits and other statistics, you must use NetScaler default syntax policies.
- Issue IDs 0370771 and 0417720: On a NetScaler appliance with the NetScaler classic operating system installed and the application firewall enabled and configured, an error in an internal pattern checking routine might cause memory corruption, which in turn might cause the appliance to crash.
- Issue IDs 0391317 and 0423289: On a NetScaler appliance with both the application firewall and integrated caching enabled, a memory leak might occur. To work around this issue, disable integrated caching.
- Issue ID 0403054: On a NetScaler appliance with the application firewall enabled, certain POST requests that lack Content-Length headers are blocked in error.
- Issue ID 0406202: On a NetScaler appliance with the application firewall enabled and a profile name that contains at least one upper-case letter, learned rules cannot be skipped, deployed, or exported. To work around this issue, ensure that all profile names use lower-case letters only.
- Issue ID 0406904: On a NetScaler appliance with the application firewall enabled, the statistics do not count hits on classic policies. Classic policies otherwise work correctly; any request that matches a classic policy is filtered correctly by the specified profile.
- Issue IDs 0422919 and 0423289: On a NetScaler appliance with the application firewall enabled and configured, if a protected web site contains a multipart web form, after repeated processing of requests and responses that contain the multipartweb form a memory leak can gradually consume available memory.

Application Firewall Signatures

- Issue ID 0376437: To improve performance, when the application firewall processes buffer overflow signatures it does not evaluate PCRE expressions unless the minLength parameter is set.

Command Line Interface

- Issue ID 0379234: The show ns runningConfig command displays the current time instead of the time at which the configuration was last modified.

Configuration Utility

- Issue ID 0416451: On the reporting tab of the NetScaler VPX configuration utility, the option for enabling the nscollect process when it is disabled rejects the user's user name and password as incorrect.
- Issue IDs 0361970, 0387024, 0397473, and 0400307: When a NetScaler session expires, a session expiry message appears in the graphical user interface, and the user has to manually enter the IP address or the domain name of the NetScaler appliance in the address bar to log back on.
- Issue IDs 0413169 and 0420113: In the configuration utility, an attempt to bind an application firewall policy to a profile results in an error message.
- Issue ID 0426594: The NetScaler configuration utility is not compatible with JRE version 7.45.

Content Switching

- Issue ID 0329544: A transaction might fail if the request is evaluated by a location based expression--CLIENT.IP.SRC.MATCHES_LOCATION(<location>)--that is bound to a content switching virtual server of type SIP_UDP, UDP, or ANY.

Global Server Load Balancing

- Issue ID 0299642: If static proximity is configured as the primary GSLB method, and it returns multiple GSLB services, the NetScaler appliance implements round robin load balancing on those services, regardless of which GSLB method is configured as the backup method. Additionally, the appliance does not consider any weights that might be configured for those GSLB services.
- Issue ID 0408374: If a configuration has a large number of GSLB services and the add location file command is used to add the location database, some of the services might not be assigned a location from the database.

High Availability

- Issue IDs 0380302, 0399048, 0400142, 0406408 and 0401234: In a high availability configuration, as a result of an internal connection timeout event, the sync ha files command might fail and display the following warning message when you run the command from the primary node: Warning: Command failed on secondary node, but succeeded on primary node. Configuration will be synchronized to ensure secondary and primary have same configuration.

- Issue IDs 0357841 and 0408502: In a high availability configuration, on a connection to an FTP virtual server with the stateful connection failover option enabled, if the FTP control connection is closed before the passive mode FTP data connection is opened, the secondary node might become unresponsive.

- Issue IDs 0420089 and 0425486: The synchronization of files in a HA setup stops working after the nsinternal user is disabled.

Load Balancing

- Issue ID 0390545: In an interactive voice response (IVR) setup, the option selected by a user is not communicated to the server because the RTSP packet is corrupted. As a result, the user is repeatedly asked to select an option from the same list.

- Issue ID 0399955 (MPX 7500): When an RTSP packet reaches NetScaler, it inserts data into the packet. If the size of the packet exceeds the limit, NetScaler splits the RTSP packet, for example, in Pkt1 and Pkt2. The NetScaler crashes when it tries to access a split RTSP packet which does not exist if the packet size is within limits.

- Issue ID 0409028: If you unbind a load balancing (LB) monitor from its service, all the connections to the configured destination IP address (destip) and port (destport) of the LB monitor are closed. In a typical L3 direct server return (DSR) deployment, the destip address and destport of the LB monitor are actually the IP address and port of the virtual server. Therefore, in a typical L3 DSR deployment, if you unbind an LB monitor from its service, all the existing connections to the virtual server are closed. As a result, performance temporarily decreases. The same behavior occurs if you delete a service.

- Issue ID 0409055: If you run a custom health monitoring script that does not require an argument, the NetScaler appliance sends an incorrect timeout to the script. As a result, the script continues to run for longer than expected. After some time, the maximum limit for the number of scripts allowed on the appliance is reached and new scripts cannot be run.

- Issue ID 0410711: If a diameter packet is received by a diameter load balancing virtual server on which persistency is enabled, and that packet contains multiple full requests and a partial request, the NetScaler fails to recognize the partial request and sends it to the server. The result is an invalid packet being sent to the server, and the NetScaler sends a 5xxx message to the client.

Load Balancing/MSSQL

- Issue ID 0401118: On a NetScaler appliance or VPX virtual appliance that is configured for load balancing in an environment that includes a Microsoft SQL server database, if a client sends a large number of long queries to the MSSQL database, the appliance might become unresponsive or fail.

Monitoring

- Issue ID 0406391: If you bind monitors to services, and then bind a DoS or SureConnect policy to one of those services, save the configuration, and restart the appliance, you lose information about monitors bound to any services created after the service to which you bound the policy was created. Also, if you run the show ns runningConfig command before restarting the appliance, the monitor binding information does not appear.

NetScaler SDX Appliance

- Issue ID 0413123: When you display the running configuration of a NetScaler instance in the Service Management interface, the double quotation marks (“) are replaced with HTML code (;quot&).

Networking

- Issue ID 0401303: When the conditions specified in an ACL rule include the != operator, the NetScaler appliance might not properly filter packets based on the ACL rule.
- Issue ID 0404861: If the NetScaler appliance has redundant L2 connectivity with a switch, the NetScaler appliance might mark its link-local IPv6 addresses as duplicate during the DAD (Duplicate address detection) process.
- Issue ID 0404849: The NetScaler appliance might restart if it receives a duplicate IPv6 fragment within a very short interval of receiving an original IPv6 fragment.
- Issue ID 0405190: When IP fragments are received on a load balancing virtual server on which the client timeout parameter set to zero, the NetScaler appliance might dump core and then restart.

Policies

- Issue ID 0410624: When a filter policy is globally bound to a NetScaler, application firewall or compression or authorization policies that are bound to a content switching virtual server are not saved in the running configuration. However, these bindings are displayed when you run the show cs vserver command.

Platform

- Issue ID 0409202: The NetScaler license is not processed if the configuration file (ns.conf) contains multiple instances of the host name, or if the host name in the ns.conf file is different from the host name in the rc.conf file. With this fix, if the ns.conf file contains multiple host names, only the name set by the set ns hostname command is used. Also, the host name in ns.conf no longer takes precedence over the host name in rc.conf.

Rewrite

- Issue ID 0401455: Modifying the content with more than one callout results in incorrect computation of the content length. This issue is not observed if all the callouts use GET requests.

SSL

- Issue IDs 0386750 and 0408393: If, when adding an entity that requires user interaction, you abort the operation before providing the requested value, a subsequent attempt to add an entity that requires user interaction fails, and the following message appears:

  User requested abort.

System

- Issue ID 0346267: The Call Home feature can be enabled by running the enable feature callhome command.
- Issue IDs 0369909 and 0381906: If you use a SNIP address for which management access is enabled as the IP address of an HTTP or HTTPS service, and the service is deleted, the NetScaler appliance fails if HTTP or HTTPS traffic is sent to that SNIP address.
- Issue ID 0391632: Stat-command output specified with the -fullValues parameter is aligned incorrectly.
- Issue ID 0391754: On a NetScaler MPX system, the SNMP count for the appliance's hardware memory and the show system memory display are incorrect. The amount of memory shown is larger than the actual amount.
- Issue ID 0401526: On a NetScaler appliance, an invalid HTTP range request results in a large amount of memory usage and the following error appears: "ERROR: Communication error with the packet engine."
- Issue ID 0407868: Remote monitoring of a high capacity appliance, such as a NetScaler MPX 22000, might indicate a drop in performance even though performance remains robust. The apparent problem is the result of a pause in the stream of monitoring data, not an actual drop in throughput.
- Issue ID 0412681: If changes are made in the nsconfig/resolv.conf file, the appliance fails to override the default DNS configurations.
- Issue ID 0415623: If you specify an invalid IPv4 address in a command that can accept either IPv4 or IPv6 address, the NetScaler shell exits automatically, because of memory corruption.

SQL DB

- Issue ID 0394093: NetScaler was buffering the query with the query length exceeding 65535 characters. This causes the NetScaler TCP window size to go down to zero, making the client to wait indefinitely.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0283556: Currently the SAML implementation supports only RSA digital signatures. DSA digital signatures are not supported.
- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberos authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, and then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.
- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

Action Analytics/Rate Limiting

- Issue ID 91353/0250526: If multiple stream identifiers and/or rate limiting identifiers evaluate a connection, the NetScaler appliance updates the counters for bandwidth, response time, and number of concurrent connections for only the identifier that evaluates the connection first. Those statistical counters are not updated for the other identifiers. However, the counter for number of requests is updated for all the identifiers that evaluate the connection.

AppFlow

- Issue ID 0327439: AppFlow records generated by the NetScaler appliance cannot be seen on SPLUNK.
- Issue ID 0333560 (nCore): AppFlow records generated by the NetScaler appliance might contain junk characters.

Application Firewall

- Issue ID 0272715: If you use the Google Chrome browser with the default Chrome PDF plugin to view the PCI-DSS report, certain links and pages do not render correctly. Workaround: Disable Chrome PDF and install the Adobe Acrobat Reader plugin for Chrome.
- Issue ID 0282932: If you use the Signature Editor to add a signature rule for a response-side check (such as the Credit Card or Safe Object check), you must also add at least one request pattern in addition to one or more response patterns. If you do not add a request pattern, the configuration utility displays an error message when you try to save the new signature rule, and the rule is not saved.
- Issue ID 0283780: When you enable the sessionless URL closure feature, you must also enable the URL closure feature. If you do not enable URL closure, the sessionless URL closure feature does not work.
- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked. Workaround: If you configure Sessionless URL Closure, set Validate Referer Header to Off.
- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported for importation as application firewall signature rules. WAS 2.0 scan reports are not supported.
- Issue ID 0313950: On a NetScaler appliance that has the application firewall configured and the Safe Object check configured, processing extremely large web pages can cause the NetScaler appliance to crash.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped. Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

Cluster

- Issue ID 0324865 (nCore VPX): In a cluster of VPX appliances that are deployed on HyperV, steered packets are dropped. Workaround: Enable MAC spoofing on the HyperV backplane interfaces.
- Issue ID 0390677: On a cluster IP address, the show interface cla/x command cannot retrieve the physical properties of the channel's member interfaces. Workaround: Use the show channel cla/x command instead.

Command Line Interface

- Issue ID 0382182 : When the output of a CLI command is piped to another command more than once, the NetScaler appliance treats the second (and later) pipes as arguments to the first piped command, instead of treating them as separate commands. This results in an invalid command and an error is thrown.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click 'Application Firewall' in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0303279: In the configuration utility, in the Rewrite Policies pane, clicking Add does not display the Create Rewrite Policy dialog box. Instead it disables the main configuration utility window.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the Create DNS View dialog box, the "Service(s) in this view" and "Policy(s) in this view" lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0333048: If you access the configuration utility through Internet Explorer 8, an attempt to bind 250 or more VIP addresses to a VLAN results in an error message about an unresponsive script.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

  Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs. Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0338513: If you use Internet Explorer 8 or Internet Explorer 9 to log on to the NetScaler configuration utility, the browser displays a blank screen, because it is displaying the compatibility view.

  Workaround: In the Compatibility View Settings dialog box, change to the standard view by clearing the Display all websites in Compatibility View check box.

- Issue ID 0352307: If you access the NetScaler configuration utility from a Mac machine with a client environment running JRE 1.7 or later, you cannot select the fields in the Java based configuration views. Workaround: Install Java 7, update 21.

- Issue ID 0353015: Load balancing virtual servers that are used by AppExpert applications are displayed in nodes other than the AppExpert node. For example, they are displayed in the Available Virtual Servers list in the Create Persistency Group dialog box (Load Balancing > Persistency Groups > Add and in the Create Persistency Group dialog box list that appears when you click the Name button in the list Create Content Switching Action dialog box Content Switching > Add > Actions).

- Issue ID 0375277: If a NetScaler connection from a client is closed without the client logging out, the session created for that connection remains active until the configured timeout period elapses. If this happens frequently, after about the 20th occurrence the user might get a "Connection limit to CFE exceeded" error message.

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to that virtual server when policy evaluation is terminated. This behavior is expected.

Domain Name System

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If the primary GSLB method fails, the backup GSLB method also fails under the following set of conditions: - A GSLB virtual server's primary GSLB method is set to round trip time (RTT) and the backup GSLB method is set to static proximity, - The primary GSLB method is set to static proximity and backup GSLB method is set to RTT, -Source IP persistence is enabled Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

Load Balancing

- Issue ID 91711/0250846: If the string (or "token") that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR("string2").AFTER_STR("string1") if the string that is enclosed by "string1" and "string2" is not larger than 64 KB.

- Issue ID 0261175: In a high availability or cluster setup, communication between a NetScaler appliance and a peer node fails if the IP address of the peer node matches the IP pattern configured for a virtual server on the appliance. Communication failure can also occur between the appliance and any IP address that is owned by a peer node, if that IP address matches the IP pattern configured for the virtual server.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

- Issue ID 0351870: If you change the load balancing group of a virtual server that has a large number of SSL sessions, the appliance might fail.

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the "show lb persistentSessions" CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the 'client.tcp.payload(n)' rule, and a request is received in multiple parts such that there is a delay between the parts, and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

Load Balancing/SSL

- Issue ID 0331621: During creation of SSL or load balancing virtual servers with the default responder action, the NetScaler appliance throws a “No such resource” error. This issue is observed only in a cluster setup.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface. Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type: `#/etc/rc.d/svmd restart`

- Issue ID 0309711: If you create an nCore VPX instance on XenServer 5.6, the instance might not start. Workaround: Upgrade to XenServer 6.0

- Issue ID 0337386: When restored from a backup, a NetScaler instance is reprovisioned by using the NetScaler XVA image currently available on the appliance, even if the backup was taken from an upgraded configuration. If multiple XVA images are available, the XVA image that was used to originally provision the instance is used, if available, to reprovision the instance. If that image is not available, any XVA image is used.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: If you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.
- Issue IDs 0283035 and 0299716: In a cluster setup, the bind vlan command throws an error when interface and IP address are specified together.
- Issue ID 0288450: The show lacp command does not display the lacp configurations. This issue is observed only in a cluster setup.
- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command set ptp -state disable and configure NTP to synchronize the time across the cluster nodes.
  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
- Issue ID 0318684: In an HA configuration in INC mode where both the nodes run the OSPF routing protocol, the secondary node drops all the L3 traffic that has the destination that was advertised by the secondary node.

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed. Workaround: Copy the certkey in the /nsconfig/ssl/ folder to all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.
- Issue ID 0343395: On the NetScaler appliance, TLS protocol version 1.2 does not support a client certificate with an RSA 4096-bit key.

System

- Issue ID 0382647: The stat system -detail command does not display the number of CPUs.

XML API

- Issue ID 0321005: The set ns hostname API now includes the ownernode parameter to specify the node for which the hostname is configured. The API is not compatible with earlier versions.

Build 77.5

Release version: Citrix NetScaler, version 10 build 77.5

Replaces build: None

Release date: August 2013

Release notes version: 2.0

Language supported: English (US)

Review the following sections:

- Changes and Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler.

Changes and Fixes

AppFlow

- Issue ID 0357496: If you enable AppFlow in Syslog, the NetScaler appliance might fail to respond. The cause is invalid typecasting of a pointer.

- Issue ID 0388650: If you enable AppFlow from a NetScaler Insight Center virtual appliance while traffic is flowing through a monitored NetScaler appliance, NetScaler Insight Center disables and then reenables the AppFlow feature for every virtual server on the NetScaler appliance. Doing that while traffic is flowing through the appliance puts some pointers out of sync. As a result, the appliance does not respond properly.

Application Firewall

- Issue ID 0236218: When configuring the Safe Commerce (credit card) check, you can now configure the application firewall to check the MIME/type of HTTP responses and skip responses that are not of the appropriate content type for Safe Commerce filtering. You can use this configuration option to prevent false positives.

  To enable MIME/type checking, at the NetScaler command line type the following command:

  bind appfw profile <name> -inspectResContentType <type>

  For <name>, substitute the name of the profile. For <type>, substitute a string that matches the MIME/type. For example, to check for and skip PDF content sent to the library profile, you would type the following:

  bind appfw profile library -inspectResContentType "text/PDF"

  To disable a MIME/type rule that you have previously enabled, use the unbind command:

  unbind appfw profile <name> -inspectResContentType <type>

- Issue ID 0383140: Relaxation rules for cross-site scripting that have special characters in field names are not honored when the application firewall action is “Transform cross-site scripts.”

- Issue ID 0390804 : If you configure an application firewall profile but do not bind any signatures to it, the NetScaler appliance becomes unresponsive or fails if a user sends a request with a JSON body to a web site protected by that profile.

- Issue ID 0403027: The application firewall includes an extraneous line break in the hidden field that it adds to forms as part of the form field consistency check. This line break is not javascript-compliant and can cause issues with javascript-enhanced forms.

Configuration Utility

- Issue ID 0360163: You cannot configure a GSLB service for which a server is not configured on the NetScaler appliance. The configuration utility displays the message `Server must be specified`.
- Issue ID 0390478: In the NetScaler configuration utility, when you modify AppFlow settings under Settings > AppFlow, the modified settings are not saved.
- issue ID 0395142: In the NetScaler configuration utility, virtual servers whose names begin with APP, AP, app, or ap are not displayed.

Content Switching

- Issue IDs 0364831 and 0386963: In random cases, if you unbind a content switching policy from a content switching virtual server, the appliance might fail.
- Issue ID 0393487: While binding a content switching policy to a content switching policy label or virtual server, you cannot specify the invoke parameter without first specifying a GotoPriorityExpression.

Global Server Load Balancing

- Issue ID 0394328: On a NetScaler appliance that has both a monitor and a GSLB view bound to a GSLB service, occasionally the view binding is not visible from the command line and is not saved in ns.conf, even though the GSLB service is properly configured and UP.

Load Balancing

- Issue ID 0335841: For MSSQL Monitor, When the data type is of type NCHAR for the column of the table, the evalRule was working fine but the evalRule failed when the data type for the other column of the table is of type CHAR.
- Issue ID 0349420: If the length of the Send String is greater than 430 characters for a HTTP-ECV load balancing monitor, it gets truncated after set lb monitor command is issued. If the send string is less than or equal to 430 chars, the Content is intact. Since we allow 512 chars to be added originally, we should ensure that 512 chars are retained throughout, even after set lb monitor cmd is issued.
- Issue ID 0349955: After you restart the appliance, the domain-based service group is shown as DOWN and the following error message appears: “Domain name cannot be resolved.”
- Issue ID 0351870: If you change the load balancing group of a virtual server that has a large number of SSL sessions, the appliance might fail.
- Issue ID 0387253: Occasionally, when you create a new load balancing virtual server in the configuration utility, a series of error messages appear. The message indicates that the load balancing feature is not licensed, and you are unable to create the virtual server.
- Issue ID 0391273: When you add a new server to an existing service group, the services in the group might be designated as DOWN even though monitoring probes succeed.
- Issue ID 0393963: If a packet engine receives a user logon request with a support-session (TASS) cookie from a session that was owned by a different packet engine, the appliance might fail.

Load Balancing/AAA-TM

- Issue ID 0390037: After authentication, if AAA generates the URL redirect, it rewrites the query portions of certain URLs into base 8 ASCII string equivalents instead of transmitting the original strings.
- Issue ID 0391105: A NetScaler appliance that has AAA-TM configured for authentication with a RADIUS Server might generate intermittent logon failures with the error message `HTTP/1.1 Internal Server Error 6`.
- Issue ID 0402472: A NetScaler appliance or VPX instance that has AAA-TM enabled and integrated caching disabled might exhibit high load or crash due to a buffer overflow if you attempt to create a KCD service account.

Load Balancing/DNS

- Issue ID 0376173: If two NetScaler appliances in a high-availability configuration have TCPB mode enabled globally, and you create a DNS TCP service, the service might be successfully created on the primary NetScaler appliance but fail on the secondary appliance.

NetScaler SDX Appliance

- Issue ID 0382221: A backup of the configuration file is created by default. If the configuration file is accidentally deleted, the backup is used when the appliance restarts.
- Issue ID 0385037: If the /var/mps/policy/mps_policy_backup.xml file is empty or corrupted, the appliance performs a core dump and the Management Service user interface becomes blank.
- Issue ID 0400164: You cannot change the default SSL certificate that is used for secure access to the Management Service.

Networking

- Issue ID 0366321: The Network Visualizer does not display the bound IP addresses of a configured VLAN.

Policy

- Issue ID 0375689: On a NetScaler appliance that has both the Responder and Application Firewall features enabled, a responder policy that accesses geolocation databases might cause the appliance to hang.
- Issue ID 0378685: The NetScaler appliance fails to respond when HTTP callouts are configured with IP address and port instead of a virtual server and if a virtual server based expression (in particular, when NetScaler evaluates the expression, even if the request comes from the callout) is configured on the appliance.

Platform

- Issue ID 0358346: NetScaler classic build is not supported on the newer NetScaler MPX platforms.
- Issue ID 0360223: In certain cases, error messages on the console of an MPX 5550/5650 or MPX 8200/8400/8600 appliance continuously scroll if the physical registers are not correctly read.
- Issue ID 0373125: The NetScaler hardware might sometimes report incorrect values for system health counters. The health counters are read over the SMBus, which is prone to reporting wrong or zero values.

SSL

- Issue ID 0333936 (nCore): If an SSL chip fails on the NetScaler MPX platform, the software attempts to reinitialize the chip and restore its operation.
- Issue ID 0352959: A memory leak occurs if a 1-byte SSL record is processed.
- Issue ID 0392328: If the case of the domain name provided in the SNI extension from the client does not match the case of the common name in the server certificate, the SSL handshake fails. The SNI extension check is not case-sensitive.
- Issue ID 0392683: In some cases, parsing an incorrectly formatted client certificate might take more than a few seconds. The delay can trigger the monitoring logic to terminate the process and restart the appliance.

System

- Issue ID 0360751: The month displayed on the CLI prompt on issuing the set prompt %d command is incorrect.
- Issue ID 0380623 (nCore): The NetScaler appliance cannot generate reports for some counters (for example, average server TTFB).
- Issue ID 0380937: Configd logs that are logged through syslog do not appear in the ns.log file, because of a conflict with library linkages.
- Issue ID 0384153: When selective acknowledgment (SACK) and partial buffering are enabled on the appliance, acknowledgments with incorrect TCP checksum are forwarded to the server.
- Issue ID 0390257: SNMP returns incorrect values for the ifOutOctets and ifInOctets counters.
- Issue ID 0392293: The NetScaler appliance wrongly advertises TCP buffer size to the client side when dynamic windows management is enabled and the service-side buffer size is larger than 40k. This problem occurs when two different TCP profiles are bound to the virtual server (buffer size is 8k) and to the service (buffer size > 40k). It causes failure when the appliance is uploading files.
- Issue ID 0394724: The SNMP module allocates memory for all OIDs in an SNMP request and queues them for further processing. This leads to memory build up in the SNMP module when there are large number of SNMP requests (each request with 100s of OIDs). This leads to memory shortage that in turn leads to memory allocation failures.

Web Interface

- Issue ID 0380241: When using Citrix Receiver for Java-client-only sites, users are unable to access their applications, because Web Interface on NetScaler fails to detect Java version 1.7.

- Issue ID 0384255: T If you access the NetScaler configuration utility by using a hostname instead of an IP address, virtual servers that are assigned to access the Web Interface sites are not displayed.

XML API

- Issue ID 0283923: The addrewriteaction API does not include the pattern argument, which is mandatory for actions of type replace_all.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0283556: Currently the SAML implementation supports only RSA digital signatures. DSA digital signatures are not supported.
- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberos authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, and then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.
- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

Action Analytics/Rate Limiting

- Issue ID 91353/0250526: If multiple stream identifiers and/or rate limiting identifiers evaluate a connection, the NetScaler appliance updates the counters for bandwidth, response time, and number of concurrent connections for only the identifier that evaluates the connection first. Those statistical counters are not updated for the other identifiers. However, the counter for number of requests is updated for all the identifiers that evaluate the connection.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

AppFlow

- Issue ID 0327439: AppFlow records generated by the NetScaler appliance cannot be seen on SPLUNK.
- Issue ID 0333560 (nCore): AppFlow records generated by the NetScaler appliance might contain junk characters.

Application Firewall

- Issue ID 0272715: If you use the Google Chrome browser with the default Chrome PDF plugin to view the PCI-DSS report, certain links and pages do not render correctly.

  Workaround: Disable Chrome PDF and install the Adobe Acrobat Reader plugin for Chrome.

- Issue ID 0282932: If you use the Signature Editor to add a signature rule for a response-side check (such as the Credit Card or Safe Object check), you must also add at least one request pattern in addition to one or more response patterns. If you do not add a request pattern, the configuration utility displays an error message when you try to save the new signature rule, and the rule is not saved.

- Issue ID 0283780: When you enable the sessionless URL closure feature, you must also enable the URL closure feature. If you do not enable URL closure, the sessionless URL closure feature does not work.

- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, requests that contain web forms with action URLs are blocked.

  Workaround: If you configure Sessionless URL Closure, set Validate Referer Header to Off.

- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported for importing as application firewall signature rules. WAS 2.0 scan reports are not supported.

- Issue ID 0303060: Application firewall statistics are not supported for NetScaler classic policies. If you need to see numbers of policy hits and other statistics, you must use NetScaler default syntax policies.

- Issue ID 0313950: On a NetScaler appliance that has the application firewall configured and the Safe Object check configured, processing extremely large web pages can cause the NetScaler appliance to crash.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

Cluster

- Issue ID 0324865 (nCore VPX): In a cluster of VPX appliances that are deployed on HyperV, steered packets get dropped.

  Workaround: Enable MAC spoofing on the HyperV backplane interfaces.

- Issue ID 0390677: On a cluster IP address, the show interface cla/x command cannot retrieve the physical properties of the channel's member interfaces.

  Workaround: Use the show channel cla/x command instead.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click 'Application Firewall' in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0303279: In the configuration utility, in the Rewrite Policies pane, clicking Add does not display the Create Rewrite Policy dialog box but disables the main configuration utility window.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0333048: If you access the configuration utility through Internet Explorer 8, an attempt to bind 250 or more VIP addresses to a VLAN results in an error message about an unresponsive script.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

  Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the Create DNS View dialog box, the "Service(s) in this view"

and "Policy(s) in this view" lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs.

  Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0338513: When you log on to NetScaler configuration utility using Internet Explorer 8 or Internet Explorer 9, the web browser displays a blank screen as the browser is displaying the compatibility view.

  Workaround: Change to the standard view, in the Compatibility View Settings dialog box, by clearing the Display all websites in Compatibility View check box.

- Issue ID 0352307: If you access the NetScaler configuration utility from a Mac machine with a client environment running JRE 1.7 or later, you cannot select the fields in the Java based configuration views.

  Workaround: Install Java 7, update 21.

- Issue ID 0353015: Load balancing virtual servers that are used by AppExpert applications are displayed in nodes other than the AppExpert node. For example, they are displayed in the Available Virtual Servers list in the Create Persistency Group dialog box (Load Balancing > Persistency Groups > Add and in the Create Persistency Group dialog box list that appears when you click the Name button in the list Create Content Switching Action dialog box Content Switching > Actions > Add).

- Issue ID 0375277: If a NetScaler connection from a client is closed without the client logging out, the session created for that connection remains active until the configured timeout period elapses. If this happens frequently, after about the 20th occurrence the user might get a "Connection limit to CFE exceeded" error message.

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to that virtual server when policy evaluation is terminated. This behavior is expected.

Domain Name System

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If the primary GSLB method fails, the backup GSLB method also fails under the following set of conditions:

  - A GSLB virtual server's primary GSLB method is set to round trip time (RTT) and the backup GSLB method is set to static proximity,

  - The primary GSLB method is set to static proximity and backup GSLB method is set to RTT,

  - Source IP persistence is enabled,

  Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

High Availability

- Issue ID 0399048: In a high availability configuration, as a result of an internal connection timeout event, the sync ha files command might fail and display the following warning message when you run the command from the primary node:

  Warning: Command failed on secondary node, but succeeded on primary node. Configuration will be synchronized to ensure secondary and primary have same configuration.

  Workaround: Run the sync ha files command from the secondary node.

Load Balancing

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the "show lb persistentSessions" CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the 'client.tcp.payload(n)' rule, and a request is received in multiple parts such that there is a delay between the parts, and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

- Issue ID 91711/0250846: If the string (or "token") that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR("string2").AFTER_STR("string1") if the string that is enclosed by "string1" and "string2" is not larger than 64 KB.

- Issue ID 0261175: In a high availability or cluster setup, communication between a NetScaler appliance and a peer node fails if the IP address of the peer node matches the IP pattern configured for a virtual server on the appliance. Communication failure can also occur between the appliance and any IP address that is owned by a peer node, if that IP address matches the IP pattern configured for the virtual server.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

Load Balancing/SSL

- Issue ID 0331621: While creating SSL or load balancing virtual servers with default responder action, the NetScaler appliance throws a “No such resource” error. This issue is observed only in a cluster setup.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type:

  ```
  #/etc/rc.d/svmd restart
  ```

- Issue ID 0309711: If you create an nCore VPX instance on XenServer 5.6, the instance might not start.

  Workaround: Upgrade to XenServer 6.0

- Issue ID 0337386: When restored from a backup, a NetScaler instance is reprovisioned by using the NetScaler XVA image currently available on the appliance, even if the backup was taken from an upgraded configuration. If multiple XVA images are available, the XVA image that was used to originally provision the instance is used, if available, to reprovision the instance. If that image is not available, any XVA image is used.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: If you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.
- Issue IDs 0283035 and 0299716: In a cluster setup, the bind vlan command throws an error when interface and IP address are specified together.
- Issue ID 0288450: The show lacp command does not display the lacp configurations. This issue is observed only in a cluster setup.
- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command set ptp -state disable and configure NTP to synchronize the time across the cluster nodes.
  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
- Issue ID 0318684: In an HA configuration in INC mode where both the nodes run the OSPF routing protocol, the secondary node drops all the L3 traffic which has the destination that was advertized by the secondary node.

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed.

  Workaround: Copy the certkey in the /nsconfig/ssl/ folder to all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.
- Issue ID 0343395: On the NetScaler appliance, TLS protocol version 1.2 does not support a client certificate with an RSA 4096-bit key.
- Issue ID 0345883 On the NetScaler appliance, TLS protocol version 1.2 does not support ephemeral Diffie-Hellman cipher suites.

XML API

- Issue ID 0321005: The set ns hostname API now includes the ownernode parameter to specify the node for which the hostname is configured. The API will not be compatible with earlier versions.

Build 76.7

Release version: Citrix NetScaler, version 10 build 76.7

Replaces build: None

Release date: May 2013

Release notes version: 3.0

Language supported: English (US)

Review the following sections:

- Changes and Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler.

Changes and Fixes

Application Firewall

- Issue ID 0333655: When the application firewall parses multipart POST requests to identify boundary text, instead of attempting to match the string "; boundary=", it instead searches for the string "boundary" within the Content-type HTTP header. The relevant RFCs permit whitespace between the semicolon (";") and the string "boundary", between the string "boundary" and the equals sign, and between the equals sign and the beginning of the boundary text value, so searching for an exact string that includes the semicolon or equals sign fails when unexpected whitespace is present. This change ensures that the application firewall correctly identifies boundary text.

- Issue ID 0369529: If an application firewall profile has the HTML cross-site scripting check configured to transform unsafe HTML, in some situations the application firewall might transform all HTML tags, including allowed HTML tags and attributes.

- Issue ID 0377610: The application firewall might crash if certain signatures are enabled and a protected web server sends a compressed response.

Configuration Utility

- Issue ID 0363408: When using the Load Balancing Wizard for Citrix XenDesktop to configure load balancing for Citrix XenDesktop, if you specify a wildcard port (*) for a load balancing virtual server, the wizard inserts an asterisk in the name of the virtual server, in the name of the associated service group, and in the name of the monitor. Because the asterisk is an invalid character for an entity name, you cannot perform any operation (such as rename, set, or remove) on those entities.

- Issue ID 0369583: If you use the configuration utility to view a Responder action, the Responder Actions page is reloaded.

- Issue ID 0376543: The View Persistence Sessions dialog box in the NetScaler configuration utility displays negative values for destination port numbers that are greater than 32767.

- Issue ID 0381521: The System Time that is displayed in the NetScaler > System Information page is incorrect.

- Issue ID 0383237: In an HA configuration, when you make configuration changes in the secondary node by using the configuration utility, the utility does not display any warning message that the configuration changes will not be propagated to the primary node.

DataStream

- Issue ID 0367120: Reference count for 'special queries'(USE/SET) stored in Netscaler were not incremented correctly, because of which Netscaler freed 'special query' even though there was a client connection referring to it. Later when a query is received on this client connection and Netscaler tries to replay the special queries linked with the connection, it crashes.

Domain Name System

- Issue ID 0292217: The NetScaler appliance functioning as a DNS proxy server and running a GSLB configuration fails under the following sequence of events:
  - The DNS virtual server receives a query for a CNAME record that does not exist on the DNS server. The queried record might or might not be associated with the domain name that is bound to the GSLB virtual server.
  - The DNS server sends a NODATA response for the CNAME record, and the appliance caches that negative response.
  - A load balancing virtual server that is part of the GSLB configuration (it is represented by a GSLB service) receives an HTTP request for the domain name for which the appliance cached the NODATA response.

Global Server Load Balancing

- Issue ID 0372920: If the NetScaler appliance has run out of memory, and you create a CNAME-based GSLB service, the appliance fails and dumps core.
- Issue ID 0378578: If a GSLB configuration includes DNS views and a GSLB virtual server that is configured with the dynamic RTT load balancing method, the NetScaler appliance does not respond with the IP address that is configured for the DNS policies. But, after the appliance stops responding with the configured IP addresses, if you configure persistence for the GSLB virtual server, the issue persists for a while, and then gets resolved automatically.

Load Balancing

- Issue ID 0335230: The NetScaler appliance fails if a client sends an RTSP load balancing virtual server an RTSP request in which the SDP content-length header has a value of 0.

- Issue ID 0349517: Sometimes, the show lb vserver <name> command does not display the content switching policies associated with the load balancing virtual server. At other times, the command displays content switching policies that are associated with other load balancing virtual servers but not with the load balancing virtual server specified in the command.

- Issue ID 0363680: CPU spikes occur on a NetScaler appliance if a load balancing virtual server and content switching virtual server are configured as follows:

  1. The load balancing virtual server is specified as a target for the content switching virtual server.

  2. Spillover persistence is configured for the load balancing virtual server.

  3. The load balancing virtual server does not have a backup virtual server.
- Issue ID 0370327: In a High Availability configuration, if some traffic is passing through a content switching virtual server for which some spillover sessions are present in the primary node, and you run the force failover command on the primary node, the node does not properly run the failover command. The secondary node then becomes unresponsive.

Monitoring

- Issue ID 0363664: The secondary appliance in a high availability configuration might fail after an upgrade if you have configured, on the appliances, an SNMP manager with a host name.

- Issue ID 0366073: IPv6 monitors of type SMTP fail if a mapped IP address is not consistent across all the processor cores in the NetScaler appliance.

NetScaler SDX Appliance

- Issue ID 0334671: If your password to log on to the Management Service contains a colon (:), you cannot create a VPX instance. With this fix, when you configure a user account on an SDX appliance, a colon is not allowed in the account password.
- Issue ID 0346496: The Management Service utility's home page does not display critical events for interfaces that are not assigned to any VPX instances.
- Issue ID 0367664: The XenServer upgrade fails in the following circumstances:
  - When the 0/2 interface is configured as the management interface instead of 0/1
  - If the IP address used for XenServer management interface is also assigned to some other device.
- Issue ID 0367788: The NetScaler appliance does not properly handle the client certificate chain with the policy mappings extension in the intermediate certificate.
- Issue ID 0371351: The Management service utility intermittently displays the state of the NetScaler instance as **Out of Service**. The state of the instance is changed back to **UP** within a minute.
- Issue ID 0372528: The SDX appliance sends power supply failure trap messages even when there is no power supply failure.

NetScaler VPX Appliance

- Issue ID 0329237: On a NetScaler VPX virtual appliance installed on VMWare ESX, if you modify the VPX to create a virtual CPU (VCPU) in addition to the two CPUs already allotted to the VPX, the appliance fails.

Networking

- Issue ID 0315773: In an Equal-cost multi-path protocol (ECMP), route selection changes with change in metric. The NetScaler may become unresponsive when the route information present in the data structure and the current selected route are different.
- Issue ID 0350486: When you set the speed of an interface to AUTO, and disable and then enable the interface, the interface comes up with a speed of 100 Mbps.
- Issue ID 0360291: An RNAT rule with RNAT IP address and a DNS service are configured on the NetScaler appliance. For DNS requests from a client, hitting the service and whose source IP address matches the RNAT rule, the NetScaler appliance forwards the DNS requests to the DNS server with source IP address field set to the RNAT IP and SNIP IP address, alternatively.
- Issue ID 0368683: For a recursive BGP route that depends on an IGP route for information, if there is some change in information in the IGP route, the NetScaler appliance does not properly update the BGP routes in its routing table.
- Issue ID 0379172: When a virtual server, which is configured as the nexthop for a PBR rule, is DOWN and non -TCP or non-UDP or non-ICMP traffic, for example GRE traffic, hits the PBR rule, the NetScaler appliance becomes unresponsive.
- Issue ID 0380685: The NetScaler becomes unresponsive when a non -TCP or non-UDP or non-ICMP traffic, for example GRE traffic, does not match any PBR rules configured on the appliance.

Platform

- Issue ID 0371521: On the MPX 8200/8400/8600 appliance, if you execute the `./ns_hw_err.bash` script, the appliance might perform a core dump and restart because of the smartctl commands present in the script.

Policies

- Issue ID 0376175: Each of the following typecasts from string (text_t or a subclass of it) simply returns the original value, if the value is not of the correct format for the type it is cast to.
  - typecast_num_t - Should check that it is a proper number (num_at)
  - typecast_unsigned_long_t - Should check that it is a proper unsigned long (unsigned_long_at)
  - typecast_double_t - Should check that it is a proper double (double_at)

Rewrite

- Issue ID 0301481: On a NetScaler appliance that has a response-side rewrite policy configured and bound to a load balancing virtual server, a request sent to the virtual server might trigger a sequence of events that causes the NetScaler appliance to fail.

SSL

- Issue ID 0275357: The NetScaler appliance fails if you add a certificate revocation list (CRL) that contains a NULL value in the nextUpdate field.
- Issue ID 0333936: If an SSL chip fails on the NetScaler MPX platform, the software now attempts to reinitialize the chip and restore its operation.
- Issue ID 0342706: If you bind a cipher or cipher group to a virtual server, service group, or service, and then save the configuration, the cipher group binding is missing from the configuration after you restart the appliance.
- Issue ID 0385542: In cluster setup, encrypted passwords are not stored in proper format.

System

- Issue ID 0333300: An LACP channel created with all of its interfaces in the UP state is shown as PARTIAL-UP instead of UP.
- Issue ID 0346613: The configuration utility displays the time for the Australia time zone as advanced by one hour.
- Issue ID 0374221: When an audit policy and a service are bound to the same virtual server, if you are modifying the syslog or nslog action, make sure that the service type, IP address and the port of the action does not match the corresponding parameters of the service.

  Note: The service type for syslog is UDP and for nslog it is TCP.
- Issue ID 0372251: When using classic and advanced policies alternatively to specify filter expression for the start nstrace command, the NetScaler appliance stops responding.
- Issue ID 0372744: A NetScaler appliance with HTML injection and AppFlow enabled, fails to respond when a web page contains an embedded URL that is longer than 4K bytes.

XML API

- Issue ID 0381778: To prevent loops when transforming a URL, you can no longer remove the priority assigned to an existing transform action. You can change an existing priority, but you cannot remove it entirely. The unset transform action command no longer accepts the -priority parameter, and the unsettransformaction_priority API has been removed from XML-API.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0283556: Currently the SAML implementation supports only RSA digital signatures. DSA digital signatures are not supported.
- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberoes authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, and then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.
- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

Action Analytics/Rate Limiting

- Issue ID 91353/0250526: If multiple stream identifiers and/or rate limiting identifiers evaluate a connection, the NetScaler appliance updates the counters for bandwidth, response time, and number of concurrent connections for only the identifier that evaluates the connection first. Those statistical counters are not updated for the other identifiers. However, the counter for number of requests is updated for all the identifiers that evaluate the connection.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

AppFlow

- Issue ID 0327439: AppFlow records generated by the NetScaler appliances cannot be seen on SPLUNK.
- Issue ID 0333560 (nCore): AppFlow records generated by the NetScaler appliance might contain junk characters.

Application Firewall

- Issue ID 0272715: If you use the Google Chrome browser with the default Chrome PDF plugin to view the PCI-DSS report, certain links and pages do not render correctly.

  Workaround: Disable Chrome PDF and install the Adobe Acrobat Reader plugin for Chrome.

- Issue ID 0282932: If you use the Signature Editor to add a signature rule for a response-side check (such as the Credit Card or Safe Object check), in addition to one or more response patterns you must also add at least one request pattern. If you do not, then when you try to save the new signature rule, the configuration utility displays an error message and does not save the rule.

- Issue ID 0283780: When you enable the sessionless URL closure feature, you must also enable the URL closure feature. If you do not enable URL closure, the sessionless URL closure feature does not work.

- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked.

  Workaround: If you configure Sessionless URL Closure, set Validate Referer Header to Off.

- Issue ID 0303060: Application firewall statistics are not supported for NetScaler classic policies. If you need to see numbers of policy hits and other statistics, you must use NetScaler default syntax policies.

- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported for importing as application firewall signature rules. WAS 2.0 scan reports are not supported.

- Issue ID 0313950: On a NetScaler appliance that has the application firewall configured and the Safe Object check configured, processing extremely large web pages can cause the NetScaler appliance to crash.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

Cluster

- Issue ID 0324865 (nCore VPX): In a cluster of VPX appliances that are deployed on HyperV, steered packets are getting dropped.

  Workaround: Enable MAC spoofing on the HyperV backplane interfaces.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click 'Application Firewall' in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0303279: In the configuration utility, in the Rewrite Policies pane, clicking Add does not display the Create Rewrite Policy dialog box but disables the main configuration utility window.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0333048: If you access the configuration utility through Internet Explorer 8, an attempt to bind 250 or more VIP addresses to a VLAN results in an error message about an unresponsive script.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

  Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the Create DNS View dialog box, the "Service(s) in this view"

and "Policy(s) in this view" lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs.

  Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0338513: When you log on to NetScaler configuration utility using Internet Explorer 8 or Internet Explorer 9, the web browser displays a blank screen as the browser is displaying the compatibility view.

  Workaround: Change to the standard view, in the Compatibility View Settings dialog box, by clearing the Display all websites in Compatibility View check box.

- Issue ID 0352307: If you access the NetScaler configuration utility from a Mac machine with a client environment running JRE 1.7 or later, you cannot select the fields in the Java based configuration views.

  Workaround: Install Java 7, update 21.

- Issue ID 0353015: Load balancing virtual servers that are used by AppExpert applications are displayed in nodes other than the AppExpert node. For example, they are displayed in the Available Virtual Servers list (Load Balancing > Persistency Groups > Add > Create Persistency Group dialog box), and in the Target LB Virtual Server list (Content Switching > Actions > Add > Create Content Switching Action dialog box > Name option button).

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated. This behavior is expected.

Domain Name System

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If a GSLB virtual server's primary GSLB method is set to round trip time (RTT) and backup GSLB method is set to static proximity, or if the primary GSLB method is set to static proximity and backup GSLB method is set to RTT, and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

High Availability

- Issue ID 0399048: In a high availability configuration, as a result of an internal connection timeout event, the sync ha files command might fail and display the following warning message when you run the command from the primary node:

  Warning: Command failed on secondary node, but succeeded on primary node. Configuration will be synchronized to ensure secondary and primary have same configuration.

  Workaround: Run the sync ha files command from the secondary node.

Load Balancing

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the "show lb persistentSessions" CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 91711/0250846: If the string (or "token") that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR("string2").AFTER_STR("string1") if the string that is enclosed by "string1" and "string2" is not larger than 64 KB.

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

- Issue ID 0261175: In a high availability or cluster setup, communication between a NetScaler appliance and a peer node fails if the IP address of the peer node matches the IP pattern configured for a virtual server on the appliance. Communication failure can also occur between the appliance and any IP address that is owned by a peer node, if that IP address matches the IP pattern configured for the virtual server.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

Load Balancing/SSL

- Issue ID 0331621: While creating SSL or load balancing virtual servers with default responder action, the NetScaler appliance throws a “No such resource” error. This issue is observed only in a cluster setup.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type: `#/etc/rc.d/svmd restart`

- Issue ID 0309711: If you create an nCore VPX instance on XenServer 5.6, the instance might not start.

  Workaround: Upgrade to XenServer 6.0

- Issue ID 0337386: When restored from a backup, a NetScaler instance is reprovisioned by using the NetScaler XVA image currently available on the appliance, even if the backup was taken from an upgraded configuration. If multiple XVA images are available, the XVA image that was used to originally provision the instance is used, if available, to reprovision the instance. If that image is not available, any XVA image is used.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.
- Issue IDs 0283035 and 0299716: In a cluster setup, the bind vlan command throws an error when interface and IP address are specified together.
- Issue ID 0288450: The show lacp command does not display the lacp configurations. This issue is observed only in a cluster setup.
- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command set ptp -state disable and configure NTP to synchronize the time across the cluster nodes.
  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```
- Issue ID 0318684: In an HA configuration in INC mode where both the nodes run the OSPF routing protocol, the secondary node drops all the L3 traffic, the destination which was advertized by the secondary node.

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator, and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed.

  Workaround: Copy the certkey under /nsconfig/ssl/ folder on all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.
- Issue ID 0343395: On the NetScaler appliance, TLS protocol version 1.2 does not support a client certificate with RSA 4096-bit key.
- Issue ID 0345883: On the NetScaler appliance, TLS protocol version 1.2 does not support ephemeral Diffie-Hellman cipher suites.

XML API

- Issue ID 0321005: The API to set the hostname for a NetScaler appliance is changed to include the owner node parameter for a cluster node. This will cause incompatibility of the API.

Build 75.7

Release version: Citrix® NetScaler®, version 10 build 75.7

Replaces build: None

Release date: April 2013

Release notes version: 2.0

Language supported: English (US)

Review the following sections:

- Changes and Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler.

Changes and Fixes

AAA Application Traffic

- Issue ID 0371118: When a user of the Google Chrome browser, version 25v or later, authenticates to a resource that is protected by AAA-TM, the user is redirected back to the login page every time he or she clicks a link after authenticating.

AppFlow

- Issue ID 0359760: The AppFlow feature is now available on ByteMobile T1100 platform with standard license.
- Issue ID 0364924: If you remove an AppFlow action while AppFlow enabled traffic is flowing through the NetScaler appliance, the appliance might fail.

Application Firewall

- Issue ID 0350947 (MPX-5500): On a NetScaler appliance with the application firewall enabled and the sessionless Form Field Consistency check enabled, if the default charset in a POST request is anything other than the expected charset, the request might be blocked.
- Issue ID 0364099: On a NetScaler appliance that has the application firewall's XML Validation security check enabled, the application firewall might hang during validation.

Configuration Utility

- Issue ID 0349711: In the upgrade wizard, selecting the **Automatically reboot** check box does not cause the appliance to automatically reboot after the software upgrade.
- Issue ID 0356683: In the NetScaler configuration utility, you can configure a feature even if the feature is not licensed.
- Issue ID 0361066: In the configuration utility, the **Location** subnode is now under the **AppExpert** node.
- Issue ID 0367612: If you use the configuration utility's **System** > **Settings** > **Configure Advanced Features** screen to change settings, and one of your changes is to unset the callhome feature, an `All commands failed [14] error` message appears.
- Issue ID 0368947: If you navigate to System > Licenses, and then in the details pane click Licenses, the Manage License view does not open.
- Issue ID 0369583: If you use the configuration utility to view a Responder action, the Responder Actions page is reloaded.
- Issue ID 0372196: On an appliance running version 10.0.73.5 of the NetScaler software, if the number of application firewall profiles on an appliance is large, you cannot use the configuration utility to display a list of the profiles. The utility throws an error.

DataStream

- Issue ID 0372380: If the NetScaler appliance delays the transmission of an MSSQL PRELOGIN response because of network congestion, it assigns an incorrect state to the MSSQL connection. Due to the incorrect connection state, the appliance fails when it receives the client's LOGIN packet.

Domain Name System

- Issue ID 0337088: A NetScaler appliance that is functioning as an end resolver might fail if it does not receive a response to one or more of the DNS queries that it generates.

Global Server Load Balancing

- Issue ID 0365173: After a persistence session of type SSLSESSION or CALLID is created for a load balancing virtual server, persistence sessions are not created for global server load balancing virtual servers. Consequently, for a global server load balancing virtual server, the NetScaler appliance uses the configured load balancing method.

Load Balancing

- Issue ID 0317281: The bind serviceGroup command, which can be used to specify either a member of or a monitor for a service group, includes two identically named parameters called state. One parameter specifies the state of a service group member's binding with the service group, and the other parameter specifies the state of a monitor's binding with the service group. When you use the command with a state parameter, the command-line interface (CLI) sometimes interprets the parameter as being associated with a member of the service group and at other times as being associated with a monitor bound to the service group. Consequently, if you use the command to specify a member, the CLI might interpret the state parameter as being associated with a monitor, and it might display an error message saying that the name of a monitor is required.

- Issue ID 0340506: A memory leak might occur on one of a pair of NetScaler appliances that are deployed as follows:

  - A RADIUS load balancing virtual server is created on one appliance, and RADIUS services are bound to the virtual server.

  - On the other NetScaler appliance, a service is created to represent the RADIUS load balancing virtual server, and a UDP-ECV monitor is bound to the service.

  The memory leak occurs on the appliance on which the RADIUS load balancing virtual server is configured.

- Issue ID 0350241: The NetScaler appliance might fail in the following set of circumstances:

  - A load balancing virtual server has a backup chain consisting of multiple backup virtual servers.

  - One or more of those backup virtual servers are dummy virtual servers (that is, their IP address and port combination is 0.0.0.0:0).

  - You disable a dummy backup virtual server or the service group bound to it, or the state of either the backup virtual server or the service group transitions to DOWN.

Monitoring

- Issue ID 0363709: If you run the clear ns config command and configuration commands for IPv6 service group members multiple times, alternately and in rapid succession, the NetScaler user interface displays incorrect details for monitors that are bound to IPv6 service group members.

NetScaler SDX Appliance

- Issue ID 0329618: If you upgrade a NetScaler SDX appliance from XenServer version 5.6 to XenServer version 6.0 and then try to modify the nsroot password, an error message appears. The error occurs because the nsroot user entry is deleted when you perform the upgrade.

- Issue ID 0330559: If you upgrade a NetScaler SDX appliance from XenServer version 5.6 to XenServer version 6.0 and then try to modify the nsroot password, an error message appears. The error occurs because the nsroot user entry is deleted when you perform the upgrade. Now, the Management Service creates an entry for nsroot if it does not find an entry in the /etc/passwd directory.

- Issue ID 0357270: If the Management Service fails to correctly apply the admin configuration, specifically the username and password, the entry for the username and password for the VPX instance is deleted from the database. If you try to modify the instance, the username field in the Modify NetScaler Wizard dialog box is blank.

- Issue ID 0360716: With NetScaler release 10 build 72.5, if you try to upload an XVA file by using Internet Explorer version 8, the following error message appears even though the file is not present on the appliance “File xxxxx.xva already exists. Do you want to overwrite?” If you click “yes," the upload is successful.

- Issue ID 0372045: If you change the system time to a future date, the backup operation runs continuously.

Networking

- Issue ID 0352992: BGP process on the NetScaler appliance may consume high CPU if advertisement interval is set to zero. With this situation, if a new process is started that consumes high CPU, the BGP process may not send out keep alive messages resulting in adjacency loss with neighbor device.

- Issue ID 0353362: For a RNAT rule, the NetScaler appliance performs RNAT processing on packets related to new connections that match the conditions specified in the RNAT rule. However, the appliance does not perform RNAT processing on packets related to existing connections that were established before the RNAT rule was created.

- Issue ID 0356664: After you restart a NetScaler appliance that has an SSL FIPS card, any delay in the initialization of the FIPS card can prevent the BGP daemon from starting.

- Issue ID 0366145: A NetScaler appliance configured for link load balancing and RNAT might fail to establish an active FTP connection from a client to an FTP server.

- Issue ID 0367266: If an RNAT rule includes an extended ACL that has some TCP parameters set, the RNAT rule may get deleted after the appliance is restarted.

- Issue ID 0369312: When you clear the configuration on a NetScaler appliance, the appliance deletes the virtual servers before the PBRs. The appliance might become unresponsive if any of the configured PBRs still includes a reference to any of the deleted virtual servers.

- Issue ID 0372754: If a service of type ANY, with the USIP parameter set to enabled and the client timeout parameter set to some value, is bound to a virtual server of type ANY, and the NetScaler appliance receives a request for a connection to the service, the TCP packet that the appliance sends to the service has the source MAC address field set to the MAC address of the next hop router.

Policy

- Issue ID 0339824: The NetScaler appliance does not respond when RESET is used as the response side action (resAction) in bidirectional policies (having request side rule).
- Issue ID 0366159: On a NetScaler appliance with a responder action for an encoded URL, the appliance might fail to recognize that the URL is encoded and therefore handle the URL improperly, causing the responder action to fail.

  The cause is that HTTP.REQ.URL implicitly sets the text mode to URL Encoded. Most operations must be performed on a decoded (plain text) URL. For example, the CONTAINS() operation needs to examine a decoded URL for the text string that it is attempting to match. If the URL is not decoded, the match might not occur if one or more characters is encoded. However, the NetScaler appliance does not decode URLs before concatenation operations. It treats an operation as a concatenation operation if the left operand, the right operand, or both are URL encoded. Not decoding URLs allows modification of the encoded URL when doing concatenation of some other portion of a URL, such as the prefix and/or suffix.

  If the user wants to concatenate using a decoded URL, the user should use the DECODE_USING_TEXT_MODE function.
- Issue ID 0370770: If an expression was URL encoded, such as in HTTP.REQ.URL, and if this expression was used to look up in a string map by using MAP_STRING(), the appliance can fail or the expression could evaluate to an incorrect value. An example expression is HTTP.REQ.URL.MAP_STRING("myMap").

SSL

- Issue ID 0352334: TLS protocol, version 1.2, handshake fails if all the following conditions are met:
  - The Client browser is Internet Explorer.
  - Client authentication is set to mandatory on the virtual server.
  - The configured client certificate on IE browser is not signed by SHA256 hash algorithm.
- Issue ID 0355336: If crypto resources are not available to a packet engine because a number of SSL cards are DOWN, all SSL virtual servers configured on the appliance are marked DOWN. The threshold value for cards going DOWN depends on the number of cores and the number of crypto cards in the appliance.
- Issue ID 0361974: If the crypto cards take longer to start than do the Access Gateway virtual servers, the virtual servers are marked DOWN.
- Issue ID 0370650 (VPX): The NetScaler VPX appliance might fail if both of the following conditions are met:
  1. OCSP is used to check for revoked certificates.
  2. Client sends the client certificate and key in the same record.

System

- Issue ID 0346613: The configuration utility displays the time for the Australia time zone as advanced by one hour.
- Issue ID 0356430: SNMP traps are not being sent when memory utilization exceeds the threshold limit.
- Issue IDs 0326105, 0370128, and 0370181: The NetScaler appliance fails to respond and then reboots on a race condition between the aggregator and the packet engine.

Web Interface

- Issue ID 0308398: The application does not load when one of the farms which is bound is a valid XenApp farm (not observed in case of invalid XenApp farm) is down or is unavailable.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0283556: Currently the SAML implementation supports only RSA digital signatures. DSA digital signatures are not supported.
- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberoes authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, and then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.
- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

Action Analytics/Rate Limiting

- Issue ID 91353/0250526: If multiple stream identifiers and/or rate limiting identifiers evaluate a connection, the NetScaler appliance updates the counters for bandwidth, response time, and number of concurrent connections for only the identifier that evaluates the connection first. Those statistical counters are not updated for the other identifiers. However, the counter for number of requests is updated for all the identifiers that evaluate the connection.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

AppFlow

- Issue ID 0327439: AppFlow records generated by the NetScaler appliances cannot be seen on SPLUNK.
- Issue ID 0333560 (nCore): AppFlow records generated by the NetScaler appliance might contain junk characters.

Application Firewall

- Issue ID 0272715: If you use the Google Chrome browser with the default Chrome PDF plugin to view the PCI-DSS report, certain links and pages do not render correctly. To work around this issue, disable Chrome PDF and install the Adobe Acrobat Reader plugin for Chrome.

- Issue ID 0282932: If you use the Signature Editor to add a signature rule for a response-side check (such as the Credit Card or Safe Object check), in addition to one or more response patterns you must also add at least one request pattern. If you do not, then when you try to save the new signature rule, the configuration utility displays an error message and does not save the rule.

- Issue ID 0283780: When you enable the sessionless URL closure feature, you must also enable the URL closure feature. If you do not enable URL closure, the sessionless URL closure feature does not work.

- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked. To work around this issue, if you configure Sessionless URL Closure, set Validate Referer Header to Off.

- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported for importing as application firewall signature rules. WAS 2.0 scan reports are not supported.

- Issue ID 0303060: Application firewall statistics are not supported for NetScaler classic policies. If you need to see numbers of policy hits and other statistics, you must use NetScaler default syntax policies.

- Issue ID 0313950: On a NetScaler appliance that has the application firewall configured and the Safe Object check configured, processing extremely large web pages can cause the NetScaler appliance to crash.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

Cluster

- Issue ID 0324865 (nCore VPX): In a cluster of VPX appliances that are deployed on HyperV, steered packets are getting dropped.

  Workaround: Enable MAC spoofing on the HyperV backplane interfaces.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click 'Application Firewall' in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0303279: In the configuration utility, in the Rewrite Policies pane, clicking Add does not display the Create Rewrite Policy dialog box but disables the main configuration utility window.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0333048: If you access the configuration utility through Internet Explorer 8, an attempt to bind 250 or more VIP addresses to a VLAN results in an error message about an unresponsive script.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

  Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the Create DNS View dialog box, the "Service(s) in this view"

and "Policy(s) in this view" lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs.

  Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0338513: When you log on to NetScaler configuration utility using Internet Explorer 8 or Internet Explorer 9, the web browser displays a blank screen as the browser is displaying the compatibility view.

  Workaround: Change to the standard view, in Tools > Compatibility View Settings dialog box, by clearing the Display all websites in Compatibility View check box.

- Issue ID 0352307: If you access the NetScaler configuration utility from a Mac machine with a client environment running JRE 1.7 or later, you cannot select the fields in the Java based configuration views.

  Workaround: Install Java 7, update 21.

- Issue ID 0353015: Load balancing virtual servers that are used by AppExpert applications are displayed in nodes other than the AppExpert node. For example, they are displayed in the Available Virtual Servers list (Load Balancing > Persistency Groups > Add > Create Persistency Group dialog box), and in the Target LB Virtual Server list (Content Switching > Actions > Add > Create Content Switching Action dialog box > Name option button).

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated. This behavior is expected.

Domain Name System

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If a GSLB virtual server's primary GSLB method is set to round trip time (RTT) and backup GSLB method is set to static proximity, or if the primary GSLB method is set to static proximity and backup GSLB method is set to RTT, and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

Load Balancing

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the "show lb persistentSessions" CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 91711/0250846: If the string (or "token") that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR("string2").AFTER_STR("string1") if the string that is enclosed by "string1" and "string2" is not larger than 64 KB.

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

- Issue ID 0261175: In a high availability or cluster setup, communication between a NetScaler appliance and a peer node fails if the IP address of the peer node matches the IP pattern configured for a virtual server on the appliance. Communication failure can also occur between the appliance and any IP address that is owned by a peer node, if that IP address matches the IP pattern configured for the virtual server.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

Load Balancing/SSL

- Issue ID 0331621: While creating SSL or load balancing virtual servers with default responder action, the NetScaler appliance throws a “No such resource” error. This issue is observed only in a cluster setup.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type: `#/etc/rc.d/svmd restart`

- Issue ID 0309711: If you create an nCore VPX instance on XenServer 5.6, the instance might not start.

  Workaround: Upgrade to XenServer 6.0

- Issue ID 0337386: When restored from a backup, a NetScaler instance is reprovisioned by using the NetScaler XVA image currently available on the appliance, even if the backup was taken from an upgraded configuration. If multiple XVA images are available, the XVA image that was used to originally provision the instance is used, if available, to reprovision the instance. If that image is not available, any XVA image is used.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.
- Issue IDs 0283035 and 0299716: In a cluster setup, the bind vlan command throws an error when interface and IP address are specified together.
- Issue ID 0288450: The show lacp command does not display the lacp configurations. This issue is observed only in a cluster setup.
- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command set ptp -state disable and configure NTP to synchronize the time across the cluster nodes.
  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator, and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed.

  Workaround: Copy the certkey under /nsconfig/ssl/ folder on all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.
- Issue ID 0343395: On the NetScaler appliance, TLS protocol version 1.2 does not support a client certificate with RSA 4096-bit key.
- Issue ID 0345883: On the NetScaler appliance, TLS protocol version 1.2 does not support ephemeral Diffie-Hellman cipher suites.

XML API

- Issue ID 0321005: The API to set the hostname for a NetScaler appliance is changed to include the owner node parameter for a cluster node. This will cause incompatibility of the API.

Build 74.4

Release version: Citrix® NetScaler®, version 10 build 74.4

Replaces build: None

Release date: February 2013

Release notes version: 3.0

Language supported: English (US)

Review the following sections:

- Changes and Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler.

Changes and Fixes

AAA Application Traffic

- Issue ID 0349418: The NetScaler appliance now supports the exclusive normalization method with SAML. For that reason, assertions posted by any SAML 2.0 compliant IDP (such as the Pingone IDP server or Oracle ID server) are now handled correctly.

AppExpert

- Issue ID 0243716: You can now configure a persistency group for the application units in an AppExpert application. In the context of an AppExpert application, a persistency group is a group of application units that you can treat as a single entity for the purpose of applying common persistence settings. When the application is exported to an application template file, the persistency group settings are included, and they are automatically applied to the application units when you import the AppExpert application.

Application Firewall

- Issue ID 0338443: The application firewall cannot use negated (!) literal strings in a fastmatch signature pattern. If you include a negated literal string in a fastmatch-designated pattern in a signatures file, the application firewall displays an error message and does not bind the signatures file to the specified profile.

- Issue ID 0360302: On a NetScaler appliance with the application firewall enabled, the cookies generated by the cookie consistency check to verify the integrity of server cookies do not have the secure flag set, as it should be for HTTPS connections.

- Issue ID 0361617: On a NetScaler appliance that has Edgesite configured, if the application firewall learning feature is enabled, it might crash intermittently. To work around this problem, disable the learning feature or reboot the NetScaler appliance.

Cluster

- Issue ID 0360131: In a cluster setup, some TCP sessions initiated by the Flow Processor are failing as Bridge Access Control Lists are applied on the Flow Receiver.

Configuration Utility

- Issue ID 0334042: The configuration utility does not display a details panel for all the entities.
- Issue ID 0349813: If you use the configuration utility to unbind all the cipher suites from a user-defined SSL cipher group, the user-defined cipher group is deleted from the appliance.
- Issue ID 0361670: If multiple domain based services are bound to a service group, and the domain name of a member cannot be resolved (its IP address is displayed as 0.0.0.0), you cannot unbind that member from the service group.
- Issue ID 0363408: When using the Load Balancing Wizard for Citrix XenDesktop to configure load balancing for Citrix XenDesktop, if you specify a wildcard port (*) for a load balancing virtual server, the wizard inserts an asterisk in the name of the virtual server, in the name of the associated service group, and in the name of the monitor. Because the asterisk is an invalid character for an entity name, you cannot perform any operation (such as rename, set, or remove) on those entities.

DataStream

- Issue ID 0357185: The MYSQL-ECV monitor closes the TCP connection with a FIN without first issuing the quit command to close the MySQL session. As a result, the `aborted_clients` counter for MYSQL servers is incremented.

High Availability

- Issue ID 0287765: In a high availability setup, SNMP traps netScalerConfigChange and netScalerConfigSave are getting generated on the secondary appliance. High Cpu usage in stats sync on 7 seconds boundary were causing latency in some transactions.

Integrated Caching

- Issue ID 0322506 (nCore): When users upgrade from 9.1 to 9.3, the number of objects being cached is reduced because of architectural changes.

Load Balancing

- Issue ID 0348302: Stateful connection failover is now supported on Layer 3 Direct Server Return (DSR) configuration that uses IP tunneling.

  Connection failover helps prevent disruption of access to applications deployed in a distributed environment. In a NetScaler High Availability (HA) setup, connection failover (or connection mirroring-CM) refers to keeping active an established TCP or UDP connection when a failover occurs.

  In stateful failover, to maintain current information about the mirrored connections, the primary appliance sends messages to the secondary appliance. The secondary appliance maintains the data related to the packets but uses it only in the event of a failover. If a failover occurs, the new primary (old secondary) appliance starts using the stored data about the mirrored connections and accepting traffic.

Monitoring

- Issue ID 0354059: The `Last response` field in the output of the show service command should indicate that a probe timed out if the following sequence of events occurs:

  1. The monitor bound to the service fails due to an internal error (for example, an unavailable ARP table entry).

  2. The error condition is corrected.

  3. Probes are successfully sent to the service, but they time out.

  Instead of text indicating that the most recent probe timed out, the content of the Last response field is `Internal error: resource unavailable to send probe`.

Networking

- Issue ID 0283793: If the NetScaler appliance receives an ICMPv6 `Packet Too Big` error for a UDP packet, it does not fragment the remaining packets to be sent to the client.

- Issue ID 0288356: With MAC-Based Forwarding (MBF) enabled, new connections to a server fail through a Virtual IP (VIP) address, if the server is configured to reach over the newly added Subnet IP (SNIP) addresses that are bound to a Layer 3 (L3) VLAN.

- Issue ID 0347842: When the NetScaler appliance reestablishes OSPF adjacency with a peer router, latency might delay the Link State (LS) updates sent by the appliance. The delay might cause the peer router to install invalid Link State Advertisements (LSAs) for a short period of time. As a result, traffic arriving during this period encounters a black-hole.

Platform

- Issue ID 0333400 The Citrix NetScaler SDX 8400/8600 platform supports NetScaler release 10 build 74.x and later.
- Issue ID 0344262: 1G copper SFP transceivers are now supported on the ixgbe (ix) interfaces. These transceivers are hot-swappable on this interface. However, fiber SFP transceivers are not supported.

  The following SFP+ and SFP transceivers, and direct access cables, are supported:

  - Intel fiber SFP+: "FTLX8571D3BCV-IT"
  - Intel fiber SFP+: "FTLX8571D3BCV-I3"
  - Finisar fiber SFP+: "FTLX8571D3BCV"
  - Intel fiber SFP+ (LR): "FTLX1471D3BCV-IT"
  - Finisar fiber SFP+ (LR): "FTLX1471D3BCV "
  - Finisar copper SFP: "FCLF-8521-3"
  - Avago copper SFP: "ABCU-5710RZ"
  - Methode DAC cable: "DM-255-100 "
  - Methode DAC cable: "DM-255-300 "
  - Methode DAC cable: "DM-255-500 "

  Note:

  - Only 10G ports support DAC cables.
  - Fiber SFPs are not supported.
- Issue ID 0357030: NetScaler release 10 build 74.x is supported on the SDX 11500/13500/14500/16500/18500/20500 NEBS platform.

Policies

- Issue ID 0334472: In some deployments you cannot remove string patterns from string maps.
- Issue ID 0342589: Existing compression policies cannot be disabled without changing the priority value.

SSL

- Issue ID 0352611: If you log on to a NetScaler account other than the administrative account and enter the show ssl service command or show running config command, the command output appears repeatedly.

System

- Issue ID 0288067: By default, the Precision Time Protocol daemon (PTPd) is disabled on a NetScaler appliance. However, if you add the node to a cluster, PTPd is automatically enabled on that node.
- Issue ID 0350189: Latency in some transactions because of high CPU usage on the 7 seconds boundary while synchronizing statistics.
- Issue ID 0353546: When you try to add a second name-based SNMP manager, you get an error message that says an SNMP manger with that name already exists.
- Issue ID 0356420: A large number of routine system health check messages are continually added to the system log.
- Issue ID 0356430: SNMP traps are not being sent.
- Issue ID 0358197: SNMP cannot complete in the 5 minutes window between polling period because it sends the request to aggregator and waits for response.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0283556: Currently the SAML implementation supports only RSA digital signatures. DSA digital signatures are not supported.
- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberoes authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, and then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.
- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

Action Analytics/Rate Limiting

- Issue ID 91353/0250526: If multiple stream identifiers and/or rate limiting identifiers evaluate a connection, the NetScaler appliance updates the counters for bandwidth, response time, and number of concurrent connections for only the identifier that evaluates the connection first. Those statistical counters are not updated for the other identifiers. However, the counter for number of requests is updated for all the identifiers that evaluate the connection.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

AppFlow

- Issue ID 0327439: AppFlow records generated by the NetScaler appliances cannot be seen on SPLUNK.
- Issue ID 0333560 (nCore): AppFlow records generated by the NetScaler appliance might contain junk characters.

Application Firewall

- Issue ID 0272715: If you use the Google Chrome browser with the default Chrome PDF plugin to view the PCI-DSS report, certain links and pages do not render correctly.

  Workaround: Disable Chrome PDF and install the Adobe Acrobat Reader plugin for Chrome.

- Issue ID 0282932: If you use the Signature Editor to add a signature rule for a response-side check (such as the Credit Card or Safe Object check), in addition to one or more response patterns you must also add at least one request pattern. If you do not, then when you try to save the new signature rule, the configuration utility displays an error message and does not save the rule.

- Issue ID 0283780: When you enable the sessionless URL closure feature, you must also enable the URL closure feature. If you do not enable URL closure, the sessionless URL closure feature does not work.

- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked. To work around this issue, if you configure Sessionless URL Closure, set Validate Referer Header to Off.

- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported for importing as application firewall signature rules. WAS 2.0 scan reports are not supported.

- Issue ID 0303060: Application firewall statistics are not supported for NetScaler classic policies. If you need to see numbers of policy hits and other statistics, you must use NetScaler default syntax policies.

- Issue ID 0313950: On a NetScaler appliance that has the application firewall configured and the Safe Object check configured, processing extremely large web pages can cause the NetScaler appliance to crash.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

Cluster

- Issue ID 0324865 (nCore VPX): In a cluster of VPX appliances that are deployed on HyperV, steered packets are getting dropped.

  Workaround: Enable MAC spoofing on the HyperV backplane interfaces.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click 'application firewall' in the navigation pane, the scroll bar moves up and the subnodes of the application firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0303279: In the configuration utility, in the Rewrite Policies pane, clicking Add does not display the Create Rewrite Policy dialog box but disables the main configuration utility window.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0333048: If you access the configuration utility through Internet Explorer 8, an attempt to bind 250 or more VIP addresses to a VLAN results in an error message about an unresponsive script.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

  Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the Create DNS View dialog box, the "Service(s) in this view"

and "Policy(s) in this view" lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs.

  Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0338513: When you log on to NetScaler configuration utility using Internet Explorer 8 or Internet Explorer 9, the web browser displays a blank screen as the browser is displaying the compatibility view.

  Workaround: Change to the standard view, in the Compatibility View Settings dialog box, by clearing the Display all websites in Compatibility View check box.

- Issue ID 0352307: If you access the NetScaler configuration utility from a Mac machine with a client environment running JRE 1.7 or later, you cannot select the fields in the Java based configuration views.

  Workaround: If you click outside and return to the browser window, you will be able to select the fields in the configuration views.

- Issue ID 0353015: Load balancing virtual servers that are used by AppExpert applications are displayed in nodes other than the AppExpert node. For example, they are displayed in the Available Virtual Servers list (Load Balancing > Persistency Groups > Add > Create Persistency Group dialog box), and in the Target LB Virtual Server list (Content Switching > Actions > Add > Create Content Switching Action dialog box > Name option button).

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated.

Domain Name System

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If a GSLB virtual server's primary GSLB method is set to round trip time (RTT) and backup GSLB method is set to static proximity, or if the primary GSLB method is set to static proximity and backup GSLB method is set to RTT, and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

Load Balancing

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the show lb persistentSessions CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 91711/0250846: If the string (or "token") that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR("string2").AFTER_STR("string1") if the string that is enclosed by "string1" and "string2" is not larger than 64 KB.

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

- Issue ID 0261175: In a high availability or cluster setup, communication between a NetScaler appliance and a peer node fails if the IP address of the peer node matches the IP pattern configured for a virtual server on the appliance. Communication failure can also occur between the appliance and any IP address that is owned by a peer node, if that IP address matches the IP pattern configured for the virtual server.

- Issue ID 0317281: The bind serviceGroup command, which can be used to specify either a member of or a monitor for a service group, includes two identically named parameters called state. One parameter specifies the state of a service group member’s binding with the service group, and the other parameter specifies the state of a monitor’s binding with the service group. When you use the command with a state parameter, the command-line interface (CLI) sometimes interprets the parameter as being associated with a member of the service group and at other times as being associated with a monitor bound to the service group. Consequently, if you use the command to specify a member, the CLI might interpret the state parameter as being associated with a monitor, and it might display an error message saying that the name of a monitor is required.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout

values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

Load Balancing/SSL

- Issue ID 0331621: While creating SSL or load balancing virtual servers with default responder action, the NetScaler appliance throws a “No such resource” error. This issue is observed only in a cluster setup.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type: `#/etc/rc.d/svmd restart`

- Issue ID 0337386: When restored from a backup, a NetScaler instance is reprovisioned by using the NetScaler XVA image currently available on the appliance, even if the backup was taken from an upgraded configuration. If multiple XVA images are available, the XVA image that was used to originally provision the instance is used, if available, to reprovision the instance. If that image is not available, any XVA image is used.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.
- Issue IDs 0283035 and 0299716: In a cluster setup, the bind vlan command throws an error when interface and IP address are specified together.
- Issue ID 0288450: The show lacp command does not display the lacp configurations. This issue is observed only in a cluster setup.
- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command set ptp -state disable and configure NTP to synchronize the time across the cluster nodes.
  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator, and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed.

  Workaround: Copy the certkey under /nsconfig/ssl/ folder on all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.
- Issue ID 0343395: On the NetScaler appliance, TLS protocol version 1.2 does not support a client certificate with RSA 4096-bit key.
- Issue ID 0345883: On the NetScaler appliance, TLS protocol version 1.2 does not support ephemeral Diffie-Hellman cipher suites.
- Issue ID 0352334: TLS protocol, version 1.2, handshake fails if all the following conditions are met:
  - The Client browser is Internet Explorer.
  - Client authentication is set to mandatory on the virtual server.
  - The configured client certificate on IE browser is not signed by SHA256 hash algorithm.

XML API

- Issue ID 0321005: The API to set the hostname for a NetScaler appliance is changed to include the owner node parameter for a cluster node.

Build 73.5

Release version: Citrix® NetScaler®, version 10 build 73.5

Replaces build: None

Release date: January 2013

Release notes version: 2.0

Language supported: English (US)

Review the following sections:

- Changes and Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler and Citrix Access Gateway.

Changes and Fixes

Access Gateway

- **Documentation:** Starting with this maintenance release, for Access Gateway issues, see http://support.citrix.com/article/CTX133966.

Application Firewall

- Issue ID 0348647: On a NetScaler appliance that has the application firewall configured, if the client sends a web form with data that contains a plus sign (+), that form field triggers a form field consistency violation. This applies for data that the user types into the form, and for data in hidden fields that was generated by a javascript or sent to the user from the server. To work around this issue, ensure that no field contains a plus sign, or temporarily disable blocking for the form field consistency check.

- Issue ID 0354289: On a NetScaler appliance that has the application firewall configured, chunked requests sent by mobile devices to XML services might receive 400-level HTTP responses. This occurs only for requests that do not contain web forms.

Cluster

- Issue ID 0343137: The configuration utility does not display the Add button while configuring linksets.

Configuration Utility

- Issue ID 0324797: The NetScaler configuration utility does not display the queue depth value for the configured priority queuing policies. This issue is observed only in a cluster setup.
- Issue ID 0334292: If you navigate to HTTP Compression > Policies or HTTP Compression > Actions, the Remove button is disabled in the task pane.
- Issue ID 0346094: The Configured table on the Monitors tab of the Configure Service dialog box does not display the correct states for monitors that are bound to a service. Any check boxes that you selected earlier, in the State column, are shown as unselected the next time you open the Configure Service dialog box for that service. However, the monitors remain active and continue to check the health of the service.
- Issue ID 0345888: If you log off and then log back on to the NetScaler configuration utility, an “Invalid username or password" error is logged in the ns.log file.
- Issue ID 0351805: The Monitor Name column of the Monitor details for service group member dialog box displays the name of the server instead of the name of the monitor.
- Issue ID 0355097: If you use the configuration utility to modify the security settings of profiles for the application firewall feature, the changes are not saved.

DataStream

- Issue ID 0354182: The flush cache contentGroup command does not flush objects that are cached in a content group of type MYSQL.

Global Server Load Balancing

- Issue ID 0344759: If you attempt to create a CNAME based GSLB service with a CNAME that is already associated with another service, the NetScaler appliance not only disallows creation of the new service, but also removes the CNAME record for that CNAME. A subsequent attempt to create a GSLB service with that CNAME is successful, and creates a new CNAME record. Therefore, two GSLB services (the previously existing service and the new one) are associated with the same CNAME.

Integrated Caching

- Issue ID 0337778: If both the rewrite feature and the Integrated caching feature are configured, the integrated caching feature might not function normally, and as a result the NetScaler appliance might fail. The problem can occur if objects are stored in selector based content groups and heavy traffic causes a server to respond slowly.
- Issue ID 0347120: For HTTP callout caching, if a response gets cached in a content group that has the minimum number of hits set to a non-zero value, the show cache object command fails.

Load Balancing/AAA Application Traffic

- Issue ID 0346093: The traffic management policy hit count shows no hits ("0") even when traffic management policies are functioning and matching traffic.

Load Balancing

- Issue ID 0278377 (nCore): Cache policy labels cannot be bound to MYSQL or MSSQL virtual servers.
- Issue ID 0330173: If a domain based service is configured with a wildcard port, its domain name does not get resolved to an IP address. Therefore, the service does not come up.
- Issue ID 0331414: The states and port numbers of load balancing virtual servers and services are not included in log entries in the newnslog file.
- Issue ID 0338196: The NetScaler appliance might fail during active-mode FTP transactions.
- Issue ID 0350458: The servicegroupbindings NITRO request (URL: `http://<NS_IP>/nitro/v1/config/servicegroupbindings/<servicegroupname>`) does not retrieve the names of t group is bound.

NetScaler SDX Appliance

- Issue ID 0318968: If you log on to a NetScaler VPX instance and change the password for access to the instance, instead of changing the password from the Management Service, connectivity from the Management Service to the instance is lost. With this release, you can restore connectivity by creating a new profile from the Management Service, assigning it the same password that you specified on the NetScaler VPX instance, and then binding the new profile to the NetScaler VPX instance.

  To create a new administrator profile, log on to the Management Service and, on the Configuration tab, navigate to NetScaler > Admin Profiles. In the details pane, click Add. In the Create NetScaler Admin Profile dialog box, type the new profile name and password. Then navigate to NetScaler > Instances and select the instance to which you want to bind the new profile. Click Modify to open the Modify NetScaler wizard and, from the Admin Profile list, select the new profile. You do not need to restart the instance for this change to take effect.

  You can also lose connectivity to XenServer by changing the password on XenServer instead of from the Management Service. To restore connectivity, you can now change the password for XenServer from the Management Service.

  To change the password, log on to the Management Service and, on the Configuration tab, navigate to System > Users. Select the nsroot user, and then click Modify. In the Modify System User dialog box, type the same password that you specified when you were logged directly on to XenServer.

- Issue ID 0329597: In certain cases, the status of a storage disk present in the SDX appliance might appear as "Missing" in the Management Service User interface under Monitoring > System Health > Storage > Disk node.

- Issue ID 0336831: If you bind a new interface to a NetScaler instance, the physical to virtual interface mapping does not change. However, if you modify a NetScaler instance that involves disabling a virtual interface, the physical interface to virtual interface mapping on the instance might change.

Networking

- Issue ID 0342151: The set l4 parameter command has a new parameter,l2connMethod, for specifying the MAC address, channel number, and VLAN ID attributes for the L2 Conn option behavior in a virtual server.

  For a load balancing virtual server with L2 Conn enabled and l2connMethod parameter of the set l4 parameter command is set to Channel or Vlan or VlanChannel, a client MAC address change no longer causes the NetScaler appliance to create a new session entry. Instead, the appliance updates the existing session entry with the new MAC address. This update resolves issues (especially with MBF) that were caused by the appliance using the old session entry instead of the new one.

- Issue IDs 0343485 and 0358382: The NetScaler appliance becomes unresponsive when highly demanding traffic (~5000 HTTP threads at a request rate of 100 KB/s) is sent through GRE and IPsec tunnels.

- Issue ID 0343789: In an High Availability configuration, BGP peer of the secondary node stays in open sent state.

- Issue ID 0346654: The NetScaler appliance does not ignore some unsupported capabilities. It might reset BGP connections even when strict-capability-match is not configured on the appliance.

NITRO API

- Issue ID 93372/0257279: You can now view the virtual servers to which a specified service is bound. The REST URL for this is `http//<nsip>/nitro/v1/config/svcbindings/svcname`.

- Issue ID 0318912: On the NetScaler appliance versions 9.2, 9.3, and 10, incorrect values are returned for cpuusagepcnt and rescpuusagepcnt on the following query: /nitro/v1/stat/system.

SSL

- Issue ID 0342706: If you bind a cipher or cipher group to a virtual server, service group, or service, and then save the configuration, the cipher group binding is missing from the configuration after you restart the appliance.

- Issue ID 0344323: An attempt to add a CA certificate fails if the modulus value of the public key is not a multiple of 512 bits.

- Issue IDs 0352611, 0357697, and 0358026: If you log on to a NetScaler account other than the administrative account and enter the show ssl service command or show running config command, the command output appears repeatedly.

- Issue ID 0353680: The add ssl certkey command fails if the private key file does not have a newline at the end of the file.

- Issue ID 0357528: On a FIPS platform, if an SSL renegotiation request is received on an SSL virtual server, the appliance fails.

System

- Issue ID 0301065: When using the HTTP monitor, the NetScaler appliance might send SYN packets from a port on which an earlier session was not closed by the server. The server then responds with a bad syn ack response, which causes the NetScaler appliance to send a RST to the server.
- Issue ID 0334500: High disk usage as the newnslog log files of NetScaler appliance version 9.2 are not automatically cleaned up on upgrade to NetScaler appliance version 9.3.
- Issue ID 0335155: When USIP is enabled, the Netscaler appliance sends a probe to the server using the client IP address as the source IP address. If the server responds to the probe with a packet having incorrect acknowledgement number, the appliance tries to probe the server again using MIP address instead of client IP address.
- Issue IDs 0355812 and 0357937: If you log on to a NetScaler appliance using an account other than the administrative account, when you execute the show monitor command, not all monitors are displayed.

Web Interface

- Issue ID 0353708: If you modify a web interface services site (for access via Citrix receiver) using the configuration utility, on a NetScaler version 10 appliance running a build older than 72.6, the services site might stop working.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0283556: Currently the SAML implementation supports only RSA digital signatures. DSA digital signatures are not supported.
- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberoes authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, and then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.
- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

Action Analytics/Rate Limiting

- Issue ID 91353/0250526: If multiple stream identifiers and/or rate limiting identifiers evaluate a connection, the NetScaler appliance updates the counters for bandwidth, response time, and number of concurrent connections for only the identifier that evaluates the connection first. Those statistical counters are not updated for the other identifiers. However, the counter for number of requests is updated for all the identifiers that evaluate the connection.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

AppFlow

- Issue ID 0327439: AppFlow records generated by the NetScaler appliances cannot be seen on SPLUNK.
- Issue ID 0333560 (nCore): AppFlow records generated by the NetScaler appliance might contain junk characters.

Application Firewall

- Issue ID 0272715: If you use the Google Chrome browser with the default Chrome PDF plugin to view the PCI-DSS report, certain links and pages do not render correctly. To work around this issue, disable Chrome PDF and install the Adobe Acrobat Reader plugin for Chrome.

- Issue ID 0282932: If you use the Signature Editor to add a signature rule for a response-side check (such as the Credit Card or Safe Object check), in addition to one or more response patterns you must also add at least one request pattern. If you do not, then when you try to save the new signature rule, the configuration utility displays an error message and does not save the rule.

- Issue ID 0283780: When you enable the sessionless URL closure feature, you must also enable the URL closure feature. If you do not enable URL closure, the sessionless URL closure feature does not work.

- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked. To work around this issue, if you configure Sessionless URL Closure, set Validate Referer Header to Off.

- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported for importing as application firewall signature rules. WAS 2.0 scan reports are not supported.

- Issue ID 0303060: Application firewall statistics are not supported for NetScaler classic policies. If you need to see numbers of policy hits and other statistics, you must use NetScaler default syntax policies.

- Issue ID 0313950: On a NetScaler appliance that has the application firewall configured and the Safe Object check configured, processing extremely large web pages can cause the NetScaler appliance to crash.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click 'Application Firewall' in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0303279: In the configuration utility, in the Rewrite Policies pane, clicking Add does not display the Create Rewrite Policy dialog box but disables the main configuration utility window.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0333048: If you access the configuration utility through Internet Explorer 8, an attempt to bind 250 or more VIP addresses to a VLAN results in an error message about an unresponsive script.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

  Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0334042: The configuration utility does not display a details panel for all the entities.

Workaround: Click 'Edit' to display the details.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the Create DNS View dialog box, the "Service(s) in this view" and "Policy(s) in this view" lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs.

  Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0338513: When you log on to NetScaler configuration utility using Internet Explorer 8 or Internet Explorer 9, the web browser displays a blank screen as the browser is displaying the compatibility view.

  Workaround: Change to the standard view, in the Compatibility View Settings dialog box, by clearing the Display all websites in Compatibility View check box.

- Issue ID 0349813: If you use the configuration utility to unbind all the cipher suites from a user-defined SSL cipher group, the user-defined cipher group is deleted from the appliance.

- Issue ID 0352307: If you access the NetScaler configuration utility from a Mac machine with a client environment running JRE 1.7 or later, you cannot select the fields in the Java based configuration views.

  Workaround: If you click outside and return to the browser window, you will be able to select the fields in the configuration views.

- Issue ID 0353015: Load balancing virtual servers that are used by AppExpert applications are displayed in nodes other than the AppExpert node. For example, they are displayed in the Available Virtual Servers list (Load Balancing > Persistency Groups > Add > Create Persistency Group dialog box), and in the Target LB Virtual Server list (Content Switching > Actions > Add > Create Content Switching Action dialog box > Name option button).

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated.

Domain Name System

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If a GSLB virtual server's primary GSLB method is set to round trip time (RTT) and backup GSLB method is set to static proximity, or if the primary GSLB method is set to static proximity and backup GSLB method is set to RTT, and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

Load Balancing

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the "show lb persistentSessions" CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 91711/0250846: If the string (or "token") that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR("string2").AFTER_STR("string1") if the string that is enclosed by "string1" and "string2" is not larger than 64 KB.

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

Load Balancing/SSL

- Issue ID 0331621: While creating SSL or load balancing virtual servers with default responder action, the NetScaler appliance throws a “No such resource” error. This issue is observed only in a cluster setup.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type: `#/etc/rc.d/svmd restart`

- Issue ID 0337386: When restored from a backup, a NetScaler instance is reprovisioned by using the NetScaler XVA image currently available on the appliance, even if the backup was taken from an upgraded configuration. If multiple XVA images are available, the XVA image that was used to originally provision the instance is used, if available, to reprovision the instance. If that image is not available, any XVA image is used.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.
- Issue IDs 0283035 and 0299716: In a cluster setup, the bind vlan command throws an error when interface and IP address are specified together.
- Issue ID 0288450: The show lacp command does not display the lacp configurations. This issue is observed only in a cluster setup.
- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command set ptp -state disable and configure NTP to synchronize the time across the cluster nodes.
  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator, and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed.

  Workaround: Copy the certkey under /nsconfig/ssl/ folder on all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.
- Issue ID 0343395: On the NetScaler appliance, TLS protocol version 1.2 does not support a client certificate with RSA 4096-bit key.
- Issue ID 0345883: On the NetScaler appliance, TLS protocol version 1.2 does not support ephemeral Diffie-Hellman cipher suites.
- Issue ID 0352334: TLS protocol, version 1.2, handshake fails if all the following conditions are met:
  - The Client browser is Internet Explorer.
  - Client authentication is set to mandatory on the virtual server.
  - The configured client certificate on IE browser is not signed by SHA256 hash algorithm.

XML API

- Issue ID 0321005: The API to set the hostname for a NetScaler appliance is changed to include the owner node parameter for a cluster node.

Build 72.5

Release version: Citrix® NetScaler®, version 10 build 72.5

Replaces build: None

Release date: November 2012

Release notes version: 5.0

Language supported: English (US)

Review the following sections:

- Changes
- Bug Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler and Citrix Access Gateway.

Changes

Configuration Utility

- Issue ID 0317403: On the Monitoring tab, when you disable a virtual server or a service, a confirmation window is displayed to confirm the disable operation.

Content Switching

- Issue ID 0248750: In this release, for a content switching policy that uses a default syntax rule, you can specify the target load balancing virtual server in a content switching action. In the content switching action, you can specify the name of the target load balancing virtual server, or you can configure a request-based expression that, at run time, computes the name of the load balancing virtual server to which to send the request. The expression option can drastically reduce the size of your content switching configuration, because you need only one policy per content switching virtual server. Content switching policies that use an action can also be bound to multiple content switching virtual servers, because the target load balancing virtual server is no longer specified in the content switching policy. The ability to bind a single policy to multiple content switching virtual servers helps to further reduce the size of your content switching configuration.

  You can also, for a content switching policy that uses a default syntax rule, specify the target load balancing virtual server when binding the policy to a content switching virtual server, as you would in earlier releases, without the need for a separate action. For domain-based and URL-based policies, an action is not available, and you continue to specify the name of the target load balancing virtual server when binding the policy to a content switching virtual server.

  For more information, see http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-map/ns-cs-basicconfig-config-cs-action-con.html.

Load Balancing

- Issue ID 0345300: If a UDP connection that is being managed by a load balancing virtual server of type UDP, SIP_UDP , DNS, RADIUS , or ANY is blocked pending a decision on persistence, and the associated protocol control block is freed before all the NetScaler buffers that reference the protocol control block are processed, the appliance might fail.

SSL

- Issue ID 0236585: You can now load a certificate bundle containing one server certificate, up to nine intermediate certificates, and optionally, a server key. Separate steps for loading and linking the certificates are no longer required.

- Issue ID 0338862: If you unbind all the cipher suites from a user-defined cipher group by using the command line, the user-defined cipher group is not deleted from the appliance.

Bug Fixes

AAA Application Traffic

- Issue IDs 0272417 and 0344661: SSO using 401-based authentication fails when an initial user request is redirected to another URL.
- Issue ID 0345220: If a AAA virtual server is configured for two-factor authentication with RADIUS challenge/response in a single-signon (SSO) environment, with the SSO name extracted from the primary authentication service and the second factor from RADIUS challenge/response, the wrong user name might be extracted. This can result in intermittent authentication failures.

Access Gateway

- Issue ID 0330636: When users log on with the Access Gateway Plug-in to an nCore Access Gateway appliance, occasionally when server-initiated connections occur, depending on the core through which the traffic is passed, the user device may fail.
- Issue IDs 0332483 and 0336091: If you have a VLAN configuration on the NetScaler appliance, when users log on with the Access Gateway Plug-in, occasionally server-initiated connections to the user device fail.
- Issue ID 0337609: When you integrate Access Gateway with a SharePoint site, after users log on successfully, when they open a Microsoft Office document, the session ends and the logon page appears.
- Issue IDs 0340122 and 0337613: After users upgrade to Access Gateway 10, Build 70.7, if you have a high availability configuration that includes an FTP server, when users log on with the Access Gateway Plug-in and initiate an FTP session, occasionally Access Gateway fails on both primary and secondary appliances while the FTP connection is active.
- Issue ID 0348694: If a published application is configured to require a user name with both capital and lower-case letters and is configured for single sign-on, after users log on with the Access Gateway Plug-in with the same user name, when they open a published desktop from the Web Interface and try to open the published application, they are prompted to enter their credentials again.
- Issue ID 0349178: After users log on to the StoreFront-based store remotely over Access Gateway from a browser and then select Log out under the users' name on the page, a page appears with message "Logoff is successful" and includes a Log on button. If users click Log on, the Storefront store-based web page is available again and authentication is not required.

AppFlow

- Issue ID 0344666: When the appflow policy evaluation fails, the NetScaler appliance sometimes continues to attempt “Appflow Logging” because of which it fails.

Application Firewall

- Issue ID 0346118: If sessionless form field consistency is enabled, a memory leak can cause fill up on the NetScaler appliance’s memory.
- Issue ID 0346384: If the Start URL feature is configured to use an uploaded HTML error object instead of an error URL, the start URL feature cannot block access to "/" even if you exclude "/" from the start URLs list.

CloudBridge

- Issue ID 0325718 (nCore): The amount of memory allocated to a packet engine can be retrieved by using show ns stat command (value of InUseMemory) or by SNMP polling (value of resMemUsage). There was a mismatch in InUseMemory and resMemUsage value for the same packet engine due to difference method used to calculate the allocated memory. This mismatch problem is now resolved and both the methods return the correct value.

Cluster

- Issue ID 0343514: The cluster instance view in the configuration utility does not display which node is the configuration coordinator.

Configuration Utility

- Issue ID 0329547 (nCore): In some cases, the value to which you set the prefetchPeriodMilliSec parameter for a cache content group might not be saved in the nsconfig file.
- Issue ID 0332839: If you access the configuration utility through Internet Explorer 8, the System > Settings > Configure TCP Parameters, dialog box has no spaces between field names and fields.
- Issue ID 0334292: If you navigate to HTTP Compression > Policies or HTTP Compression > Actions, the 'Remove' button is disabled in the task pane.

  Note: You can access the command line interface from the configuration utility. Navigate to System > Diagnostics > Command Line interface.
- Issue ID 0335701: You cannot add an SSL service with the Clear Text Port option in the configuration utility, because the option is disabled.
- Issue ID 0336854: When you open a log file in Syslog messages viewer, all the logs are not displayed when the uncompressed log file size is more than 10MB.
- Issue ID 0342735: Users might not be able to enable or disable NTP synchronization by using the configuration utility.
- Issue ID 0345828: When you log on to the NetScaler configuration utility by using certain versions of Internet Explorer 8, the web browser does not load the configuration utility.
- Issue ID 0346060: When you access the NetScaler configuration utility from a client environment using JRE 7, in certain configurations, the NetScaler configuration utility displays "Operation in Progress" message when you open a load balancing virtual server configuration.

Content Switching

- Issue ID 0315161: A NetScaler appliance fails under the following sequence of events:

  1. You associate an HTTP load balancing virtual server with an HTTP profile and a backup load balancing virtual server of type TCP.
  2. You configure a content switching virtual server to switch requests on the basis of content switching policies, and you set the load balancing virtual server as a target for the content switching virtual server.
  3. The HTTP load balancing virtual server goes down.
  4. When the content switching virtual server receives a request, it happens to select the load balancing virtual server.
  5. Because the HTTP virtual server is down, the content switching virtual server selects the backup load balancing virtual server, which is of type TCP.
  6. The appliance attempts to access the HTTP profile, which cannot be associated with a load balancing virtual server of type TCP.
- Issue ID 0344944: When you remove a content switching virtual server, the NetScaler appliance fails to remove some or all of the configuration information that binds load balancing virtual servers to the content switching virtual server. Consequently, if the state of a load balancing virtual server changes, the appliance attempts to update the state of the content switching virtual server, which no longer exists. When attempting such a state update, the appliance fails.

Domain Name System

- Issue IDs 0330529 and 0322151: The following message might be displayed if you disable a virtual server-based DNS name server: 'ERROR: Name server does not exist. [nsnet_recvrpcioctl]'

Global Server Load Balancing

- Issue ID 0308555: In certain scenarios, if the primary and backup GSLB methods are static proximity and dynamic RTT, respectively, requests for domain name resolution are not processed correctly. As a result, the appliance can fail.

Integrated Caching

- Issue ID 0331520: After an upgrade to 10.0, the NetScaler appliance might occasionally fail because of internal memory handling issues.

Load Balancing

- Issue ID 0333200: If rule based persistence is configured for a load balancing virtual server, and the virtual server receives traffic from a content switching virtual server, the load balancing virtual server's persistence sessions expire at the end of the configured timeout period, even if new requests arrive before session expiry.

Load Balancing/AAA Application Traffic

- Issue ID 0346093: The traffic management policy hit count shows no hits ("0"), even when traffic management policies are functioning and matching traffic.

Monitoring

- Issue ID 0339736: The NetScaler appliance might fail when generating the SNMP trap described in the following scenario:
  - You set the response timeout threshold parameter for a monitor that is bound to a domain based service.
  - You configure the MONITOR-RTO-THRESHOLD SNMP alarm on the NetScaler appliance.
  - The response timeout threshold is exceeded by a domain based service, and the appliance attempts to generate the monRespTimeoutAboveThresh trap.

Networking

- Issue ID 0334312: During a warm restart of the NetScaler appliance, a daemon might fail to start. After not receiving heartbeats from the daemon, the Pitboss process restarts the appliance.
- Issue ID 0336136: If a NetScaler appliance acting as a DHCP relay agent receives DHCP Discover traffic that is not from a Layer 3 VLAN, the appliance might disconnect from the default gateway and remain disconnected for some time.
- Issue ID 0336886: When a VIP with OSPF LSA TYPE-1 exists on the NetScaler appliance, any new VIPs configured with TYPE-5 are saved as TYPE-1.
- Issue ID 0341895: The state of the IPSEC tunnel becomes DOWN and SA reformation/rekeying does not happen after the IKE lifetime expires.
- Issue ID 0343578: The NetScaler appliance drops an ARP request if it arrives on a VLAN to which two different subnets are bound and the source IP address and the destination IP address in the ARP request packet belongs to these different subnets bound to the VLAN.

Policies

- Issue ID 0291487: NetScaler appliances running version 9.2 build 52.1 or later and have a large number (in the hundreds) of policy bindings can experience performance issues on 'save ns config' and 'show config' operations. This can lead to interruption in services.
- Issue IDs 0332600 and 0335877: The running configuration does not show the command used to bind a policy to a load balancing virtual server, in the following scenarios:
  - When a policy is globally bound.
  - When a service is bound to same load balancing virtual server.

SSL

- Issue ID 0302532: The NetScaler appliance fails if all of the following conditions are met:
  - A certificate revocation list (CRL) is present and linked with a CA certificate, and the CA certificate is continuously updated.
  - The CRL is uploaded by using HTTP, and auto refresh is enabled on the CRL.
  - Client authentication is enabled. Therefore, the client is verified for every GET request.

System

- Issue ID 0241964: The SNMP engine ID does not get saved to the ns.conf file after the configurations are saved. Hence the engine ID is not retained across reboots. Also, the default SNMP engine ID is not displayed on issuing the 'show snmp engineid' command.
- Issue ID 0306237: If the number of dynamic services running on the NetScaler appliance exceeds 64k, any service created could not be accessed even after when the number of services is less than 64k.
- Issue ID 0334585: The NetScaler appliance runs out of memory when processing the traffic management logout URL.

Web Interface

- Issue ID 0341459: An invalid argument error is thrown when you try to create a web interface site with default access method selected as 'GatewayDirect' and authentication point selected as 'Web Interface'.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0283556: Currently, the SAML implementation supports only RSA digital signatures. DSA digital signatures are not supported.
- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberoes authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, and then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.
- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

Access Gateway

- Issue ID 92543/0251596: After you configure Access Gateway to provide user connections through Citrix Receiver, when users right-click the Receiver icon in the notification area, the Log on option does not appear. Users must connect by using the Web browser or they must right-click the Receiver icon and then, depending on the version of Receiver they are using, click About or Preferences from the Receiver menu and Plug-in Status or Advanced from the Receiver panel. You can also enable the log on option to appear when users right-click the Receiver icon by adding the following settings in the registry:
  - Add the Receiver key (if the key does not already exist) under the following registry locations:
    - `HKEY_CURRENT_USER\Software\Citrix\`
    - `HKEY_LOCAL_MACHINE\Software\Citrix\`
  - Add the Inventory key in the following registry locations:
    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`
    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`
  - In the Inventory key, configure the following **REG_SZ** values:
    - **VPNAddress**. Provide the value as the Web address for the Access Gateway appliance; for example, https://<AccessGatewayFQDN>.
    - **VPNPrompt1**. Provide the value as 'UserName'.
    - **VPNPrompt2**. Provide the value as '*Password'.

      Note: To mask the password, enter an asterisk (*) before the word.

      In addition, if you configure double-source authentication that requires authentication with LDAP plus RSA authentication, you need to also add the following as **REG_SZ**:
    - **VPNPrompt3**. Provide the value as '*Passcode'.
- Issue ID 0261547: When you enable Access Gateway as a reverse proxy and you enable basic preauthentication and post- authentication scans, as well as encryption and client choices, when users log on with the Access Gateway Plug-in, the preauthentication scan passes, but the post-authentication scan fails.
- Issue ID 0275079: When users access applications published on XenApp, each user consumes multiple Access Gateway licenses per application. Instead, one session ID should be shared across the applications the user accesses. As a result, users exceed their allocated license count and an SSL error occurs.
- Issue ID 0278218: If you configure an endpoint policy, the preauthentication policy runs as expected. When users try to log on with the Access Gateway Plug-in, however, occasionally the post-authentication policy does not work as expected and authentication fails.
- Issue ID 0285995: If you configure Access Gateway to assign an intranet IP address to user devices that connect to Access Gateway, when users log on with the Access

Gateway Plug-in, the secure DNS dynamic update does not occur and the intranet IP address is not registered with the DNS Server.

- Issue ID 0288469: After you configure a virtual server to use the Access Gateway Plug-in for Java, when users log on with the Access Gateway Plug-in by using a browser that has a 64-bit Java Runtime Environment (JRE) installed, the plug-in fails to establish a connection.

- Issue ID 0291264: If you create a Web Interface 5.4 site and enable authentication through Access Gateway, and you enable single sign-on with a smart card to the Web Interface that enables smart card pass-through, when users log on with the Access Gateway Plug-in, the users' desktops are not listed on the Web Interface.

- Issue ID 0291821: If you create a Web Interface 5.4 site and enable authentication with a smart card through Access Gateway, and you configure the 'Single Sign-on Domain' on the 'Published Applications' tab using the format domainname.com instead of domainname, when users start a published application or desktop, authentication fails.

- Issue ID 0292005: When users connect with clientless access and try to download a file larger than 1 gigabyte (GB) from the file share on the home page, as the file is downloading, if an upload is attempted, the download process fails but the upload continues.

- Issue ID 0298971: When users log on with the Access Gateway Plug-in for Java and the Web Interface opens in Internet Explorer 9, if users do not turn on Compatibility View in Internet Explorer, when they click a published application, the following error appears: Resource shortcuts are not available.

- Issue ID 0299515: If you configure an intranet IP address on Access Gateway, when users connect with the Access Gateway Plug-in on a computer running Windows XP Service Pack 3 and try to access a CIFS share hosted on a computer in the secure network, users receive an error that the share is inaccessible.

- Issue ID 0300511: When users log on using clientless access and click a bookmark from the home page to open a Distributed File Share (DFS), if the target folder resides on a different computer than the computer where the domain DFS server resides, the share does not open.

- Issue ID 0309017: When you configure a preauthentication and post-authentication policy with an expression to scan a user device for a file, Access Gateway does not check for expression syntax. As a result, Access Gateway accepts inappropriate syntax configuration and the scan fails.

- Issue ID 0327433: If you configure a virtual server by using the Remote Access wizard and configure a Secure Ticket Authority (STA), the status of the server appears as UP. However, in the configuration utility, on the Home tab, under Alerts, a message states that the STA server is not configured. You must bind the server globally in order to clear the message.

- Issue ID 0337886: If users select Automatically detect settings in Internet Explorer on a computer running Windows XP, when users log on with the Access Gateway Plug-in and then log off from Access Gateway, the Automatically detect settings check box is not restored to the previously configured setting.

- Issue ID 0338451: If hundreds of concurrent sessions occur, the generation of a support file takes several hours.

- Issue ID 0340346: If you configure a session time-out setting, after users connect to Access Gateway, even though the session expires according to the value you enter, the actual process of closing the session takes longer.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

AppFlow

- Issue ID 0327439: AppFlow records generated by the NetScaler appliances cannot be seen on SPLUNK.
- Issue ID 0333560 (nCore): AppFlow records generated by the NetScaler appliance might contain junk characters.

Application Firewall

- Issue ID 0272715: If you use the Google Chrome browser with the default Chrome PDF plugin to view the PCI-DSS report, certain links and pages do not render correctly.

  Workaround: Disable Chrome PDF and install the Adobe Acrobat Reader plugin for Chrome.
- Issue ID 0282932: If you use the Signature Editor to add a signature rule for a response-side check (such as the Credit Card or Safe Object check), in addition to one or more response patterns you must also add at least one request pattern. If you do not, then when you try to save the new signature rule, the configuration utility displays an error message and does not save the rule.
- Issue ID 0283780: If you enable the sessionless URL closure feature, you must also enable the URL closure feature. If you do not, the sessionless URL closure feature does not work.
- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked. To work around this issue, if you configure Sessionless URL Closure, set Validate Referer Header to Off.
- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported for importing as application firewall signature rules. WAS 2.0 scan reports are not supported.
- Issue ID 0303060: Application firewall statistics are not supported for NetScaler classic policies. If you need to see numbers of policy hits and other statistics, you must use NetScaler default syntax policies.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

Cluster

- Issue ID 0343137: The configuration utility does not display the "Add" button while configuring linksets.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click 'Application Firewall' in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0303279: In the configuration utility, in the Rewrite Policies pane, clicking Add does not display the Create Rewrite Policy dialog box but disables the main configuration utility window.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0324797: The NetScaler configuration utility does not display the queue depth value for the configured priority queuing policies. This issue is observed only in a cluster setup.

  Workaround: You can view the queue depth of the policy by using the 'show pq policy' command on the command line interface.

- Issue ID 0333048: Using the Configuration Utility in Internet Explorer version 8, when you attempt to bind 250 or more VIP addresses to a VLAN, the Configuration Utility displays an unresponsive script error.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

  Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0334042: The configuration utility does not display a details panel for all the entities.

  Workaround: Click 'Edit' to display the details.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the 'Create DNS View' dialog box, the 'Service(s) in this view' and 'Policy(s) in this view' lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs.

  Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0338513: When you log on to NetScaler configuration utility using Internet Explorer 8 or Internet Explorer 9, the web browser displays a blank screen as the browser is displaying the compatibility view.

  Workaround: Change to the standard view, in the Compatibility View Settings dialog box, by clearing the Display all websites in Compatibility View check box.

- Issue ID 0349813: If you use the configuration utility to unbind all the cipher suites from a user-defined SSL cipher group, the user-defined cipher group is deleted from the appliance.

- Issue ID 0352307: If you access the NetScaler configuration utility from a Mac machine with a client environment running JRE 1.7 or later, you cannot select the fields in the Java based configuration views.

  Workaround: If you click outside and return to the browser window, you will be able to select the fields in the configuration views.

- Issue ID 0353015: Load balancing virtual servers that are used by AppExpert applications are displayed in nodes other than the AppExpert node. For example, they are displayed in the Available Virtual Servers list (Load Balancing > Persistency Groups > Add > Create Persistency Group dialog box), and in the Target LB Virtual Server list (Content Switching > Actions > Add > Create Content Switching Action dialog box > Name option button).

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated.

Domain Name System

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If a GSLB virtual server’s primary GSLB method is set to round trip time (RTT) and backup GSLB method is set to static proximity, or if the primary GSLB method is set to static proximity and backup GSLB method is set to RTT, and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

Load Balancing

- Issue ID 0278377 (nCore): Cache policy labels cannot be bound to MYSQL or MSSQL virtual servers.
- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the 'show lb persistentSessions' CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.
- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).
- Issue ID 91711/0250846: If the string (or 'token') that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR('string2').AFTER_STR('string1') if the string that is enclosed by 'string1' and 'string2' is not larger than 64 KB.
- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.
- Issue ID 0278377 (nCore): Cache policy labels cannot be bound to MYSQL or MSSQL virtual servers.
- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

Load Balancing/SSL

- Issue ID 0331621: While creating SSL or load balancing virtual servers with default responder action, the NetScaler appliance throws a 'No such resource' error. This issue is observed only in a cluster setup.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type : #/etc/rc.d/svmd restart

- Issue ID 0337386: When restored from a backup, a NetScaler instance reverts to the release and build in which it was originally provisioned, even if the backup was taken from an upgraded configuration.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.

- Issue IDs 0283035 and 0299716: In a cluster setup, the 'bind vlan' command throws an error when interface and IP address are specified together.

- Issue ID 0288450: The 'show lacp' command does not display the lacp configurations. This issue is observed only in a cluster setup.

- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command 'set ptp -state disable' and configure NTP to synchronize the time across the cluster nodes.

  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator, and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed.

  Workaround: Copy the certkey under /nsconfig/ssl/ folder on all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.
- Issue ID 0343395: On the NetScaler appliance, TLS protocol version 1.2 does not support a client certificate with RSA 4096-bit key.
- Issue ID 0345883: On the NetScaler appliance, TLS protocol version 1.2 does not support ephemeral Diffie-Hellman cipher suites.
- Issue ID 0352334: TLS protocol, version 1.2, handshake fails if all the following conditions are met:
  - The Client browser is Internet Explorer.
  - Client authentication is set to mandatory on the virtual server.
  - The configured client certificate on IE browser is not signed by SHA256 hash algorithm.

XML API

- Issue ID 0321005: The API to set the hostname for a NetScaler appliance is changed to include the owner node parameter for a cluster node.

Build 71.6

Release version: Citrix® NetScaler® release 10 build 71.6

Replaces build: None

Release date: October 2012

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Changes
- Bug Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler and Citrix Access Gateway.

Changes

Configuration Utility

- Issue ID 0319070: The Setup wizard is not launched automatically if a mapped IP (MIP) address or a Subnet IP (SNIP) address is not configured on the NetScaler appliance.

NetScaler SDX Appliance

- Issue ID 0332251: You can now configure LACP from within a NetScaler VPX instance hosted on a NetScaler SDX appliance. Make sure that the interfaces that are part of the channel are not shared with other instances, and a dedicated channel is configured for an instance. For more information, see Configuring LACP on a NetScaler VPX Instance.

Bug Fixes

AAA Application Traffic

- Issue ID 0319434: If 401 basic authentication is enabled on a load balancing virtual server, and authentication fails either due to invalid credentials or a Kerberos authentication failure, the NetScaler packet engine might crash.

Access Gateway

- Issue ID 82828/0243556: You can configure a forced time-out to disconnect the Access Gateway Plug-in automatically with a value (in minutes) that exceeds 255. You can now enter a value as high as 3,000 (in minutes, which is equivalent to 50 hours).
- Issue ID 0331288: When split tunneling is OFF, when users try to connect with an Access Gateway Plug-in, occasionally host routes added by the plug-in may block communication between the Internet IP address and the Domain Name Server. Users may experience network connectivity issues, such as the inability to access file shares on the network.
- Issue ID 0329113: When you configure Intranet IP addresses on Access Gateway and bind the addresses to a virtual server, the bound IPs addresses do not appear in the configuration utility.
- Issue ID 0329603: When you enable a preauthentication scan, and you enable the user device to connect through a proxy server, when users log on with the Access Gateway Plug-in for the Mac OX X Version 2.1.3, Access Gateway fails.
- Issue ID 0336499: When users log on to Access Gateway by using Citrix Receiver and then log off by using the Receiver icon in the taskbar, the computer loses network access. To restore network access, users must either disable and then enable their network interface or restart their computer. To avoid the issue, users can log off from the Access Interface home page.
- Issue ID 0338220: If you configure client certificate-based expressions for preauthentication or post-authentication scans, when users try log on to Access Gateway, occasionally, the scan fails. To avoid the issue, you can use the classic or MPX 5500 platforms or you can bind the certificate-based policy globally to a virtual server.

Application Firewall

- Issue ID 0329401: On a NetScaler appliance that has the Application Firewall enabled and both cookie transformation and encryption on, secure memory usage increases slowly and continuously until the NetScaler appliance starts to drop connections.
- Issue ID 0332176: On a NetScaler appliance that has the application firewall enabled, user logons can be extremely slow. The cause is that a back-end server does not set a Content-Length header that the NetScaler expects. As a result the NetScaler appliance does not close the connection with the user's browser. To work around this issue, you can do one of the following:
  - Add a rewrite policy to the configuration that appends a content-length header of zero ('Content-Length: 0') to the logon page.
  - Disable the application firewall.
- Issue ID 0333332: When signatures that work on post body are enabled, a large post request may cause an HA failover.
- Issue ID 0335102: On a NetScaler appliance that has the application firewall enabled, adding a large number of signatures objects can cause high CPU loads.

CloudBridge

- Issue ID 0313629: When the time on a NetScaler is modified, either due to Network Time Protocol Daemon (NTPD) or other external factors to the time lesser than the boot time, the iked process may start consuming 100% of CPU resources.
- Issue ID 0334949: If you use configuration utility to remove an IPv4 tunnel for CloudBridge from a NetScaler appliance, the remove process succeeds but the following Java exception is displayed 'ClassNotFoundException'.

Cluster

- Issue ID 0332594: The RIP (Routing Information Protocol) and Cache Redirection features cannot be enabled in a NetScaler cluster setup.

Configuration Utility

- Issue ID 93754/0257608: When you view the configuration difference between files, the corrective commands generated for bind or unbind commands of load balancing and content switching virtual servers might not be accurate in some cases.
- Issue ID 0305248: In the Reporting tool, when users try to generate a 'system entities statistics' report for load balancing virtual servers, the load balancing virtual servers configured on the appliance might be displayed as being inactive. Users cannot choose the virtual server to view the statistics.
- Issue ID 0310203: In the Reporting tool, when users try to generate a custom report for load balancing virtual servers, the virtual servers might be displayed as being inactive. Users cannot choose the virtual server to view the statistics.
- Issue ID 0333577: When configuring the Transformation URL Profile, an error occurs if you set Priority to a value higher than 2147483647 (maximum allowed value).
- Issue ID 0333836: If you have configured global server load balancing by using the GSLB wizard, Wizard for Citrix XenApp, or Wizard for Citrix XenDesktop, and you attempt to view the GSLB Visualizer, Prefuse information might be logged to the Java console. However, you can view the GSLB Visualizer, and the functionality is not affected.
- Issue ID 0334280: After you rename a compression policy, the new name might not be reflected in the configuration utility.
- Issue ID 0334284 If you navigate to HTTP Compression > Policies and click Policy Manager in the task pane, the following error message might appear: No such policy exists.
- Issue ID 0334773: In the Synchronize 'GSLB Configuration' dialog box, the Command parameter is unavailable when the 'Synchronization Option' parameter is set to its default value (automatic synchronization).
- Issue ID 0335008: The exception 'netscape.javascript.JSException' is logged to the Java console when you create a DNS key by using the NetScaler configuration utility. However, the DNS key is created, and there is no loss in functionality.
- Issue ID 0335235: The NetScaler configuration utility does not show globally bound AppFlow policies in the policy manager. This issue is observed only in a cluster setup.
- Issue ID 0335701: You cannot add an SSL service with the Clear Text Port option in the configuration utility, because the option is disabled.
- Issue ID 0335719: The exception 'netscape.javascript.JSException' is logged to the Java console when you sign a DNS zone by using the NetScaler configuration utility, and the browser’s status bar does not report the status of the zone-signing operation. However, the zone is signed, and there is no loss in functionality.
- Issue ID 0335913: In a cluster setup, you cannot enable a server entry that is disabled, because the 'Enable' button is unavailable. However, you can disable a server entry by using the NetScaler command line interface.

Domain Name System

- Issue IDs 0268748 and 0333310: In a cluster setup, if you save the configuration and reboot an appliance, the default name-server records for the thirteen root servers, and their associated address records, become unavailable. If you need them, you have to add them manually after you perform a reboot.
- Issue ID 0318199: If core memory is not available when the NetScaler appliance is processing an RRSIG record received in a response, the appliance fails.
- Issue ID 0319100: Default DNS actions, policies, and policy bindings are not displayed in a cluster setup.

Integrated Caching

- Issue ID 0334895: On a NetScaler appliance configured with five policy engines, responses might not be cached even if memory is available for caching.
- Issue ID 0337446: When a byte-range request sent to integrated cache is larger than the size of cached object and the if-range header is also set, the NetScaler appliance fails.

Load Balancing

- Issue ID 0314738: If you issue the 'force HA sync -force' command when HA synchronization is disabled on both nodes, the services on the secondary node are marked as DOWN. The services remain in that state until after a failover. When a failover occurs, the failover of some services might be delayed by a few seconds while monitors learn the actual states of those services. Until the monitors learn and correct the states, new connections to those services might be rejected. Consequently, you might also observe a brief period of outage following a failover.
- Issue ID 0318310: While creating a load balancing monitor, you cannot specify a send string that has a length of more than 76 characters. This issue is observed only in a cluster setup.
- Issue ID 0336400: In a two-node cluster that has been configured with a small number of services, if you restart a node or disable and reenable a node, the node might indefinitely remain in the service-state-synchronization stage.

NetScaler SDX Appliance

- Issue ID 0331900: If you try to upload a file larger than 300 MB to the NetScaler SDX appliance, the upload fails.
- Issue ID 0332313: 100 percent CPU usage is observed when the Management Service takes daily backup.
- Issue ID 0332819: If you try to create a high availability pair between two VPX instances without explicitly logging on to the second instance, an error message appears.
- Issue ID 0334340: If you upgrade the Management Service on which a NetScaler instance with a description of greater than 32 characters is provisioned, the instance is not migrated, and therefore, complete data related to the instance is not available in the database. Later, if you delete this instance and provision a new instance with the same IP address, the operation fails.
- Issue ID 0337090: A NetScaler VPX instance provisioned on an SDX appliance might fail if a warm restart is performed on the instance.

Networking

- Issue ID 0322026: In an L2 DSR configuration, packets arriving on the loop back interface are dropped even when the traffic rate on the interface is low.

Platform

- Issue ID 0321989: NetScaler release 10 build 71.x is supported on the new MPX 5550/5650 platforms.

Policies

- Issue ID 0291975: The SYS.VSERVER('<vserver_name>').THROUGHPUT expression returns an incorrect throughput value.
- Issue ID 0337576: The Netscaler might become unresponsive, if you used a request URL with encoding (for example, using %20) in an expression to the left of ALT, &&, or ||, and clauses to the right used strings. In addition, if the request URL was concatenated with another string, the final result would incorrectly contain a decoded URL, not the encoded one.
- Issue ID 0338916: Policies that are bound to policy labels are not available in the ns.conf file after saving the configurations. As a result, these bindings are lost after the appliance is rebooted.

SSL

- Issue ID 0257122: The close-notify parameter setting for an entity no longer has to be inherited from the global settings. You can set the close-notify parameter at the entity (virtual server, service, or service group) level. This enhancement provides the flexibility to set this parameter for one entity and unset it for another entity. However, make sure that you set this parameter at the global level. Otherwise, the setting at the entity level does not apply.
- Issue ID 0336920: On a cluster setup, replicating session entries across the nodes of the cluster is not supported.

System

- Issue ID 0277102: When you execute the 'show events' command, the NetScaler appliance might fail if the number of events to be displayed is more than 2^31.
- Issue ID 0333385: A hash collision might put the NetScaler aggregator into a recursive loop, causing the aggregator to fail. The NetScaler appliance might also fail, because of the aggregator failure.
- Issue ID 0336838: If HTML Injection and EdgeSight Monitoring are enabled on a NetScaler appliance and an HTTP request with a blank referer header is received, the appliance fails.
- Issue ID 0338244: The CallHome feature checks for compact flash drive and hard disk drive errors every six minutes instead of every six hours. If any errors are found, the appliance's data is uploaded to the Citrix Technical Support server.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberoes authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, and then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.

- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

- Issue ID 0327446: On an Outlook for Web Access (OWA) 2010 server that is protected by AAA-TM with single sign-on (SSO) enabled, when a user who uses the Firefox or Chrome browsers logs off, some OWA 2010 images do not appear.

- Issue ID 0334363: In the Citrix NetScaler configuration utility, when a user clicks the AAA-Application Traffic Wizard link, the configuration utility displays error message of 'Unknown Error'. The browser is then frozen til the session times out.

Access Gateway

- Issue ID 0340346: If you configure a session time-out setting, after users connect to Access Gateway, even though the session expires according to the value you enter, the actual process of closing the session takes longer.

- Issue ID 0278218: If you configure an endpoint policy, the preauthentication policy runs as expected. When users try to log on with the Access Gateway Plug-in, however, occasionally the post-authentication policy does not work as expected and authentication fails.

  - Issue ID 0327433: If you configure a virtual server by using the Remote Access wizard and configure a Secure Ticket Authority (STA), the status of the server appears as UP. However, in the configuration utility, on the Home tab, under Alerts, a message states that the STA server is not configured. You must bind the server globally in order to clear the message.
- Issue ID 0275079: When users access applications published on XenApp, each user consumes multiple Access Gateway licenses per application. Instead, one session ID should be shared across the applications the user accesses. As a result, users exceed their allocated license count and an SSL error occurs.

- Issue ID 92543/0251596: After you configure Access Gateway to provide user connections through Citrix Receiver, when users right-click the Receiver icon in the notification area, the Log on option does not appear. Users must connect by using the Web browser or they must right-click the Receiver icon and then, depending on the version of Receiver they are using, click About or Preferences from the Receiver menu and Plug-in Status or Advanced from the Receiver panel. You can also enable the log on option to appear when users right-click the Receiver icon by adding the following settings in the registry:

  - Add the Receiver key (if the key does not already exist) under the following registry locations:

    - `HKEY_CURRENT_USER\Software\Citrix\`

    - `HKEY_LOCAL_MACHINE\Software\Citrix\`
  - Add the Inventory key in the following registry locations:

    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`

    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`
  - In the Inventory key, configure the following **REG_SZ** values:

    - **VPNAddress**. Provide the value as the Web address for the Access Gateway appliance; for example, https://<AccessGatewayFQDN>.

    - **VPNPrompt1**. Provide the value as 'UserName'.

    - **VPNPrompt2**. Provide the value as '*Password'.

      Note: To mask the password, enter an asterisk (*) before the word.

      In addition, if you configure double-source authentication that requires authentication with LDAP plus RSA authentication, you need to also add the following as **REG_SZ**:

    - **VPNPrompt3**. Provide the value as '*Passcode'.

- Issue ID 0261547: When you enable Access Gateway as a reverse proxy and you enable basic preauthentication and post- authentication scans, as well as encryption and client choices, when users log on with the Access Gateway Plug-in, the preauthentication scan passes, but the post-authentication scan fails.

- Issue ID 0285995: If you configure Access Gateway to assign an intranet IP address to user devices that connect to Access Gateway, when users log on with the Access Gateway Plug-in, the secure DNS dynamic update does not occur and the intranet IP address is not registered with the DNS Server.

- Issue ID 0288469: After you configure a virtual server to use the Access Gateway Plug-in for Java, when users log on with the Access Gateway Plug-in by using a browser that has a 64-bit Java Runtime Environment (JRE) installed, the plug-in fails to establish a connection.

- Issue ID 0291264: If you create a Web Interface 5.4 site and enable authentication through Access Gateway, and you enable single sign-on with a smart card to the Web Interface that enables smart card pass-through, when users log on with the Access Gateway Plug-in, the users' desktops are not listed on the Web Interface.

- Issue ID 0291821: If you create a Web Interface 5.4 site and enable authentication with a smart card through Access Gateway, and you configure the 'Single Sign-on Domain' on the 'Published Applications' tab using the format domainname.com instead of domainname, when users start a published application or desktop, authentication fails.

- Issue ID 0292005: When users connect with clientless access and try to download a file larger than 1 gigabyte (GB) from the file share on the home page, as the file is downloading, if an upload is attempted, the download process fails but the upload continues.

- Issue ID 0298971: When users log on with the Access Gateway Plug-in for Java and the Web Interface opens in Internet Explorer 9, if users do not turn on Compatibility View in Internet Explorer, when they click a published application, the following error appears: Resource shortcuts are not available.

- Issue ID 0299515: If you configure an intranet IP address on Access Gateway, when users connect with the Access Gateway Plug-in on a computer running Windows XP Service Pack 3 and try to access a CIFS share hosted on a computer in the secure network, users receive an error that the share is inaccessible.

- Issue ID 0300511: When users log on using clientless access and click a bookmark from the home page to open a Distributed File Share (DFS), if the target folder resides on a different computer than the computer where the domain DFS server resides, the share does not open.

- Issue ID 0309017: When you configure a preauthentication and post-authentication policy with an expression to scan a user device for a file, Access Gateway does not check for expression syntax. As a result, Access Gateway accepts inappropriate syntax configuration and the scan fails.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

AppFlow

- Issue ID 0333560 (nCore): AppFlow records generated by the NetScaler appliance might contain junk characters.

Application Firewall

- Issue ID 0282932: If you use the Signature Editor to add a signature rule for a response-side check (such as the Credit Card or Safe Object check), in addition to one or more response patterns you must also add at least one request pattern. If you do not, then when you try to save the new signature rule, the configuration utility displays an error message and does not save the rule.

- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked. To work around this issue, if you configure Sessionless URL Closure, set Validate Referer Header to Off.

- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported for importing as application firewall signature rules. WAS 2.0 scan reports are not supported.

- Issue ID 0303060: Application firewall statistics are not supported for NetScaler classic policies. If you need to see numbers of policy hits and other statistics, you must use NetScaler default syntax policies.

Cache Redirection

- Issue ID 0287688: If you set the 'L2Conn' parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the 'L2Conn' parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

Cluster

- Issue ID 0343514: The cluster instance view in the configuration utility does not display which node is the configuration coordinator.
- Issue ID 0343137: The configuration utility does not display the "Add" button while configuring linksets.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click 'Application Firewall' in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0303279: In the configuration utility, in the 'Rewrite Policies' pane, clicking 'Add' does not display the 'Create Rewrite Policy' dialog box but disables the main configuration utility window.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0324797: The NetScaler configuration utility does not display the queue depth value for the configured priority queuing policies. This issue is observed only in a cluster setup.

  Workaround: You can view the queue depth of the policy by using the 'show pq policy' command on the command line interface.

- Issue ID 0332839: If you access the configuration utility through Internet Explorer 8, the System > Settings > Configure TCP Parameters, dialog box has no spaces between field names and fields.

- Issue ID 0333048: Using the Configuration Utility in Internet Explorer version 8, when you attempt to bind 250 or more VIP addresses to a VLAN, the Configuration Utility displays an unresponsive script error.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0334042: The configuration utility does not display a details panel for all the entities.

  Workaround: Click 'Edit' to display the details.

- Issue ID 0334292: If you navigate to HTTP Compression > Policies or HTTP Compression > Actions, the 'Remove' button is disabled in the task pane.

  Workaround: Use the command line interface to remove the policy or action.

  Note: You can access the command line interface from the configuration utility. Navigate to System > Diagnostics > Command Line interface.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the 'Create DNS View' dialog box, the 'Service(s) in this view' and 'Policy(s) in this view' lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs.

  Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0335701: You cannot add an SSL service with the Clear Text Port option in the configuration utility, because the option is disabled.

- Issue ID 0338513: When you log on to NetScaler configuration utility using Internet Explorer 8 or Internet Explorer 9, the web browser displays a blank screen as the browser is displaying the compatibility view.

  Workaround: Change to the standard view, in the Compatibility View Settings dialog box, by clearing the Display all websites in Compatibility View check box.

- Issue ID 0342735: Users might not be able to enable or disable NTP synchronization using the configuration utility.

  Workaround: Use command-line interface to enable or disable NTP synchronization.

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated.

Domain Name System

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

- Issue IDs 0330529 and 0322151: The following message might be displayed if you disable a virtual server-based DNS name server: 'ERROR: Name server does not exist. [nsnet_recvrpcioctl]'

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If a GSLB virtual server’s primary GSLB method is set to round trip time (RTT) and backup GSLB method is set to static proximity, or if the primary GSLB method is set to static proximity and backup GSLB method is set to RTT, and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

Load Balancing

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the 'show lb persistentSessions' CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 91711/0250846: If the string (or 'token') that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR('string2').AFTER_STR('string1') if the string that is enclosed by 'string1' and 'string2' is not larger than 64 KB.

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

- Issue ID 0278377 (nCore): Cache policy labels cannot be bound to MYSQL or MSSQL virtual servers.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

Load Balancing/SSL

- Issue ID 0331621: While creating SSL or load balancing virtual servers with default responder action, the NetScaler appliance throws a 'No such resource' error. This issue is observed only in a cluster setup.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type:

  #/etc/rc.d/svmd restart

- Issue ID 0337386: When restored from a backup, a NetScaler instance reverts to the release and build in which it was originally provisioned, even if the backup was taken from an upgraded configuration.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.
- Issue ID 0283035 and 0299716: In a cluster setup, the 'bind vlan' command throws an error when interface and IP address are specified together.
- Issue ID 0288450: The 'show lacp' command does not display the lacp configurations. This issue is observed only in a cluster setup.
- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command 'set ptp -state disable' and configure NTP to synchronize the time across the cluster nodes.
  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator, and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed.

  Workaround: Copy the certkey under /nsconfig/ssl/ folder on all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.

XML API

- Issue ID 0321005: The API to set the hostname for a NetScaler appliance is changed to include the owner node parameter for a cluster node.

Build 70.7

Release version: Citrix® NetScaler® release 10 build 70.7

Replaces build: None

Release date: September 2012

Release notes version: 4.0

Language supported: English (US)

Review the following sections:

- Changes and Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler and Citrix Access Gateway.

Changes and Fixes

AAA Application Traffic

- Issue ID 0327114: On a NetScaler appliance with NetScaler 10 build 69.4 nc installed, if you use the configuration utility to configure authentication on a load-balancing virtual server, the following error message appears:

  No Authentication Host specified

  The configuration utility then removes the authentication host from the configuration. This behavior occurs regardless of whether you are configuring authentication host settings on the virtual server for the first time, or modifying existing authentication host settings on the virtual server.

Access Gateway

- Issue ID 0308733: If you configure Access Gateway with additional appliances in which global server load balancing (GSLB) is enabled, when users log on with the Access Gateway Plug-in, occasionally the connection times out, a time-out error appears, such as 'Your Citrix Access Gateway session timed-out and you are not connected,' and the session disconnects.

- Issue ID 0319901: If you enable Integrated Caching and Web Interface on Netscaler on an Access Gateway appliance, and then change the URL for the Web Interface, Access Gateway might fail.

- Issue ID 0320210: When users connect with the Access Gateway Plug-in on a computer running Windows XP, the Group Policy Object is not applied.

- Issue ID 0321425: If you configure a virtual server with a default authentication type by using the Access Gateway wizard, if Access Gateway restarts, the configuration is not maintained and authentication fails.

- Issue ID 0329621: If you configure an endpoint policy and bind the policy to a virtual server, the preauthentication policy is not working as expected. Users with devices that meet the requirements may not be able to log on to Access Gateway.

AppFlow

- Issue ID 0288343: You can now configure the source IP address (SNIP or MIP address), to be used for AppFlow traffic. When you add an Appflow collector by using the add appflow collector command, you can use the -netprofile option to associate a netprofile to which the source IP address is bound. By default, the Appflow exporter takes NSIP address as the source IP address if you do not specify the -netprofile option.

  > add appflow collector <col_name> -IPAddress <IP_addr> [-netprofile {netprofile_name}]

- Issue ID 0311033 (nCore): AppFlow records can now log X-Forwarded-For HTTP header information. You can enable the logging with the set appflow param -httpXForwardedFor ENABLED command or by using the configuration utility.

- Issue ID 0313091: AppFlow records might not display the start time of the current transaction. Instead, they display the start time of the previous transaction due to reuse of connections.

- Issue ID 0320239 (nCore): HTTP method names might be occasionally truncated in the AppFlow records.

Application Firewall

- Issue ID 0299940: The change profile type command does not work correctly.

  - If you try to change a profile type to Web 2.0, the profile type remains HTML.

  - If you try to change a profile type to XML, the Profile Type field disappears completely.

  When you use the configuration utility to change the profile type, the profile type is actually changed correctly, but the display is incorrect. When you use the NetScaler command line, the actual profile type is set as shown above.

- Issue ID 0302294: Learned relaxations are sometimes not removed from the review list after they have been deployed. To manually remove a learned relaxation that has already been deployed, in the Manage Learned Rules dialog box select the relaxation and then click Skip.

- Issue ID 0329539 (nCore): On a NetScaler appliance with the application firewall enabled, occasionally the NetScaler appliance crashes when retrieving a page from a protected web site that sets one or more cookies.

- Issue ID 0330642: On a NetScaler appliance with both the application firewall and Integrated Caching features enabled, the NetScaler appliance might experience occasional resets when its memory fills up. The cause is a small memory leak.

- Issue ID 0331112 (nCore): In the NetScaler 9.3 58.2.nc build, when applying the HTML or XML SQL Injection check the application firewall does not transform special strings even when Transformation is enabled. This issue was fixed in build 58.4.nc.

Cache Redirection

- Issue ID 0328353: When you use the configuration utility to bind a cache redirection policy to a cache redirection virtual server, the policy is added to the content switching (CSW) policy tab instead of cache redirection (CRD) policy tab. If you try to resolve this issue by using the CR virtual server wizard, the following error message appears: 'Please specify Target.'
- Issue ID 0330033: Tabs for filter/compression policy bindings are not displayed for a cache redirection virtual server, and it is not possible to bind those policies to a cache redirection virtual server.
- Issue ID 0330139: If you use the configuration utility to unset a cache virtual server for a cache redirection virtual server, the process fails and the following error message appears: invalid argument.

Call Home

- Issue ID 0311617: When upgrading the NetScaler appliance to 10.70 or a later build, the appliance prompts you to enable the Call Home feature.

Cloud Gateway

- Issue ID 0327119: When you create policy rules from the configuration utility, an error occurs and the policies are not configured.

Configuration Utility

- Issue ID 0298686 (nCore): If the details pane contains too may records to display on one screen, the header row moves off the screen if you scroll down.
- Issue ID 0311358: The NetScaler configuration utility fails to load when accessed from Internet Explorer version 7 browser running on Windows 2003 or Windows XP.
- Issue ID 0314769: When the certificate used to sign the JAR files expires, the application's digital signature cannot be verified. An error is displayed when the user tries to access the NetScaler GUI.
- Issue ID 0319061: The configuration utility does not throw the 'Feature not supported' prompt when configuring the following unsupported features on a NetScaler cluster: Bridge groups, Network Bridge, VMAC6, and FIS.
- Issue ID 0322821: When the SRADV (Static Route Advertisement) mode is ON, the static routes which are not explicitly disabled for advertisement will be advertised using all the routing protocols. However, the advertised protocols column for route in the configuration utility does not show any protocol list. This issue is observed only in a cluster setup.
- Issue ID 0322894: The configuration utility displays an inappropriate error message when adding a forwarding session that has an invalid subnet mask. This issue is observed only in a cluster setup.
- Issue ID 0322914: When the IP is not resolved for a hostname based SNMP manager, the 'Resolved IP' column of the SNMP Manager table is shown as blank instead of 'Unresolved IP'. This issue is observed only in a cluster setup.
- Issue ID 0323175: The configuration utility displays a negative value for the index of the data set or pattern set, when the index is set to its maximum value. The command line interface displays the correct value.
- Issue ID 0325400: After adding a local authentication policy by using the configuration utility, the request profile field is showing blank. By default, the request profile must be Local. This issue is observed only in a cluster setup.
- Issue ID 0326018: The dashboard does not display the Precision Time Protocol (PTP) counters for the cluster node. This issue is observed only in a cluster setup.
- Issue ID 0326354: In System > Settings > Change global system settings, regardless of the base threshold value configured for surge protection, the value is displayed as 0. This issue is observed only in a cluster setup.
- Issue ID 0326413: An error occurs if you use the NetScaler configuration utility to configure a large preauthentication policy (for example, a policy with 900 characters).
- Issue ID 0327136: The configuration utility does not allow you to set the 'Max Clients' parameter of a service to its maximum value of 4294967294. This issue is observed only in a cluster setup.
- Issue ID 0327551: In the configuration utility, all features appear to be enabled even when the features are disabled.

- Issue ID 0328660: In the configuration utility, when you view the virtual server persistence sessions, a persistence type setting of DIAMETER is displayed as SOURCE IP.

- Issue ID 0328715: In the configuration utility, the details of the monitor bound to a service do not include response codes for a monitor of type DIAMETER.

- Issue ID 0328747: In the Reporting tool, when users try to generate 'system entities statistics' report for GSLB domains, the GSLB domain names configured on the appliance might not be displayed in the entities list.

- Issue ID 0328844: While configuring the OCSP responder through the configuration utility, the default value of the HTTP response timeout is erroneously taken as 0ms. The default value of the HTTP response timeout must be 2000ms. This issue is observed only in a cluster setup.

- Issue ID 0329154: In System > Auditing > Recent audit messages, when you set number of audit messages to be displayed to 256 (maximum allowed value), a 'Value entered is out of range' error message is displayed on clicking Refresh. This issue is observed only in a cluster setup.

- Issue ID 0329826: If you use the configuration utility to view the license for features, warning messages are seen for the features that are licensed but not supported. This issue is observed only in a cluster setup.

- Issue ID 0331158: When you access NetScaler configuration utility from Internet Explorer 8 or Internet Explorer 9, the web browser displays only a grey bar at the top of the screen as the browser is displaying the compatibility view.

- Issue ID 0331604: If you access a load balancing virtual server after a NOPOLICY is bound to it, the configuration utility might display the following error: 'no such policy exists'

- Issue ID 0332795: On systems that have JRE 1.6.0_24 and 1.7.0_06, the configuration utility cannot load the Java applet. Therefore, you cannot perform any operations on the configuration utility.

- Issue ID 0332876: When you use the configuration utility to change the password of a user, the Change Password dialog displays encrypted password in the Password and Confirm Password fields.

- Issue ID 0333026: On a system running the Windows 7, 64-bit operating system, the configuration utility cannot load the Java applet. Therefore, you cannot perform any operations on the configuration utility.

Content Switching

- Issue ID 0230903: The content switching feature now supports the ability to bind a policy to multiple virtual servers or policy labels. To support multiple policy bind functionality, the target load balancing virtual server is specified in the action and attached to the policy. This enhancement enables you to reuse an existing policy by binding it to the virtual servers. You can also combine multiple policies in a policy label and apply the policy label to the virtual server.

- Issue ID 0330045: The configuration changes made by using the bind cs vserver and bind cs policylabel commands are not saved in the configuration file. Therefore, the CS policy bindings are lost the first time the NetScaler appliance is restarted after an upgrade to release 10.

- Issue ID 0330290: You cannot use the configuration utility to bind a content switching policy to a content switching virtual server if the policy is configured with only a domain value. The bind fails, and the following error message appears: 'Priority cannot be specified for URL-based content switching policy.'

- Issue ID 0331029: If you use the configuration utility to open a content switching virtual server that has a default policy bound to it, the process fails and the following error message appears: No Such Resource.

DataStream

- Issue ID 0323442: The DataStream feature does not support dynamic stored procedures. Consequently, dynamic stored procedures fail if they use the sp_prepexec and sp_prepare stored procedures.

Global Server Load Balancing

- Issue ID 0324486: When creating a local GSLB site in the NetScaler configuration utility, if you set the Trigger Monitors option to MEPDOWN, the GSLB site does not appear in the details pane until after you click 'Refresh'.

- Issue ID 0326364: Even though a GSLB virtual server is configured with the static proximity method, and some requests match a DNS policy whose action uses a DNS view to restrict matching requests to only a subset of the bound services, the NetScaler appliance uses the round robin method to load balance requests across all of the GSLB services that are bound to the GSLB virtual server. The issue can occur if the locations that correspond to the source IP addresses in the DNS requests are not found in the location database.

- Issue ID 0328911: When configuring monitoring for a GSLB service by using the NetScaler configuration utility, if you include monitors that cannot be used with GSLB services (for example, ARP monitors) along with monitors that can be used with GSLB services (for example, TCP monitors), the configuration utility displays an error message for the invalid monitor bindings, but the valid bindings succeed. When you unbind an invalid monitor from the service, the message 'Error' is displayed. No further information is provided in the message.

Integrated Caching

- Issue ID 0329485: When the NetScaler appliance responds to a byte range request, it might get into an infinite loop for one specific request, which might cause the appliance to fail.

Load Balancing

- Issue ID 0314738: If you issue the 'force HA sync -force' command when HA synchronization is disabled on both nodes, the services on the secondary node are marked as DOWN. The services remain in that state until after a failover. When a failover occurs, the failover of some services might be delayed by a few seconds while monitors learn the actual states of those services. Until the monitors learn and correct the states, new connections to those services might be rejected. Consequently, you might also observe a brief period of outage following a failover.

- Issue ID 0323317: The configuration commands for binding views to GSLB services are not shown in the output of the show ns runningConfig or show gslb runningConfig commands. Additionally, the configuration commands are lost during a reboot or upgrade.

- Issue ID 0323891: The NetScaler CLI and configuration utility display incorrect values for the following counters, which are used for monitoring services, including GSLB services :

  - Total number of monitoring probes sent

  - Total number of failed probes

  - Current number of failed probes
- Issue ID 0324061: When you configure a SIP-UDP load balancing virtual server by using the NetScaler command-line interface, the default setting for persistence type is CALLID. However, when you use the configuration utility to configure a SIP-UDP virtual server, the default setting for persistence type is NONE.

- Issue ID 0324576: The automatic domain based service group scaling option (the autoScale parameter) has been moved from the bind serviceGroup command to the add serviceGroup command. The possible values of the parameter have changed from YES and NO to DNS and DISABLED, respectively.

  To configure a service group to scale automatically, using the NetScaler command line, at the NetScaler command prompt, type the following command:

  add serviceGroup <serviceGroupName>@ <serviceType> -autoScale DNS

  To configure a service group to scale automatically, using the NetScaler configuration utility, go to Load Balancing > Service Groups > Add. In the Create Service Group dialog box, on the Advanced tab, from the Auto Scale Mode list, select DNS.

- Issue ID 0329191 (nCore): If an AppExpert application that was used to load user configuration to the NetScaler appliance is removed, the appliance becomes unavailable.

- Issue ID 0330276: The virtual router IDs (VRIDs) that are configured on the NetScaler appliance are not available in the Virtual Router ID list in the Create IP and Configure IP dialog boxes (Network > IPs > Add/Open). Consequently, you cannot use the configuration utility to bind a VRID to a virtual server.

Monitoring

- Issue ID 0320571: The state of a service is shown as UP even when the service is down. Consequently, the NetScaler appliance continues to forward requests to that service, and clients do not receive responses to their requests.

NetScaler SDX Appliance

- Issue ID 0326655: If you upgrade the Management Service from an earlier build to build 56.x or 57.x, restarting the appliance while data migration is in progress might corrupt your data contents.
- Issue ID 0326663: In release 9.3, the upgrade process fails if you attempt to upgrade the Management Service from build 48.6 to build 56.5 or 57.5.
- Issue ID 0326878: The Management Service shows duplicate entries for NetScaler VPX instances because of intermittent database connection failures. This is only a display issue. However, if a VPX instance is configured with an external authentication server for the nsroot (administrator) user, the authentication server might show several authentication failures.
- Issue ID 0327984: You can now apply a hotfix for XenServer from the Management Service. On the Configuration tab, expand Management Service, and then click XenServer Files. In the details pane, click Hotfixes, and then click Upload. After uploading the hotfix to the appliance, click Apply. If an error occurs in the process of applying the hotfix, an error message displays the cause of the problem.

NetScaler VPX Appliance

- Issue ID 0328540: After you install the initial NetScaler virtual appliance, if you try to save the configuration and licenses are not present on the appliance, the appliance becomes unresponsive. Restart the appliance and load the licenses. Restart the appliance again for the changes to take effect. Then save the configuration.
- Issue ID 0329966: After you install the initial NetScaler virtual appliance (.xva image) for build 69.4, if you run the 'save config' command and licenses are not present on the appliance, the appliance becomes unresponsive. Restart the appliance and load the licenses. Restart the appliance again for the changes to take effect. Then run the 'save config' command.

Networking

- Issue ID 0321868: BGP does not advertise default route to the peer, with default-originate flag, if the state of a learnt default route toggles.
- Issue ID 0324432: The NetScaler appliance forwards (L3 mode) certain response packets with IP header checksum value 0xFFFF, which is an invalid value according to RFC 1624. As a result, the router drops these packets.
- Issue ID 0330118: OSPF maximum age link-state advertisements (LSAs) are not removed from the NetScaler appliance because the maximum age walker processes suspended indefinitely.
- Issue ID 0330165: After upgrading the Netscaler appliance to 10.69.4 build, the appliance does not learn a ARP entry from a ARP reply packet, if the MAC addresses in the Ethernet header (Source MAC) and ARP header(Sender MAC) of the ARP reply packet are different.

Platform

- Issue ID 0276184: NetScaler release 10 build 70.x is supported on the new MPX 8200/8400/8600 platform.

Policy

- Issue ID 0291487: NetScaler appliances running version 9.2 build 52.1 or later and have a large number (in the hundreds) of policy bindings can experience performance issues on 'save ns config' and 'show config' operations. This can lead to interruption in services.
- Issue ID 0322964: Removed the 'unset audit syslogPolicy' and 'unset audit nslogPolicy' commands from NetScaler release 10 build 70 onwards.
- Issue ID 0324700: Removed the 'unset filter policy' command from NetScaler release 10 build 70 onwards.

Responder

- Issue ID 0324200 (nCore): On a NetScaler appliance with the responder feature configured to redirect requests from authenticated members of a particular group to a custom web page, the redirections sometimes fail. The reason is that, when the responder feature is invoked before the AAA session is completely established (as is the case when a user selects a choice after initial logon), the user's AAA session is not transferred from one core to the other. Responder therefore fails to identify the user as a member of the targeted group.
- Issue ID 0330133: On a NetScaler appliance with the responder feature enabled and a respondWith response configured, if a user sends a request with a large Content-Length header, the NetScaler appliance might appear to hang. The cause of the apparent hang is that the NetScaler appliance expects a request of the specified Content-Length, and waits for the rest of the request before responding to it.

Rewrite

- Issue ID 0301481: On a NetScaler appliance that has a response-side rewrite policy configured and bound to a load balancing virtual server, a request sent to the virtual server might trigger a sequence of events that causes the NetScaler appliance to fail.

SSL

- Issue ID 0327173: The ciphers bound to an SSL virtual server are not displayed in the configuration utility.

System

- Issue ID 0271783: If you configure an RNAT rule and enable the TCP proxy option for RNAT, the NetScaler appliance functions as a proxy for internal clients and maintains separate client-side and server-side connections. In certain scenarios, this behavior might result in a service type mismatch between the client-side and server-side connections, and the appliance might reboot with a core dump.

- Issue IDs 0306352 and 0332253: When using the configuration utility or SSH to log on to the appliance, the "Connection limit to CFE exceeded" message might be displayed. This message is displayed if an earlier session was closed without logging out of the session.

- Issue ID 0306660 (nCore): You can now use the 'set ns tcpparam connFlushIfNoMem <connFlushIfNoMem>' command on a NetScaler appliance to close existing connections if memory is not available for a new connection. When using this command, you must specify the type of connection to be closed. By default, this feature is disabled on the appliance.

- Issue IDs 0312893 and 0331073: When you run the 'show run' command, the NetScaler appliance might fail even if the you have permission to run the command.

- Issue ID 0325665: An unrelated error code is displayed on executing the ‘set filter prebodyinjection/postbodyinjection’ commands.

- Issue ID 0323190: In rare cases, the NetScaler appliance fails when some pages are recovered from the free queue before the page table scan is complete.

- Issue ID 0327118: In the configuration utility, the minimum and maximum values allowed for number of audit messages is incorrect. The maximum and minimum values displayed are 255 and 0, but the correct values are 256 and 1.

- Issue ID 0330336 (nCore): IPv6 addresses might occasionally be captured in the audit log, even though IPv6 addresses are not configured.

Web Interface

- Issue ID 0306731: If the Rewrite feature is not enabled, the Enable access through receiver client option for a Web Interface(WI) site does not work. This is because the functionality of the option depends on some rewrite policies on the appliance.

- Issue ID 0315502: The Configuration Utility displays an error message when you try to disable the Web Interface feature.

- Issue ID 0315951: If the Responder feature is not enabled, the Make Site Path Case Insensitive option for a Web Interface(WI) site does not work. This is because the functionality of the option depends on some Responder polies on the appliance.

- Issue ID 0324373: In the Web Interface (WI) configuration wizard, for a WI site in gateway direct mode, the state of the Enable Access through Receiver Client option is shown selected even when there are no rewrite policies bound to the selected Access Gateway virtual server.

- Issue ID 0331904: In the Web Interface (WI) configuration wizard, the Enable Access through Receiver Client option remain selected even when you try to clear the option.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberoes authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, adn then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.

- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

- Issue ID 0327446: On an Outlook for Web Access (OWA) 2010 server that is protected by AAA-TM with single sign-on (SSO) enabled, when a user who uses the Firefox or Chrome browsers logs off, some OWA 2010 images do not appear.

- Issue ID 0334363: In the Citrix NetScaler configuration utility, when a user clicks the AAA-Application Traffic Wizard link, the configuration utility displays error message of 'Unknown Error'. The browser is then frozen til the session times out.

Access Gateway

- Issue ID 0249975: When users log on with the Access Gateway Plug-in, the 'File Transfer' tab on the Access Interface is available, but the 'File Transfer option' is not available if users right-click the Access Gateway icon in the notification area.

- Issue ID 92543/0251596: After you configure Access Gateway to provide user connections through Citrix Receiver, when users right-click the Receiver icon in the notification area, the Log on option does not appear. Users must connect by using the Web browser or they must right-click the Receiver icon and then, depending on the version of Receiver they are using, click About or Preferences from the Receiver menu and Plug-in Status or Advanced from the Receiver panel. You can also enable the log on option to appear when users right-click the Receiver icon by adding the following settings in the registry:

  - Add the Receiver key (if the key does not already exist) under the following registry locations:

    - `HKEY_CURRENT_USER\Software\Citrix\`

    - `HKEY_LOCAL_MACHINE\Software\Citrix\`
  - Add the Inventory key in the following registry locations:

    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`

    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`
  - In the Inventory key, configure the following **REG_SZ** values:

    - **VPNAddress**. Provide the value as the Web address for the Access Gateway appliance; for example, https://<AccessGatewayFQDN>.

    - **VPNPrompt1**. Provide the value as 'UserName'.

    - **VPNPrompt2**. Provide the value as '*Password'.

      Note: To mask the password, enter an asterisk (*) before the word.

      In addition, if you configure double-source authentication that requires authentication with LDAP plus RSA authentication, you need to also add the following as **REG_SZ**:

    - **VPNPrompt3**. Provide the value as '*Passcode'.
- Issue ID 0261547: When you enable Access Gateway as a reverse proxy and you enable basic preauthentication and post- authentication scans, as well as encryption and client choices, when users log on with the Access Gateway Plug-in, the preauthentication scan passes, but the post-authentication scan fails.

- Issue ID 0275079: When users access applications published on XenApp, each user consumes multiple Access Gateway licenses per application. Instead, one session ID should be shared across the applications the user accesses. As a result, users exceed their allocated license count and an SSL error occurs.

- Issue ID 0278218: If you configure an endpoint policy, the preauthentication policy runs as expected. When users try to log on with the Access Gateway Plug-in, however, occasionally the post-authentication policy does not work as expected and

authentication fails.

- Issue ID 0285995: If you configure Access Gateway to assign an intranet IP address to user devices that connect to Access Gateway, when users log on with the Access Gateway Plug-in, the secure DNS dynamic update does not occur and the intranet IP address is not registered with the DNS Server.

- Issue ID 0288469: After you configure a virtual server to use the Access Gateway Plug-in for Java, when users log on with the Access Gateway Plug-in by using a browser that has a 64-bit Java Runtime Environment (JRE) installed, the plug-in fails to establish a connection.

- Issue ID 0291264: If you create a Web Interface 5.4 site and enable authentication through Access Gateway, and you enable single sign-on with a smart card to the Web Interface that enables smart card pass-through, when users log on with the Access Gateway Plug-in, the users' desktops are not listed on the Web Interface.

- Issue ID 0291821: If you create a Web Interface 5.4 site and enable authentication with a smart card through Access Gateway, and you configure the 'Single Sign-on Domain' on the 'Published Applications' tab using the format domainname.com instead of domainname, when users start a published application or desktop, authentication fails.

- Issue ID 0292005: When users connect with clientless access and try to download a file larger than 1 gigabyte (GB) from the file share on the home page, as the file is downloading, if an upload is attempted, the download process fails but the upload continues.

- Issue ID 0298971: When users log on with the Access Gateway Plug-in for Java and the Web Interface opens in Internet Explorer 9, if users do not turn on Compatibility View in Internet Explorer, when they click a published application, the following error appears: Resource shortcuts are not available.

- Issue ID 0299515: If you configure an intranet IP address on Access Gateway, when users connect with the Access Gateway Plug-in on a computer running Windows XP Service Pack 3 and try to access a CIFS share hosted on a computer in the secure network, users receive an error that the share is inaccessible.

- Issue ID 0300511: When users log on using clientless access and click a bookmark from the home page to open a Distributed File Share (DFS), if the target folder resides on a different computer than the computer where the domain DFS server resides, the share does not open.

- Issue ID 0309017: When you configure a preauthentication and post-authentication policy with an expression to scan a user device for a file, Access Gateway does not check for expression syntax. As a result, Access Gateway accepts inappropriate syntax configuration and the scan fails.

- Issue ID 0319607: If an authentication server and Access Gateway reside in the same domain, the appliance may fail.

- Issue ID 0327433: If you configure a virtual server by using the Remote Access wizard and configure a Secure Ticket Authority (STA), the status of the server appears as UP. However, in the configuration utility, on the Home tab, under Alerts, a message states that the STA server is not configured. You must bind the server globally in order to clear the message.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

AppFlow

- Issue ID 0333560 (nCore): AppFlow records generated by the NetScaler appliance might contain junk characters.

Application Firewall

- Issue ID 0282932: If you use the Signature Editor to add a signature rule for a response-side check (such as the Credit Card or Safe Object check), in addition to one or more response patterns you must also add at least one request pattern. If you do not, then when you try to save the new signature rule, the configuration utility displays an error message and does not save the rule.

- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked. To work around this issue, if you configure Sessionless URL Closure, set Validate Referer Header to Off.

- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported for importing as application firewall signature rules. WAS 2.0 scan reports are not supported.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

CloudBridge

- Issue ID 0334949: If you use configuration utility to remove an IPv4 tunnel for CloudBridge from a NetScaler appliance, the remove process succeeds but the following Java exception is displayed: 'ClassNotFoundException'.

Cluster

- Issue ID 0332594: The RIP (Routing Information Protocol) and Cache Redirection features cannot be enabled in a NetScaler cluster setup.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click Application Firewall in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0319070: The Setup wizard is not launched automatically if a mapped IP (MIP) address or a Subnet IP (SNIP) address is not configured on the NetScaler appliance.

- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0324797: The NetScaler configuration utility does not display the queue depth value for the configured priority queuing policies. This issue is observed only in a cluster setup.

  Workaround: You can view the queue depth of the policy by using the 'show pq policy' command on the command line interface.

- Issue ID 0332839: If you access the configuration utility through Internet Explorer 8, the 'System' > 'Settings' > 'Configure TCP Parameters,' dialog box has no spaces between field names and fields.

- Issue ID 0333048: Using the Configuration Utility in Internet Explorer version 8, when you attempt to bind 250 or more VIP addresses to a VLAN, the Configuration Utility displays an unresponsive script error.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0333836: If you have configured global server load balancing by using the GSLB wizard, Wizard for Citrix XenApp, or Wizard for Citrix XenDesktop, and you attempt to

view the GSLB Visualizer, Prefuse information might be logged to the Java console. However, you can view the GSLB Visualizer, and the functionality is not affected.

- Issue ID 0334042: The configuration utility does not display a details panel for all the entities.

  Workaround: Select the entity and click 'Open' to display the details.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

  Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0334280: After you rename a compression policy, the new name might not be reflected in the configuration utility.

  Workaround: Refresh the page to see the renamed policy.

- Issue ID 0334284: If you navigate to HTTP Compression > Policies and click 'Policy Manager' in the task pane, the following error message might appear: No such policy exists.

  Workaround: Refresh the page and try again.

- Issue ID 0334292: If you navigate to HTTP Compression > Policies or HTTP Compression > Actions, the Remove button is disabled in the task pane.

  Workaround: Use the command line interface to remove the policy or action.

  Note: You can access the command line interface from the configuration utility. Navigate to System > Diagnostics > Command Line interface.

- Issue ID 0334773: In the Synchronize GSLB Configuration dialog box, the Command parameter is unavailable when the Synchronization Option parameter is set to its default value (automatic synchronization).

- Issue ID 0335008: The exception 'netscape.javascript.JSException' is logged to the Java console when you create a DNS key by using the NetScaler configuration utility. However, the DNS key is created, and there is no loss in functionality.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the Create DNS View dialog box, the 'Service(s) in this view' and 'Policy(s) in this view' lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0335235: The NetScaler configuration utility does not show globally bound AppFlow policies in the policy manager. This issue is observed only in a cluster setup.

- Issue ID 0335701: You cannot add an SSL service with the Clear Text Port option in the configuration utility, because the option is disabled.

- Issue ID 0335719: The exception “netscape.javascript.JSException” is logged to the Java console when you sign a DNS zone by using the NetScaler configuration utility, and the browser’s status bar does not report the status of the zone-signing operation. However, the zone is signed, and there is no loss in functionality.

- Issue ID 0333577: When configuring the Transformation URL Profile, an error occurs if you set Priority to a value higher than 2147483647 (maximum allowed value).

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs.

  Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0335913: In a cluster setup, you cannot enable a server entry that is disabled, because the Enable button is unavailable. However, you can disable a server entry by using the NetScaler command line interface.

- Issue ID 0338513: When you log on to NetScaler configuration utility from Internet Explorer 8 or Internet Explorer 9, the web browser displays a blank screen as the browser is displaying the compatibility view.

  Workaround: Change to the standard view, in the 'Compatibility View Settings' dialog box, by clearing the 'Display all websites in Compatibility View' check box.

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated.

Domain Name System

- Issue IDs 0268748 and 0333310: In a cluster setup, if you save the configuration and reboot an appliance, the default name-server records for the thirteen root servers, and their associated address records, become unavailable. If you need them, you have to add them manually after you perform a reboot.

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

- Issue ID 0330529: The following message might be displayed if you disable a virtual server-based DNS name server: 'ERROR: Name server does not exist. [nsnet_recvrpcioctl]'

Global Server Load Balancing

- Issue ID 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If a GSLB virtual server’s primary GSLB method is set to round trip time (RTT) and backup GSLB method is set to static proximity, or if the primary GSLB method is set to static proximity and backup GSLB method is set to RTT, and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

Load Balancing

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the 'show lb persistentSessions' CLI command displays an internal representation of thepersistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 91711/0250846: If the string (or 'token') that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR('string2').AFTER_STR('string1') if the string that is enclosed by 'string1' and 'string2' is not larger than 64 KB.

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

- Issue ID 0318310: While creating a load balancing monitor, you cannot specify a send string that has a length of more than 76 characters. This issue is observed only in a cluster setup.

- Issue ID 0331621: While creating SSL or load balancing virtual servers with default responder action, the NetScaler appliance throws a 'No such resource' error. This issue is observed only in a cluster setup.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type : #/etc/rc.d/svmd restart

- Issue ID 0337386: When restored from a backup, a NetScaler instance reverts to the release and build in which it was originally provisioned, even if the backup was taken from an upgraded configuration.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.

- Issue ID 0283035 and 0299716: In a cluster setup, the 'bind vlan' command throws an error when interface and IP address are specified together.

- Issue ID 0288450: The 'show lacp' command does not display the lacp configurations. This issue is observed only in a cluster setup.

- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command 'set ptp -state disable' and configure NTP to synchronize the time across the cluster nodes.

  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.

- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator, and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed.

  Workaround: Copy the certkey under /nsconfig/ssl/ folder on all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.

System

- Issue ID 0338244: The CallHome feature checks for compact flash drive and hard disk drive errors every six minutes instead of every six hours. If any errors are found, the appliance's data is uploaded to the Citrix Technical Support server.

Build 69.4

Release version: Citrix® NetScaler®, version 10 build 69.4

Replaces build: None

Release date: August 2012

Release notes version: 3.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Changes
- Bug Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler and Citrix Access Gateway.

Enhancements

Smart Card Authentication for Web Interface Site using Access Gateway (Issue ID 0287639)

The NetScaler appliance now supports smart card authentication for web interface on NetScaler through Access Gateway. On using this enhancement, you can configure a web interface site that can be accessed by logging into an Access Gateway virtual server by using a smart card. To use this enhancement, you must upgrade the NetScaler to the latest build and install the new web interface tar file 'nswi-1.5.tgz'. For more information, see the 'Using Smart Card Authentication for Web Interface on NetScaler' topic in the 'Web Interface' chapter of the *Citrix NetScaler Administration Guide*.

Automatically Populating the Default Value of a Virtual Server on a Web Interface Site (Issue ID 0300470)

While modifying a web interface site configured in Direct mode, the default value for the virtual server is now automatically populated with one of the load balancing virtual servers configured during the creation of the web interface site.

Case Sensitivity on the Web Interface Wizard (Issue ID 0246466)

An option 'Make Site Path Case Insensitive' on the web interface wizard has been introduced. When you enable this option, the NetScaler appliance ignores case sensitivity in the site name part of the URL request for a web interface site configured on the NetScaler appliance.

Multiple Binding of Content Switching PI Policies to Content Switching Virtual Servers and Policy-labels (Issue ID 67323/0230903)

The multiple policy binding feature enables you to bind a policy to multiple virtual servers or policy labels. Earlier, you could bind a policy only to a single virtual server or policy label and to reuse an existing policy, you needed to create a copy of the same policy with a different name before attaching it to another virtual server. With the multiple policy binding feature, you can reuse an existing policy for multiple virtual servers.

Global State Update Option for Content Switching (Issue ID 0274449)

You can now enable the state update option globally for content switching virtual servers configured on the NetScaler appliance. If a specific virtual server's local state update option is set to DISABLED, that setting is overridden by a global ENABLED setting. However, a local setting of ENABLED overrides a global setting of DISABLED for the state update option. As shown in the following table, state update is not disabled for a virtual server unless both the global and local options are set to DISABLED.

Global state update setting	Virtual server state update setting	Effective state update setting on the virtual server
ENABLED	ENABLED	Enabled
ENABLED	DISABLED	Enabled
DISABLED	ENABLED	Enabled
DISABLED	DISABLED	Disabled

To configure the state update option globally by using the NetScaler command line, at the NetScaler command prompt, type the following command:

```
set cs parameter [-stateupdate ( ENABLED | DISABLED )]
```

To configure the state update option globally by using the NetScaler configuration utility

1. In the navigation pane, click 'Content Switching'.
2. In the details pane, click 'Configure Content Switching parameter'.
3. In the 'Set Content Switching Parameters' dialog box, select the 'State Update' check box.
4. Click 'OK'.

Support for Load Balancing Diameter Traffic (Issue ID 86737/0246690)

You can now load balance Diameter traffic. The Diameter protocol is a next generation Authentication, Authorization, and Accounting (AAA) signaling protocol mainly used on mobile devices such as laptops and mobile phones. It is a peer-to-peer protocol as opposed to the traditional client-server model that is used by most other protocols. For more information, see the 'Configuring Diameter Load Balancing' topic in the Load Balancing' chapter of the *Citrix NetScaler Traffic Management Guide*.

Stateless Connection Failover Supported for IPv6 (Issue ID 0276300)

You can now bind an IPv6 service to a load balancing virtual server with connection failover set to stateless.

Options for Branch IP Address in the Load Balancing wizard for Branch Repeater (Issue ID 0275289)

In the 'Load Balancing wizard for Branch Repeater', when specifying a branch whose traffic is to be accelerated, you can specify either the primary IP address or the accelerated pair A (apA) IP address of a Branch Repeater appliance.

NetScaler SDX - System Health Monitoring (Issue ID 0291018)

A supplemental software pack supports system health monitoring on the NetScaler SDX appliance for hardware and software components, disks, fan, voltage, temperature, and power supply sensors, and interfaces. For more information about this enhancement, see the 'System Health Monitoring' chapter in the *Citrix NetScaler SDX Administration Guide*. To install the supplemental software pack, see http://support.citrix.com/article/ctx132877.

New Health Monitoring Gadget on the NetScaler SDX Appliance (Issue ID 0313835)

You can now view the top 25 critical health monitoring events in the Health Monitoring gadget on the Home tab in the Management Service user interface. Select an event to view details or to delete the event.

Session Management for Communication with NetScaler Instances (Issue ID 0287133)

All HTTP and HTTPS communication between the Management Service and a NetScaler VPX Instance is now through a persistent session. A session ID is associated with each VPX instance and all HTTP and HTTPS communication between the Management Service and the instance uses this session ID.

Session Management for Communication with XenServer (Issue ID 0303527)

With XenServer version 6.0 and later, HTTP communication between the Management Service and XenServer is now over a persistent session. All HTTP communication between the Management Service and XenServer uses one session ID. For earlier versions of XenServer, basic authentication (user name and password) is used.

SNMP Support on the NetScaler SDX Appliance (Issue ID 94071/0257902)

You can now configure a Simple Network Management Protocol (SNMP) agent on the Citrix NetScaler SDX appliance to generate asynchronous events, which are called traps. For more information about this enhancement, see the 'SNMP' chapter in the *Citrix NetScaler SDX Administration Guide*.

Installing a Supplemental Pack for XenServer (Issue ID 0303515)

You can now install the NetScaler SDX supplemental packs from the Management Service without manually opening an ssh connection to XenServer. To install this pack, on the configuration tab, in the navigation pane, expand Management Service, and then click XenServer Files. In the details pane, click 'Supplemental Packs'. You can upload the supplemental pack to the SDX appliance and also download it to create a backup on your client.

Change Management on the NetScaler SDX Appliance (Issue ID 0291024)

You can now track any changes to the configuration on a NetScaler VPX instance from the Management Service. To view these changes, on the configuration tab, in the navigation pane, expand NetScaler, and then click Change Management. The details pane lists the device name with IP address, date and time when it was last updated, and whether there is a difference between the saved configuration and running configuration. Select a device to view its running configuration, saved configuration, revision history of configuration changes, and difference between the configuration before and after an upgrade. You can download the configuration of a NetScaler VPX instance to your client. By default, the Management Service polls all the instances every 24 hours but you can change this interval by clicking Configure Poll Interval in the details pane.

Configuring Tagged VLANs on the NetScaler SDX Appliance (Issue IDs 0278369 and 0284146)

You can now configure a tagged VLAN, without configuring an NSVLAN, at the time of provisioning a NetScaler instance. For more information about this enhancement, see the 'Provisioning NetScaler Instances' chapter in the *Citrix NetScaler SDX Administration Guide*.

Cloud Bridge CLI Commands Simplified (Issue ID 0307496)

Simplified the Cloud Bridge CLI commands for configuring IPSec Tunnel.

Filtering out Connection Table using CSW/LB vserver Policy Expressions (Issue ID 0302889)

Added policy expressions for the 'show connectiontable' command to filter out connections of a specific content switching or load balancing virtual server.

For example: `show connectiontable CONNECTION.LB_VSERVER.NAME.EQ("v1")`

Configuration Utility Simplified (Issue ID 0306109)

Simplified the configuration utility to ease the process to connect to the cloud service providers.

Application Firewall - Learning from Trusted Clients/Networks Only (Issue ID 86758/0246711)

You can now configure the application firewall learning feature to learn from trusted clients or networks only, instead of learning from all traffic that it processes. By restricting learning to trusted clients, you can prevent attacks against your protected web sites and web services from being learned as normal use and therefore not blocked. Currently trusted learning can be configured only from the NetScaler command line.

To configure the application firewall to learn from trusted clients or networks only, first enable the trusted learning feature. Next, add your trusted clients and networks. To add a trusted client, add the client's IP. IPv4 and IPv6 IPs are both supported. You can use a prefix of /0 after the IP, but that is not necessary. To add a trusted network, add the network in CIDR format.

To enable and configure trusted learning, at the NetScaler command line type the following commands:

set appfw profile <profileName> -enabletrustedLearning (on|off)
bind appfw profile <profileName> -trustedLearningClients (<ip_addr>|<ipv6_addr>|<cidr/prefix>) -state (ena

For <profileName>, substitute the name of the application firewall profile that you want to associate with these trusted learning settings. If you want to add a trusted client or network to the configuration but not configure the application firewall to learn from it yet, set state to disabled. You can add an optional comment to document which client or network you added and why.

The following commands enable trusted learning, add a trusted client at 10.178.16.34, and add a trusted network at 10.102.30.0/24.

set appfw profile TestProfile -enabletrustedLearning on
bind appfw profile TestProfile -trustedLearningClients 10.178.16.34 -state enabled -comment "Trusted client
bind appfw profile TestProfile - trustedLearningClients 10.102.30.0/24 -state enabled -comment "Trusted ne

New TACACS+ Configuration Parameter (Issue ID 0257671)

If you configure a TACACS+ server for authentication, when users without the appropriate permissions enter a command, the command does not execute, but the command is recorded in an accounting log. A new configuration parameter corrects this behavior.

New Syntax for Binding Content Switching Policies and Load Balancing Virtual Servers to a Content Switching Virtual Server (Issue ID 0291791)

For the 'bind cs vserver command', the 'targetVserver' parameter is now deprecated. If you attempt to set the parameter, the following warning appears: “Warning: Argument deprecated [targetVserver].”

This release introduces the 'lbvserver' parameter, for binding the default load balancing virtual server to the content switching virtual server, and the 'targetLBVserver' parameter, for binding other load balancing virtual servers through content switching policies.

In the NetScaler configuration utility, there are no changes in how you bind a default load balancing virtual server or a load balancing virtual server that is not the default.

To specify a default load balancing virtual server by using the NetScaler command line, at the NetScaler command prompt, type the following command:

```
bind cs vserver <csvservername> -lbvserver <targetVservername>
```

To specify a load balancing virtual server other than the default virtual server by using the NetScaler command line, at the NetScaler command prompt, type the following command:

```
bind cs vserver <csvservername> -policyName <policyname> [-priority <positive_integer>] -targetLBVserve
```

Application Firewall Profile Comment Support (Issue ID 0291927)

You can now add a comment to an archived application firewall profile to describe the contents and state of the archive more fully. The comment can be from 1 to 255 characters in length, and can contain letters, numbers, and most punctuation. In the configuration utility, you add a comment on the Export Application Firewall Profile dialog box, in the Comments text box. At the NetScaler command line, you add a comment by typing the following command:

archive appfw profile -comment "<string>"

For <string>, substitute the comment.

Rich policy support for SIP-UDP (Issue ID 0309107)

RULE based persistence now support SIP based policies as part of rule based persistence for SIP-UDP virtual servers. You can configure SIP based policies using the add lb vserver command. For example, the following code shows how to configure RULE based persistence for SIP-UDP virtual server:

add lb vserver sipvip1 SIP_UDP 10.102.27.68 5060 -persistenceType RULE -lbMethod CALLIDHASH -rule sip.re

Note: Only SIP request based policies are supported, rate limiting policies cannot be configured as part of the rule.

Option to Save the Config in Remote GSLB Sites after Config Synchronization (Issue ID 0287324)

The new Save Configuration option specifies that all participating nodes automatically save their configurations after synchronization. The master saves its configuration immediately before synchronization begins. Slave nodes save their configurations after the synchronization process is complete. A slave node saves its configuration only if it is successfully updated to match the master node's configuration. If synchronization fails on a slave node, you must manually investigate the cause of the failure and take corrective action.

To specify the option when using the NetScaler configuration utility to synchronize GSLB configurations, select the Save Configuration check box in the Save GSLB Configuration dialog box. If using the CLI, specify the saveConfig option for the sync gslb config command. The saveConfig option is mutually exclusive with the command's preview option.

SAML IDP and SP-Initiated Logouts Support for AAA-TM (Issue ID 0286268)

Support for SAML IDP- and SP-initiated logouts has been added to AAA-TM. An SP-initiated logout is performed when a user logs out of a AAA-TM session, but not when a user's AAA-TM session times out or when the 'kill aaa sessions' command is used. An IDP-initiated logout is performed when the IDP sends a 'clear session' request to the NetScaler appliance.

Searching NetScaler Entities in the Configuration Utility

You can use the 'Search' functionality to search for NetScaler entities displayed in the details or the data pane of the NetScaler configuration utility. If you want to perform string matching operations that are more complex than the operations that you perform with the simple CONTAINS search, you can use regular expressions.

Support for AES Ciphers on SSLv3 (Issue ID 0302510)

The following AES ciphers are now supported on the SSLv3 protocol.

1. Cipher Name: TLS1-AES-256-CBC-SHA

   Description: TLSv1 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1

2. Cipher Name: TLS1-AES-128-CBC-SHA

   Description: TLSv1 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1

3. Cipher Name: TLS1-DHE-DSS-AES-256-CBC-SHA

   Description: TLSv1 Kx=DH Au=DSS Enc=AES(256) Mac=SHA1

4. Cipher Name: TLS1-DHE-DSS-AES-128-CBC-SHA

   Description: TLSv1 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1

5. Cipher Name: TLS1-DHE-RSA-AES-256-CBC-SHA

   Description: TLSv1 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1

6. Cipher Name: TLS1-DHE-RSA-AES-128-CBC-SHA

   Description: TLSv1 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1

7. Cipher Name: TLS1-ADH-AES-128-CBC-SHA

   Description: TLSv1 Kx=DH Au=None Enc=AES(128) Mac=SHA1

8. Cipher Name: TLS1-ADH-AES-256-CBC-SHA

Description: TLSv1 Kx=DH Au=None Enc=AES(256) Mac=SHA1

Changes

Compression

- Issue ID 0299887: The output of the 'show cmp global' command is now similar to the output of the 'show' commands that you use for viewing global bindings for other types of default syntax policies. The 'show cmp global' command continues to display all the globally bound classic policies along with their priority values. But, for default syntax policies, the command displays only those global bind points to which policies are bound, along with a count of the number of policies that are bound to each of them.

  To view the details for a given global bind point, you can specify the bind point as the argument to the 'type' parameter. When you specify a global bind point, the command displays all the policies that are bound to the bind point, along with their priorities and Goto expressions. Classic policy bindings are not displayed if you specify a global bind point.

  Example:

  ```
  > sh cmp global -type RES_DEFAULT
  ```

  Advanced Policies:

  1. Policy Name: ns_adv_nocmp_xml_ie

     Priority: 8700

     GotoPriorityExpression:END

  2. Policy Name: ns_adv_nocmp_mozilla_47

     Priority: 8800

     GotoPriorityExpression: END

  3. . . .

     Done

     >

Load Balancing

- Issue ID 0302112: The use of SIP rate limiting expressions for rewrite policies is disabled to prevent the NetScaler from becoming unavailable.

SSL

- Issue ID 0316577: The SSL crypto card instrumentation is enhanced to provide more information on error status during initialization and at runtime.
- Issue ID 0325800: There are changes to the 'add ssl cipher' and 'bind ssl cipher' commands in NetScaler release 10 build 69.4. Now, there are two commands to create a cipher group and bind ciphers to this cipher group. The command to bind an SSL cipher to a virtual server or service has also changed. For more information about these changes, see http://support.citrix.com/article/CTX134118.

XML API

- Issue ID 0299194: The following XML APIs related to ACL and PBR features are deprecated:
  - unsetnspbr6_icmptype
  - unsetnspbr6_nexthopval
  - setnspbr_state
  - setnsacl_state
  - setnspbr6_state
  - setnsacl6_state

Bug Fixes

AAA Application Traffic

- Issue ID 0288572: On a NetScaler appliance with AAA-TM enabled and Kerberos/NTLM authentication configured, Likewise support fails to start, and the following error message is displayed: /libexec/ld-elf.so.1: Shared object 'libkrb5support.so' not found, required by 'libgssapi_krb5.so'

- Issue ID 0307258: When you create a AAA-TM profile by using the configuration utility, the configuration utility displays the global persistency settings as the settings that it assigned to the profile. However, instead of actually deriving the persistency values from the global persistency settings, it sets persistency for the profile to zero (0). You can verify this issue by typing the following command at the NetScaler command line:

  show tm sessionaction <profileName>

  You can fix the persistency settings for any AAA-TM profile that is affected by this issue by typing the following command at the NetScaler command line:

  set tm sessionAction <profileName> -persistentCookie ENABLED -persistentCookieValidity <positive_integ

  For <positive_integer>, substitute the number of minutes that the persistency cookie is to remain valid. Then, use the 'show tm sessionaction' command to verify your changes.
- Issue ID 0313931: On a NetScaler appliance that has AAA-TM enabled, if a user takes more than four minutes to finish authenticating and the AAA session expires, the user is unable to authenticate. When the user clicks the 'click here' link to return to the logon page, instead of being redirected to the logon page, the user is redirected to the 'Expired Session' page repeatedly.

- Issue ID 0314561: On a NetScaler appliance with AAA-TM enabled and single sign-on (SSO) configured, if a user who uses the Google Chrome browser takes more than four minutes to authenticate and the session expires, the browser displays a blank page instead of the Session Expired page.

- Issue ID 0322445: On a NetScaler appliance that has AAA-TM enabled and a load balancing virtual server configured to support 401 basic authentication, if a user sends a GET request that does not contain a Host header, the NetScaler appliance crashes.

Access Gateway

- Issue ID 90726/0249979: If you configure client certificate-based expressions for preauthentication or post-authentication scans and if users log on with a client certificate on an nCore Access Gateway model MPX 7500 appliance or higher, the scan fails and users cannot log on. This issue does not occur on the MPX 5500 appliance.

- Issue ID 0289662: If you disable split tunneling, When users log on with the Access Gateway Plug-in and try to make a Voice over Internet Protocol (VoIP) call to a mobile phone by using Cisco Unified Personal Communicator application, the call does not connect.

- Issue ID 0289686: If users connect with the Access Gateway Plug-in for Mac and then log off from the Web Interface, if users log on again within five minutes, the connection fails. This only occurs if you enable ICA proxy in Access Gateway.

- Issue ID 0290220: When users log on to Access Gateway with the Access Gateway Plug-in for Mac OS X, the home page is slow to appear or does not appear in the Web browser.

- Issue ID 0290976: When you configure a post authentication policy on Access Gateway and configure the policy to redirect the connection to the Web Interface if the endpoint analysis fails, when users log on with the Access Gateway Plug-in, if the user device fails the endpoint analysis scan, users receive the Access Gateway logon page instead of the Web Interface.

- Issue ID 0299406: If you configure a policy to restrict access to certain files, when users log on with clientless access and try to access the file, Access Gateway fails.

- Issue ID 0300221: When users log on to an nCore Access Gateway model MPX 7500 or higher, if there is high memory usage, the Access Gateway might fail. This issue does not occur on the MPX 5500.

- Issue ID 0301060: When you configure address pools, enable intranet IP addresses, and disable spillover, when users log on with the Access Gateway Plug-in and then try to log on from a second user device, the Transfer Login page appears. However, the message appears incorrectly as text only on a blank page. When users click 'Cancel', the button is disabled, rather than redirecting users to the logon page again.

- Issue ID 0301338: If a user password is longer than 31 characters, when users try to log on through the 'Access Gateway Plug-in logon' dialog box rather than through a Web browser, logon fails. A message appears stating that the user name and password are invalid.

- Issue ID 0301557: If users connect with the Access Gateway Plug-in and two network adapters have active connections on the user device, DNS resolution does not occur and users cannot access internal resources. If users disable one network adapter, users can then access internal resources.

- Issue ID 0301799: Access Gateway might not release all user sessions, which results in maximum usage of the licenses. When this occurs, users cannot log on and you must restart Access Gateway.

- Issue ID 0302268: After the preauthentication scan passes and users log on, if an internal processing error occurs, Access Gateway fails.

- Issue ID 0302490: If users log on with Receiver for Chromebook through Access Gateway, when users log off, Access Gateway does not release the session. Users must close the Web browser to log on again.
- Issue ID 0303265: If servers in the internal network return a UDP packet with zero length, Access Gateway fails.
- Issue ID 0306346: When users log on to the configuration utility, the following issues occur:
  - When using an Internet Explorer 8 Web browser, a blank page appears.
  - When using a Firefox 11 Web browser, many features in the navigation tree do not appear.
  - When using a Google Chrome Web browser, the only features that appear in the navigation tree are System, Network, DNS, SSL, VPN, and AppExpert.
- Issue ID 0320493: If your authentication policies include the rules REQ.SSL.CLIENT.CERT.EXISTS and REQ.SSL.CLIENT.CERT.NOTEXISTS, and users log on with a smart card, the following might occur:
  - If smart card authentication fails, users are redirected to the Web Interface and prompted again for the smart card credentials.
  - If users do not enter smart card credentials, they are redirected to the Web Interface and prompted for their user name and password in order to authenticate with RADIUS.

AppFlow

- IssueID 0301461 (nCore): If you enable the 'clientTrafficOnly' parameter when the AppFlow feature is enabled, the NetScaler appliance fails. By default, the 'clienttrafficonly' parameter is disabled.
- Issue ID 0302578 (nCore): If you enable AppFlow when the NetScaler device is in transparent mode, or when the load balancing virtual servers use wildcards for the IP address and port to dynamically learn the backend services, the NetScaler device fails.

Application Firewall

- Issue ID 51944/0219171: Imported application firewall objects -- such as WSDLs and XML Schemas -- cannot be removed from the NetScaler appliance by using the 'clear config' command. You must explicitly remove these objects. To remove an imported object by using the NetScaler command line, open a Unix shell and type 'rm <objectFilename>'. To remove an imported object by using the configuration utility, select the object, and then click Remove.

- Issue ID 85151/0245424: You can now add a comment to an application firewall profile to describe it more fully. The comment can be from 1 to 255 characters in length, and can contain letters, numbers, and most punctuation. In the configuration utility, you add a comment on the Create Application Firewall Profile dialog box or Configure Application Firewall Profile dialog box, General tab, in the Comments text box. At the NetScaler command line, you add a comment by typing the following command:

  ```
  set appfw profile -comment "<string>"
  ```

  For <string>, substitute the comment.

- Issue ID 87741/0247559: Handling of half-width and double-width characters by the HTML SQL Injection check transformation feature has been modified to ensure that these characters are identified as special characters, preventing inappropriate blocking and transformation.

- Issue ID 0284784: When a web site sends a MIME-encoded web form to a user with the MIME boundary enclosed in double quotations, and the user returns the web form as a POST request, the application firewall resets the connection with a reset code of 9845.

- Issue ID 0291389: When you configure an audit policy to send the application firewall logs to a remote Syslog server, the logs do not contain the profile name and URL of the connection that generated the log, and field names and values are incorrect. If you configure the audit policy to create local logs, the missing information is included in the logs.

- Issue ID 0300223: In the configuration utility, 'Application Firewall Profiles' pane, when you import a profile, the configuration utility is not automatically refreshed, giving the impression that the import failed. The profile is actually imported successfully. To see it in the Profiles list, click 'Refresh'.

- Issue ID 0300383: On a NetScaler classic build that has the application firewall learning feature enabled, under heavy load the configuration utility can become unavailable and the NetScaler can freeze or hang.

- Issue ID 0300465: When upgrading from the NetScaler 9.3 to the NetScaler 10 release, all signature rules, SQL special strings, and SQL keywords are now automatically upgraded to the new schema.

- Issue IDs 0301817 and 0302295: Local safe object signature rules work only if the Location is set to HTTP_RESP_BODY, and maxLength is defined.

- Issue ID 0302282: If a local safe object signature rule is defined, and the signatures object is bound to a profile, the safe object check is not run on traffic that is processed through that profile.

- Issue ID 0302368: In the 'Manage Learned Rules' dialog box, you might not be able to deploy or remove certain learned relaxations that contain special characters.
- Issue ID 0303057: If a log for a Transform action has missing parameters, the fields that contain those parameters are not clickable in the Syslog Viewer, and that log cannot be deployed to create a new rule or relaxation.
- Issue ID 0307082: When the NetScaler appliance sends an HTTP/1.0 100-Continue response on behalf of a protected web server, it now also sets the TCP Push flag in the response packet. This change resolves certain performance issues that might have been encountered when enabling the application firewall for some XML-based web services.
- Issue ID 0307542: If a hostname greater than 93 characters in length is assigned to a NetScaler appliance that has the application firewall enabled, the application firewall learning feature crashes.
- Issue ID 0309289: When a client sends a chunked POST request to an application firewall-protected web server, the request might not be correctly transmitted to the web server, resulting in a failed connection.
- Issue ID 0319787: On a NetScaler appliance with the application firewall feature enabled, the comment stripping feature does not correctly parse web pages that have an HTML comment that is terminated with two hyphens, a space, two more hyphens, and a greater-than symbol (-- -->). In other words, you cannot have a string consisting of two hyphens and a space immediately preceding the usual comment termination string (-->). If you do, the comment stripping feature does not detect the final two hyphens and greater-than symbol as a comment terminator. The comment stripping feature therefore strips all content that follows the missed comment terminator.
- Issue ID 0320145: If a user requests a URL from an application-firewall protected web site, and the requested web page has embedded URL links that contain hash (#) characters, the request might trigger a Start URL check violation. If blocking is enabled for the Start URL check, the request might be blocked.

Cluster

- Issue ID 0276162: Cluster commands are not propagated from the configuration coordinator to other nodes, when you log on to the cluster IP address using the Password Authentication mechanism. However, the commands are propagated when you log on to the cluster IP address using the Keyboard Interactive mechanism.
- Issue ID 0290504: You cannot form a cluster of NetScaler appliances by using the configuration utility, if you are accessing the configuration utility over a secure channel (https instead of http.)
- Issue ID 0302924: In the configuration utility, the NetScaler appliances that are added to the cluster by using the 'Discover NetScalers' option, are not automatically saved and rebooted.
- Issue ID 0318723: When a new node joins the cluster or an existing node is rebooted, the ACL, ACL6, SIMPLEACL, and SIMPLEACL6 configurations with TTL value are not automatically synchronized on that node.

Command Line Interface

- Issue ID 0262838: The CLI man page for the set dns parameter command has the following errors:
  - It displays 'ENABLED' as the default value for the 'cacheRecords' parameter. The possible values are only 'YES' and 'NO', and the default value is 'YES'.
  - It displays NS_FOUR as the default value for the 'resolutionOrder' order parameter. The possible values are only 'OnlyAQuery', 'OnlyAAAAQuery', 'AThenAAAAQuery', and 'AAAAThenAQuery'. The default value is 'OnlyAQuery'.

Configuration Utility

- Issues IDs 0244945, 0245825, and 0273344: When viewed in Internet Explorer version 8 or 9, the Dashboard page has several display issues (for example, excessive scroll bars, inconsistent column width, horizontal scroll bar missing from the Vserver view).
- Issue ID 0299883: When users access NetScaler using the configuration utility, the following issues are observed:
  - When you select a policy on the DNS Policies page, the Global Bindings button becomes inactive.
  - On the 'Virtual Servers' page, under 'Load Balancing', the header bar in the details pane moves off the page if you scroll down.
  - The configuration difference command produces an error message: Secondary NS not found.
- Issue ID 0300376: If you create an SSL service by modifying an existing virtual server and set some parameters in the 'Advanced' tab, the service is not created. The service is created if you do not set any advanced parameters or do not click the 'Advanced' tab.
- Issue ID 0302742: If you use the configuration utility to bind a compression policy (for example, app_cmp) to an AppExpert application, the following error message appears: Policy 'app_cmp' cannot be inserted. It does not have expression with advanced syntax.
- Issue ID 0303492: Creating an IP entity does not update the table that displays information about the configured IP addresses.
- Issue ID 0303494: Cache update causes issues with removal of an IP object.
- Issue ID 0303495: If you remove an IP object, cache-update issues cause Internet explorer to display unknown error.
- Issue ID 0303504: You cannot use the numeric keypad to specify values in the following text boxes:
  - Destination IP Address, in either the 'Create SNMP Trap Destinations' or the 'Configure Trap Destinations' dialog box.
  - IP Address, in the Create SNMP Managers dialog box.
- Issue ID 0303910: The Configuration page does not load if accessed from Internet Explorer 9 on a client machine running JRE 1.6 build 14.
- Issue ID 0308459: In 'Enable/disable service group member' view, the 'Enable' and 'Disable' buttons are inactive when the state of a service group member is one of the following - 'GOING OUT OF SERVICE', 'DOWN WHEN GOING OUT OF SERVICE' or 'GOING OUT OF SERVICE (graceful)'.
- Issue ID 0314258: When you modify any PBR rule from the configuration utility, the NetScaler appliance changes the APPLIED status of the PBR to NOTAPPLIED.
- Issue ID 0323197: An HTTP monitor with extended 'respCode' range cannot be configured through the configuration utility. If it is configured through the CLI, an error occurs when it is viewed in the configuration utility.

- Issue ID 0323890: An error occurs when a user tries to remove the monitors from a load balancing service by using the 'Remove' button in the configuration utility's Configure Service window.

Content Switching

- Issue ID 0308757: A TCP content switching virtual server with a wildcard port fails to respond to clients with a SYN-ACK. Consequently, the content switching functionality fails for the virtual server.

DataStream

- Issue ID 0303980: A monitor of type MSSQL becomes unavailable if you replace the existing query with a shorter query.

HTML Injection

- Issue ID 0302088: When HTML Injection is enabled for web forms that use the 'GET' method, ES monitoring does not function properly.

Integrated Caching

- Issue ID 0288716 (Cluster): In cases, where there is a delay in processing the cache invalidation request originating from other cluster nodes, if the client sends a request before the cache invalidation request is processed on the node, the cache will serve old content.

Load Balancing

- Issue ID 89129/0248646: For non-HTTP load balancing virtual servers for which rule based persistence has been configured, the appliance does not automatically refresh the session time-out setting during a file download. Therefore, if the download is not completed before the session times out (and another request does not arrive before the session times out), the time-out setting is not refreshed, and requests that arrive during what would otherwise have been the extended time-out interval are forwarded to whatever server is selected by the configured load balancing method.

  A consequence of this behavior is failure to accelerate some Repeater Plug-in connections in a WAN optimization configuration. If a persistence session that was created for a request from a Repeater Plug-in expires before the complete response is sent to the client, the next request from the Repeater Plug-in is sent to a different Branch Repeater appliance and is therefore not accelerated. When that happens, the Branch Repeater graphical user interface indicates that the reason for the connection not being accelerated is 'Not enough room left in the TCP packet header to append unit specific options (5).'

- Issue ID 0278377 (nCore): Cache policy labels cannot be bound to MYSQL or MSSQL virtual servers.

- Issue ID 0285672: When using load balancing of Branch Repeaters in a cluster setup, there is no response from the server and the request hangs.

- Issue ID 0289339: Service group members that are configured to scale automatically are not synchronized correctly with the secondary appliance in a high availability pair. The issue can lead to appliance failure during a failover event.

- Issue ID 0304847: In the load balancing monitor structure in the XML API, the 'flags' field is now deprecated.

- Issue ID 0305045: The WI-Extended monitor sends probes to port 80 regardless of the port number for which it is configured.

- Issue ID 0309954: A GSLB virtual server becomes unavailable if you use the same IP address as the public IP address for both a local and a remote GSLB service, bind monitors to the services, and then bind the services to the virtual server.

- Issue ID 0318838: A NetScaler policy or action fails if it uses a SIP expression that is based on the Contact header. For example, a rewrite action does not work if it is configured to rewrite the Contact header.

NetScaler SDX Appliance

- Issue ID 88556/0248194: When provisioning a NetScaler instance, if you have entered invalid NetScaler settings for any of the IP address, Netmask, or Gateway parameters, you cannot modify the values for those parameters.

- Issue ID 90586/0249864: Log on to the Management Service user interface fails after 25 days.

- Issue ID 0289151: If you provision a NetScaler VPX instance with approximately 12288MB (12GB) of memory and then upgrade the instance, the upgrade operation fails and the following error message appears:

  ERROR: NetScaler on nCore VPX requires minimum 2 Gigabytes and 2 CPUs to start.

- Issue ID 0310014: If you have provisioned a NetScaler VPX instance running release 9.3 on a NetScaler SDX appliance running release 10, and the instance is restarted, the existing session between the Management Service and the VPX instance expires and an error message appears if you try to modify any settings on that instance after it restarts.

- Issue ID 0313155: NTP synchronization might fail if you add a new NTP server by using the Management Service user interface because the default contents of the ntp.conf file are not flushed.

NetScaler VPX Appliance

- Issue ID 0302377: If you install a NetScaler VPX virtual appliance on Microsoft Server 2008 R2 by using Hyper-V Manager, or if you install a NetScaler VPX virtual appliance on VMware ESX 3.5 or 4.0, you are not prompted to specify the IP address, subnet mask, and gateway. The appliance starts with the default IP address of 192.168.100.1.

Networking

- Issue ID 0243105: When there are ECMP routes for a prefix, for every new route addition or deletion, the NetScaler appliance withdraws all the UP routes and adds them back again to its routing table. This results in a period of time when there are no routes to the prefix.
- Issue ID 0277297: NetScaler APIs do not display some of the attributes that are displayed in the output of 'show connectiontable -detail full' command.
- Issue ID 0300820: When the NetScaler appliance receives an unpredicted flow of SYNs, it blocks the connect system calls used by OSPF daemon. This causes delay in sending out the hello packets resulting in adjacency failure.
- Issue ID 0302613: When an OSPF connection times out, the NetScaler appliance removes and applies back the router configuration. This causes an adjacency flap which momentary drops all the advertised routes.
- Issue ID 0305420: If the NetScaler appliance receives any traffic which hits a virtual server of type ANY then only for the first packet of this traffic the TTL value set to 255 and for the remaining packets, belonging the same session, the TTL value remains same. This applies to even fragment packets, where only for the first fragment of the packet the TTL value is set to 255 and for the remaining fragments the TTL value is unchanged.
- Issue ID 0311243: When a virtual server, which has a listen policy bound to it, receives IPv4 fragments of a request that evaluates the policy to TRUE, the NetScaler appliance becomes unresponsive while performing service lookup on the received IPv4 fragments
- Issue ID 0312412: The command 'sh ip ospf <1-65535> database', in the VTYSH command prompt, displays the database for all the OSPF processes instead of just for the process id specified.
- Issue ID 0318668: A virtual server of type ANY drops the IPv6 ECHO reply if the ECHO request didn't pass through the appliance and the related IPv6 to IPv4 mapping is not present in appliance.

Platform

- Issue ID 0275149 (nCore): On a NetScaler appliance that has LACP configured and interface speed set to AUTO, if the link speed on one of the interfaces in a channel is reduced after autonegotiation with the device at the other end, the interface is treated as DOWN by the LACP channel on the peer device. However, the NetScaler appliance does not identify the new reduced link speed and continues to treat the interface as UP.

Policy

- Issue ID 0291487: NetScaler appliances running version 9.2 build 52.1 or later and have a large number (in the hundreds) of policy bindings can experience performance issues on 'save ns config' and 'show config' operations. This can lead to interruption in services.
- Issue ID 0291975: The SYS.VSERVER('<vserver_name>').THROUGHPUT expression returns an incorrect throughput value.
- Issue ID 0311268: You cannot add a rule of the form 'HTTP.REQ/RES.BODY(<num>).CONTAINS(<string2>)' where <string2> has the property that its length is greater than the length of <string1>. <string1> is already existing string in the already configured policy expression 'HTTP.REQ/RES.BODY(<num>).CONTAINS(<string1>)'.

  For example, the second command provided below might not succeed if there exists some request for which the evaluation of rule in cs_example is in progress.

  -> add cs policy cs_example -rule 'HTTP.REQ.BODY(1000).CONTAINS("MyLengthIs12")
  -> add cs policy cs_example_break -rule 'HTTP.REQ.BODY(1000).CONTAINS("MyLengthIsBIG15")

Reporting

- Issue ID 0313793: You can now include period (.), colon (,), and hyphen (-) special characters in report titles.

SNMP

- Issue ID 0309930: The SNMP OID for vsvrCurSslVpnUsers is getting counter values only from core 0.

SSL

- Issue ID 0316577: The SSL crypto card instrumentation is enhanced to provide more information on error status during initialization and at runtime.

Stream Analytics

- Issue ID 0307283: NetScaler supports a maximum of 500 stream session records. Stream records beyond the maximum supported value are not tracked. The statistics command, 'stat stream identifier', displays a maximum 500 stream records.

System

- Issue ID 93169/0257092 (nCore): NetScaler nCore appliances now support keep-alive for TCP connections. When this feature is enabled, with the default settings, the appliance probes any TCP connection that has been idle for 15 minutes. If the appliance does not receive a response from the peer within 75 seconds, it sends a second probe. If no response to that probe is received within 75 seconds, the appliance sends a third, final probe. If no response to the final probe is received within 75 seconds, the appliance resets the connection.

  By default, this feature is disabled. In addition to enabling the feature, you can change the default values for connection idle time, number of probes to send to the peer, and the interval at which to send probes. In the CLI, use the following command to change the default settings:

  set ns tcpProfile <name> [-KA ENABLED] [-KAconnIdleTime <positive_integer>] [-KAmaxProbes <positive_

  In the configuration utility, you can change the settings in the System > Profiles > TCP Profiles > Add TCP Profile or Configure TCP Profile dialog box.

- Issue ID 0270163: When the NetScaler appliance runs processes such as gzip, the usage of the management CPU increases. Hence, high CPU usage alerts may get generated even though the packet engines are not actively processing packets.

- Issue ID 0275501: A user can view all of the virtual servers configured on the NetScaler appliance, even though the user is bound to a command policy that has a condition for restricting the user to view only a set of virtual servers.

- Issue ID 0285015: Requests buffers larger than 24KB lead to buffer overflow and result in the web log module not working.

- Issue ID 0302004: For load balancing virtual servers that have SOURCEIP persistence configured, client IP header insertion might fail for HTTP CONNECT requests sent to that virtual server.

- Issue ID 0319417: Server response in which the HTTP header spans more than 16 nsbs is reset even if the 'drop invalid requests' flag is disabled.

Web Interface

- Issue ID 86538/0246528: The following dialog boxes under 'Upload Plugins' available in the 'Web Interface' pane of the configuration utility do not work as expected:

  - Windows Client

  - Linux Client

  - Macintosh Client

- Issue ID 0322207: In a high availability setup, delays in Apache Tomcat start-up might prevent the propagation of web interface configurations to the secondary appliance. As a result, the web interface configurations are not available when the secondary appliance becomes primary.

XML

- Issue ID 0304314: SOAP requests that do not conform to a WSDL are not handled properly by the XML validation module.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberoes authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, adn then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.

- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

- Issue ID 0327114: On a NetScaler appliance with NetScaler 10 build 69.4 nc installed, if you use the configuration utility to configure authentication on a load-balancing virtual server, the following error message appears:

  No Authentication Host specified

  The configuration utility then removes the authentication host from the configuration. This behavior occurs regardless of whether you are configuring authentication host settings on the virtual server for the first time, or modifying existing authentication host settings on the virtual server.

Access Gateway

- Issue ID 90722/0249975: When users log on with the Access Gateway Plug-in, the 'File Transfer' tab on the Access Interface is available, but the 'File Transfer option' is not available if users right-click the Access Gateway icon in the notification area.

- Issue ID 92543/0251596: After you configure Access Gateway to provide user connections through Citrix Receiver, when users right-click the Receiver icon in the notification area, the Log on option does not appear. Users must connect by using the Web browser or they must right-click the Receiver icon and then, depending on the version of Receiver they are using, click About or Preferences from the Receiver menu and Plug-in Status or Advanced from the Receiver panel. You can also enable the log on option to appear when users right-click the Receiver icon by adding the following settings in the registry:

  - Add the Receiver key (if the key does not already exist) under the following registry locations:

    - `HKEY_CURRENT_USER\Software\Citrix\`

    - `HKEY_LOCAL_MACHINE\Software\Citrix\`
  - Add the Inventory key in the following registry locations:

    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`

    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`
  - In the Inventory key, configure the following **REG_SZ** values:

    - **VPNAddress**. Provide the value as the Web address for the Access Gateway appliance; for example, https://<AccessGatewayFQDN>.

    - **VPNPrompt1**. Provide the value as 'UserName'.

    - **VPNPrompt2**. Provide the value as '*Password'.

      Note: To mask the password, enter an asterisk (*) before the word.

      In addition, if you configure double-source authentication that requires authentication with LDAP plus RSA authentication, you need to also add the following as **REG_SZ**:

    - **VPNPrompt3**. Provide the value as '*Passcode'.
- Issue ID 0261547: When you enable Access Gateway as a reverse proxy and you enable basic preauthentication and post- authentication scans, as well as encryption and client choices, when users log on with the Access Gateway Plug-in, the preauthentication scan passes, but the post-authentication scan fails.

- Issue ID 0275079: When users access applications published on XenApp, each user consumes multiple Access Gateway licenses per application. Instead, one session ID should be shared across the applications the user accesses. As a result, users exceed their allocated license count and an SSL error occurs.

- Issue ID 0285995: If you configure Access Gateway to assign an intranet IP address to user devices that connect to Access Gateway, when users log on with the Access Gateway Plug-in, the secure DNS dynamic update does not occur and the intranet IP

address is not registered with the DNS Server.

- Issue ID 0288469: After you configure a virtual server to use the Access Gateway Plug-in for Java, when users log on with the Access Gateway Plug-in by using a browser that has a 64-bit Java Runtime Environment (JRE) installed, the plug-in fails to establish a connection.

- Issue ID 0291264: If you create a Web Interface 5.4 site and enable authentication through Access Gateway, and you enable single sign-on with a smart card to the Web Interface that enables smart card pass-through, when users log on with the Access Gateway Plug-in, the users' desktops are not listed on the Web Interface.

- Issue ID 0291821: If you create a Web Interface 5.4 site and enable authentication with a smart card through Access Gateway, and you configure the 'Single Sign-on Domain' on the 'Published Applications' tab using the format domainname.com instead of domainname, when users start a published application or desktop, authentication fails.

- Issue ID 0292005: When users connect with clientless access and try to download a file larger than 1 gigabyte (GB) from the file share on the home page, as the file is downloading, if an upload is attempted, the download process fails but the upload continues.

- Issue ID 0298971: When users log on with the Access Gateway Plug-in for Java and the Web Interface opens in Internet Explorer 9, if users do not turn on Compatibility View in Internet Explorer, when they click a published application, the following error appears: Resource shortcuts are not available.

- Issue ID 0299515: If you configure an intranet IP address on Access Gateway, when users connect with the Access Gateway Plug-in on a computer running Windows XP Service Pack 3 and try to access a CIFS share hosted on a computer in the secure network, users receive an error that the share is inaccessible.

- Issue ID 0300511: When users log on using clientless access and click a bookmark from the home page to open a Distributed File Share (DFS), if the target folder resides on a different computer than the computer where the domain DFS server resides, the share does not open.

- Issue ID 0308733: If you configure Access Gateway with additional appliances in which global server load balancing (GSLB) is enabled, when users log on with the Access Gateway Plug-in, occasionally the connection times out, a time-out error appears, such as 'Your Citrix Access Gateway session timed-out and you are not connected,' and the session disconnects.

- Issue ID 0309017: When you configure a preauthentication and post-authentication policy with an expression to scan a user device for a file, Access Gateway does not check for expression syntax. As a result, Access Gateway accepts inappropriate syntax configuration and the scan fails.

- Issue ID 0319607: If an authentication server and Access Gateway reside in the same domain, the appliance may fail.

- Issue ID 0319901: If you enable Integrated Caching and Web Interface on Netscaler on an Access Gateway appliance, and then change the URL for the Web Interface, Access Gateway might fail.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

Application Firewall

- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked. To work around this issue, if you configure Sessionless URL Closure, set Validate Referer Header to Off.

- Issue ID 0299940: The change profile type command does not work correctly.

  - If you try to change a profile type to Web 2.0, the profile type remains HTML.

  - If you try to change a profile type to XML, the Profile Type field disappears completely.

  When you use the configuration utility to change the profile type, the profile type is actually changed correctly, but the display is incorrect. When you use the NetScaler command line, the actual profile type is set as shown above.

- Issue ID 0301813: When deploying a learned Cross-Site Request Forgery relaxation from the Syslog Viewer, the configuration utility does not deploy the relaxation, but displays the following error message: 'CSRF Tag validation failed'.

- Issue ID 0302294: Learned relaxations are sometimes not removed from the review list after they have been deployed. To manually remove a learned relaxation that has already been deployed, in the Manage Learned Rules dialog box select the relaxation and then click 'Skip'.

- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported when importing signature rules. WAS 2.0 scan reports are not supported.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

- Issue ID 0328353: When you use the configuration utility to bind a cache redirection policy to a cache redirection virtual server, the policy is added to the content switching (CSW) policy tab instead of cache redirection (CRD) policy tab. If you try to resolve this issue by using the CR virtual server wizard, the following error message appears: 'Please specify Target.'

- Issue ID 0330033: Tabs for filter/compression policy bindings are not displayed for a cache redirection virtual server, and it is not possible to bind those policies to a cache redirection virtual server.

- Issue ID 0330139: If you use the configuration utility to unset a cache virtual server for a cache redirection virtual server, the process fails and the following error message appears: invalid argument.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0251463: When you click the Applications node in AppExpert, the configuration utility throws a null pointer exception. The issue occurs sporadically.

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278097: In the configuration utility, if you click Application Firewall in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0298686: If the details pane contains too may records to display on one screen, the header row moves off the screen if you scroll down.

- Issue ID 0300506: On the MPX 17000 platform, if you use the configuration utility to upgrade from release 9.2 build 55.5 to release 10, the appliance does not restart automatically after the upgrade.

  Workaround: Restart the appliance manually by using the command line or the configuration utility.

- Issue ID 0303279: In the configuration utility, in the Rewrite Policies pane, clicking Add does not display the Create Rewrite Policy dialog box but disables the main configuration utility window.

- Issue ID 0311358: The NetScaler configuration utility fails to load when accessed from Internet Explorer version 7 browser running on Windows 2003 or Windows XP.

  Workaround: Use Internet Explorer version 8 and above.

- Issue ID 0319061: The configuration utility does not throw the 'Feature not supported' prompt when configuring the following unsupported features on a NetScaler cluster: Bridge groups, Network Bridge, VMAC6, and FIS. This issue is observed only in a cluster setup.

- Issue ID 0322821: When the SRADV (Static Route Advertisement) mode is ON, the static routes which are not explicitly disabled for advertisement will be advertised using all the routing protocols. However, the advertised protocols column for route in the configuration utility does not show any protocol list. This issue is observed only in a cluster setup.

- Issue ID 0322894: The configuration utility displays an inappropriate error message when adding a forwarding session that has an invalid subnet mask. This issue is observed only in a cluster setup.

- Issue ID 0322914: When the IP is not resolved for a hostname based SNMP manager, the 'Resolved IP' column of the SNMP Manager table is shown as blank instead of 'Unresolved IP'. This issue is observed only in a cluster setup.

- Issue ID 0323175: The configuration utility displays a negative value for the index of the data set or pattern set, when the index is set to its maximum value. The command line

interface displays the correct value.

- Issue ID 0325400: After adding a local authentication policy by using the configuration utility, the request profile field is showing blank. By default, the request profile must be Local. This issue is observed only in a cluster setup.

- Issue ID 0326354: In System > Settings > Change global system settings, regardless of the base threshold value configured for surge protection, the value is displayed as 0. This issue is observed only in a cluster setup.

  Workaround: You can view the base threshold vale by using the 'show ns spParams' command.

- Issue ID 0326018: The dashboard does not display the Precision Time Protocol (PTP) counters for the cluster node. This issue is observed only in a cluster setup.

  Workaround: PTP counters can be viewed by using the 'stat cluster node' command.

- Issue ID 0327136: The configuration utility does not allow you to set the 'Max Clients' parameter of a service to its maximum value of 4294967294. This issue is observed only in a cluster setup.

  Workaround: You can set the maximum value by using the “set service” command.

- Issue ID 0327551: In the configuration utility, all features appear to be enabled even when the features are disabled.

- Issue ID 0328660: In the configuration utility, when you view the virtual server persistence sessions, a persistence type setting of DIAMETER is displayed as SOURCE IP.

- Issue ID 0328715: In the configuration utility, the details of the monitor bound to a service do not include response codes for a monitor of type DIAMETER.

- Issue ID 0328844: While configuring the OCSP responder through the configuration utility, the default value of the HTTP response timeout is erroneously taken as 0ms. The default value of the HTTP response timeout must be 2000ms. This issue is observed only in a cluster setup.

  Workaround: You must explicitly set the HTTP response timeout in the configuration utility.

- Issue ID 0329154: In System > Auditing > Recent audit messages, when you set number of audit messages to be displayed to 256 (maximum allowed value), a 'Value entered is out of range' error message is displayed on clicking Refresh. This issue is observed only in a cluster setup.

- Issue ID 0329826: If you use the configuration utility to view the license for features, warning messages are seen for the features that are licensed but not supported. This issue is observed only in a cluster setup.

- Issue ID 0332768: On Internet Explorer 8, the configuration utility does not show the pop-up for installing the JRE plugin.

- Issue ID 0332795: On systems that have JRE 1.6.0_24 and 1.7.0_06, the configuration utility cannot load the Java applet. Therefore, you cannot perform any operations on the configuration utility.

Workaround: Uninstall JRE 1.6.0_24 and 1.7.0_06 and install JRE 1.6.0_31.

- Issue ID 0332876: When you use the configuration utility to change the password of a user, the Change Password dialog displays encrypted password in the Password and Confirm Password fields.
- Issue ID 0333026: On a system running the Windows 7, 64-bit operating system, the configuration utility cannot load the Java applet. Therefore, you cannot perform any operations on the configuration utility.
- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Cloud Gateway

- Issue ID 0327119: When you create policy rules from the configuration utility, an error occurs and the policies are not configured.

Content Switching

- Issue ID 0330290: You cannot use the configuration utility to bind a content switching policy to a content switching virtual server if the policy is configured with only a domain value. The bind fails, and the following error message appears: 'Priority cannot be specified for URL-based content switching policy.'
- Issue ID 0331029: If you use the configuration utility to open a content switching virtual server that has a default policy bound to it, the process fails and the following error message appears: No Such Resource.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated.

Domain Name System

- Issue ID 0291053: Under the following sequence of events, the NetScaler appliance sends the client a cached NXDOMAIN response instead of the IP addresses that are configured in the DNS action for response rewrite:

  1. A security-aware name server sends the appliance a DNSSEC-enabled NXDOMAIN response for a non-existent domain. The appliance, which is designed to not rewrite DNSSEC-enabled responses, relays the negative response to the client without modifying it. The appliance also caches the response.

  2. A client sends the appliance a request for the same domain, but it does not set the DNSSEC OK EDNS header bit.

  This behavior is expected, and ensures that security-aware and security-oblivious clients receive the same response.

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0324486: When creating a local GSLB site in the NetScaler configuration utility, if you set the Trigger Monitors option to MEPDOWN, the GSLB site does not appear in the details pane until after you click Refresh.

- Issue ID 0326001: If a GSLB virtual server's primary and backup GSLB methods are both set to round trip time (RTT) or static proximity and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT or static proximity as the primary GSLB method, do not use the same method as the backup GSLB method.

- Issue ID 0328911: When configuring monitoring for a GSLB service by using the NetScaler configuration utility, if you include monitors that cannot be used with GSLB services (for example, ARP monitors) along with monitors that can be used with GSLB services (for example, TCP monitors), the configuration utility displays an error message for the invalid monitor bindings, but the valid bindings succeed. When you unbind an invalid monitor from the service, the message 'Error' is displayed. No further information is provided in the message.

Load Balancing

- Issue ID 0248750: NetScaler now supports dynamic selection of a load balancing virtual server. The lb virtual server is identified at the run time using an expression in the content switching action.

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the 'show lb persistentSessions' CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 91711/0250846: If the string (or 'token') that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR('string2').AFTER_STR('string1') if the string that is enclosed by 'string1' and 'string2' is not larger than 64 KB.

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

- Issue ID 0324061: When you configure a SIP-UDP load balancing virtual server by using the NetScaler command-line interface, the default setting for persistence type is CALLID. However, when you use the configuration utility to configure a SIP-UDP virtual server, the default setting for persistence type is NONE.

- Issue ID 0330276: The virtual router IDs (VRIDs) that are configured on the NetScaler appliance are not available in the Virtual Router ID list in the Create IP and Configure IP dialog boxes (Network > IPs > Add/Open). Consequently, you cannot use the configuration utility to bind a VRID to a virtual server.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type: #/etc/rc.d/svmd restart

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.
- Issue ID 0299716: In a cluster setup, the 'bind vlan' command throws an error when interface and IP address are specified together.

  Workaround: Bind the interface and IP address individually, by using separate 'bind vlan' commands.
- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command 'set ptp -state disable' and configure NTP to synchronize the time across the cluster nodes.
  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0327173: The ciphers bound to an SSL virtual server are not displayed in the configuration utility.

System

- Issue ID 0325665: An unrelated error code is displayed on executing the 'set filter prebodyinjection/postbodyinjection' commands.

- Issue ID 0327118: In the configuration utility, the minimum and maximum values allowed for number of audit messages is incorrect. The maximum and minimum values displayed are 255 and 0, but the correct values are 256 and 1.

Web Interface

- Issue ID 0306731: If the Rewrite feature is not enabled, the Enable access through receiver client option for a Web Interface(WI) site does not work. This is because the functionality of the option depends on some rewrite policies on the appliance.

- Issue ID 0315502: The Configuration Utility displays an error message when you try to disable the Web Interface feature.

- Issue ID 0315951: If the Responder feature is not enabled, the Make Site Path Case Insensitive option for a Web Interface(WI) site does not work. This is because the functionality of the option depends on some Responder polies on the appliance.

  Workaround: Enable the Responder feature before you select the Make Site Path Case Insensitive option for a WI site.

- Issue ID 0324373: In the Web Interface (WI) configuration wizard, for a WI site in gateway direct mode, the state of the Enable Access through Receiver Client option is shown selected even when there are no rewrite policies bound to the selected Access Gateway virtual server.

- Issue ID 0331904: In the Web Interface (WI) configuration wizard, the Enable Access through Receiver Client option remain selected even when you try to clear the option.

Enhancement Releases

This section describes the enhancements, changes, bug fixes, and known issues provided in the enhancement releases of the Citrix® NetScaler® and Citrix® NetScaler® SDX.

Build 75.7007.e

Release version: Citrix NetScaler release 10.e build 75.7007.e

Replaces build: None

Release date: July 2013

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Bug Fixes
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 75.7. The release notes are available in the Build 75.7 section on Citrix eDocs.
- The enhancements, bug fixes, and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Enhancements

CloudBridge Release 7.0

- To learn about the enhancements in CloudBridge Release 7.0, see the "Enhancements" section of the CloudBridge 7.0 release notes at Citrix CloudBridge 7.0 Release Notes.

Bug Fixes

AAA Application Traffic

- Issue ID 0372362: When Kerberos Constrained Delegation is configured with a content switching virtual server, the NetScaler appliance might hang or crash. The cause is a GET request with multiple authorization headers. (Only one authorization header is expected.)

- Issue ID 0387076: On a NetScaler appliance with AAA enabled and Kerberos Constrained Delegation single sign-on configured, after several single sign-on requests are successfully authenticated, the virtual server principle can unexpectedly become blank. When this happens, subsequent authentication requests fail.

Known Issues and Workarounds

Application Firewall

- Issue ID 0363711: On a NetScaler appliance that has AAA, Kerberos authentication, KCD, and MSSQL monitor enabled, each monitor probe causes a memory leak that eventually results in the NetScaler appliance experiencing an out-of-memory condition that requires a restart to clear.

NetScaler VPX on AWS

- Issue ID 0337614: Custom scriptable monitors do not work on NetScaler VPX on AWS.
- Issue ID 0340395: While configuring HA between two VPX instances in AWS, if you first configure HA on the VPX instance with a single ENI, HA configuration does not work as expected.

  Workaround: Configure the instance with two or more ENIs before configuring HA on the instance with one ENI.
- Issue ID 0344678: If you remove HA configuration from the primary instance first, HA configuration is not removed and causes the primary instance to reboot.

  Workaround: Remove HA configuration from the secondary instance first before removing HA configuration from the primary instance.
- Issue ID 0346689: In INC mode, HA configuration between two NetScaler VPX instances in AWS does not work properly.

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.
- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.
- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

Build 74.4006.e

Release version: Citrix NetScaler release 10.e build 74.4006.e

Replaces build: None

Release date: April 2013

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 74.4. The release notes are available in the Build 74.4 section on Citrix eDocs.
- The enhancements and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Enhancements

Offload DNSSEC Operations to the NetScaler Appliance

- Issue IDs 0246717 and 0249691: For DNS zones for which your DNS servers are authoritative, you can offload DNSSEC operations to the NetScaler appliance. When a DNS server sends a response, the appliance signs the response on the fly before relaying it to the client. The appliance also caches the signed response. Apart from reducing the load on the DNS servers, offloading DNSSEC operations to the appliance gives you the following benefits:

  - You can sign records that the DNS servers generate programmatically. Such records cannot be signed by routine zone signing operations performed on the DNS servers.

  - You can serve signed responses to clients even if you have not implemented DNSSEC on your servers.

  To configure DNSSEC offloading for a zone, you add the zone to the NetScaler appliance and set the zone's Proxy Mode and DNSSEC Offload parameters to YES and ENABLED, respectively. Optionally, you configure NSEC record generation for that zone.

  To enable DNSSEC offload for a zone by using the NetScaler command line

  At the NetScaler command line, type:

  add dns zone <zoneName> **-proxyMode YES -dnssecOffload ENABLED [-nsec (ENABLED | DISABLED)]**

  To enable DNSSEC offload for a zone by using the configuration utility

  1. In the navigation pane, expand DNS, and then click Zones.

  2. In the details pane, do one of the following:

     - To create a zone on the appliance, click Add.

     - To configure DNSSEC offloading for an existing zone, click the zone, and then click Open.

  3. In the Create DNS Zone or Configure DNS Zone dialog box, select the Proxy Mode and DNSSEC Offload check boxes.

  4. Optionally, if you want the NetScaler appliance to generate NSEC records for the zone, select the NSEC check box.

  5. Click OK.

  You must also generate DNS keys for the zone, add the keys to the zone, and then sign the zone with the keys. These configuration tasks are the same as the tasks you perform for configuring DNSSEC on the NetScaler appliance.

  After you configure DNS offload, you must flush the DNS cache on the appliance. Flushing the DNS cache ensure that any unsigned records in the cache are removed and subsequently replaced by signed records.

  Note: DNSSEC offload is supported on all NetScaler MPX platforms, except the NetScaler MPX 9700/10500/12500/15500 FIPS platform. The feature is also supported on NetScaler VPX appliances hosted on NetScaler SDX platforms.

DNSSEC offload is not supported in a NetScaler cluster.

Known Issues and Workarounds

Application Firewall

- Issue ID 0363711: On a NetScaler appliance that has AAA, Kerberos authentication, KCD, and MSSQL monitor enabled, each monitor probe causes a memory leak that eventually results in the NetScaler appliance experiencing an out-of-memory condition that requires a restart to clear.

Domain Name System

- Issue ID 0376662: The NetScaler appliance might fail in the following scenario:
  - You have configured DNSSEC offload and enabled NSEC record generation for a zone on the appliance.
  - The appliance receives a DNS NODATA/NXDOMAIN query for that zone, over TCP, and the DNSSEC OK bit in the query is set.

NetScaler VPX on AWS

- Issue ID 0337614: Custom scriptable monitors do not work on NetScaler VPX on AWS.
- Issue ID 0340395: While configuring HA between two VPX instances in AWS, if you first configure HA on the VPX instance with a single ENI, HA configuration does not work as expected.

  Workaround: Configure the instance with two or more ENIs before configuring HA on the instance with one ENI.
- Issue ID 0344678: If you remove HA configuration from the primary instance first, HA configuration is not removed and causes the primary instance to reboot.

  Workaround: Remove HA configuration from the secondary instance first before removing HA configuration from the primary instance.
- Issue ID 0346689: In INC mode, HA configuration between two NetScaler VPX instances in AWS does not work properly.

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.
- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.
- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

Build 73.5002.e

Release version: Citrix® NetScaler® release 10.e build 73.5002.e

Replaces build: None

Release date: March 2013

Release notes version: 2.0

Language supported: English (US)

Review the following sections:

- Bug Fixes
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 73.5. The release notes are available in the Build 73.5 section on Citrix eDocs.
- The bug fixes and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Bug Fixes

AAA Application Traffic

- Issue ID 0349418: The NetScaler appliance now supports the exclusive normalization method with SAML. For that reason, assertions posted by any SAML 2.0 compliant IDP (such as the Pingone IDP server or Oracle ID server) are now handled correctly.

NetScaler SDX Appliance

- Issue ID 0367461: If a NetScaler VPX instance provisioned on a NetScaler SDX appliance is upgraded to release 10.0 build 71.6014.e or release 10.0 build 72.5005.e, all existing LA channels, and any new channels that you create, acquire the same, incorrect, MAC address. As a result, the services might go down and you might not be able to access the VPX instance by using the NetScaler IP (NSIP) address.

Known Issues and Workarounds

Application Firewall

- Issue ID 0363711: On a NetScaler appliance that has AAA, Kerberos authentication, KCD, and MSSQL monitor enabled, each monitor probe causes a memory leak that eventually results in the NetScaler appliance experiencing an out-of-memory condition that requires a restart to clear.

NetScaler VPX on AWS

- Issue ID 0337614: Custom scriptable monitors do not work on NetScaler VPX on AWS.
- Issue ID 0340395: While configuring HA between two VPX instances in AWS, if you first configure HA on the VPX instance with a single ENI, HA configuration does not work as expected.

  Workaround: Configure the instance with two or more ENIs before configuring HA on the instance with one ENI.
- Issue ID 0344678: If you remove HA configuration from the primary instance first, HA configuration is not removed and causes the primary instance to reboot.

  Workaround: Remove HA configuration from the secondary instance first before removing HA configuration from the primary instance.
- Issue ID 0346689: In INC mode, HA configuration between two NetScaler VPX instances in AWS does not work properly.

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.
- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.
- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

Build 72.5005.e

Release version: Citrix® NetScaler® release 10.e build 72.5005.e

Replaces build: None

Release date: January 2013

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Bug Fixes
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 72.5. The release notes are available in the Build 72.5 section on Citrix eDocs.
- The enhancements, bug fixes, and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Enhancements

GUI Support for Kerberos Protocol Transition and Constrained Delegation

- Issue ID 0288056: Kerberos Protocol Transition (KPT) and Kerberos Constrained Delegation (KCD) can now be configured by using the configuration utility as well as the NetScaler command line.

KCD Support for Microsoft SQL Data Stream

- Issue IDs 0307491 and 0329542: Kerberos Constrained Delegation (KCD) is now supported for the Microsoft SQL server and the MSSQL data stream.

Bug Fixes

AAA Application Traffic

- Issue ID 0325382: To configure Kerberos-Constrained Delegation (KCD) on a NetScaler appliance with AAA-TM enabled, the appliance must be part of the authentication server's domain. You can add the appliance to that domain by creating a negotiate policy as if a client-side negotiation were intended, or by using the Likewise domainjoin command.

- Issue ID 0354718: On a NetScaler appliance that has AAA and Kerberos Constrained Delegation (KCD) enabled, if you configure a service without first configuring the associated server, the appliance might hang.

Known Issues and Workarounds

Application Firewall

- Issue ID 0363711: On a NetScaler appliance that has AAA, Kerberos authentication, KCD, and MSSQL monitor enabled, each monitor probe causes a memory leak that eventually results in the NetScaler appliance experiencing an out-of-memory condition that requires a restart to clear.

NetScaler VPX on AWS

- Issue ID 0337614: Custom scriptable monitors do not work on NetScaler VPX on AWS.
- Issue ID 0340395: While configuring HA between two VPX instances in AWS, if you first configure HA on the VPX instance with a single ENI, HA configuration does not work as expected.

  Workaround: Configure the instance with two or more ENIs before configuring HA on the instance with one ENI.
- Issue ID 0344678: If you remove HA configuration from the primary instance first, HA configuration is not removed and causes the primary instance to reboot.

  Workaround: Remove HA configuration from the secondary instance first before removing HA configuration from the primary instance.
- Issue ID 0346689: In INC mode, HA configuration between two NetScaler VPX instances in AWS does not work properly.

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.
- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.
- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

Build 71.6016.e

Release version: Citrix® NetScaler® release 10.e build 71.6016.e

Replaces build: None

Release date: December 2012

Release notes version: 2.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 71.6. The release notes are available in the Build 71.6 section on Citrix eDocs.
- The enhancements and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Enhancements

AutoScale: Automatically Scaling Your Application Fleet in a CloudPlatform Environment

- Issue ID 0311703: In an environment deployed and managed by using Citrix® CloudPlatform, automatic scaling of an application fleet can be achieved by using the Citrix® NetScaler® appliance. CloudPlatform provides a feature called AutoScale, as part of its elastic load balancing feature. A CloudPlatform user can use the AutoScale feature to specify thresholds for various conditions for automatically scaling the application fleet upward and downward. The scale up and scale down conditions can vary from simple use cases, such as a server's CPU usage, to complex use cases, such as a combination of a server's CPU usage and responsiveness. CloudPlatform, in turn, configures the NetScaler appliance to load balance traffic to the application virtual machines (VMs), monitor application thresholds and performance, and trigger scale up and scale down actions to add or remove VMs from the application fleet.

  For more information about how AutoScale works on the NetScaler appliance, see http://support.citrix.com/proddocs/topic/ns-system-10-map/ns-autoscale-automatic-scaling-in-cloudplatform-env-wrapper-con.html.

  For answers to frequently asked questions, see http://support.citrix.com/proddocs/topic/ns-faq-map/ns-faq-autoscale-ref.html.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0325382: To configure Kerberos-Constrained Delegation (KCD) on a NetScaler appliance with AAA-TM enabled, the appliance must be part of the authentication server's domain. You can add the appliance to that domain by creating a negotiate policy as if a client-side negotiation were intended, or by using the Likewise 'domainjoin' command.

  1. To create a negotiate policy, at the NetScaler command prompt type the following commands:

     > add authentication negotiateAction <negActionName> -domain <domain> -domainUser <domainuse
     > add authentication negotiatePolicy <negPolName> ns_true <negActionName>

     For <negActionName>, substitute a name for the negotiation action. For <domain>, substitute the domain of the authentication server. For <domainuser>, substitute the user name for logging on. For <passwd>, substitute the password for that user name. For <negPolName>, substitute a name for the negotiation policy.
  2. To use the Likewise 'domainjoin' command, at the NetScaler command prompt type the following commands to open a shell and then run domainjoin:

     > shell
     # /opt/likewise/bin/domainjoin-cli join <domain> <domainuser>

     For <domain>, substitute the domain of the authentication server. For <domainuser>, substitute the user name that is used to log on to the domain.

NetScaler VPX on AWS

- Issue ID 0337614: Custom scriptable monitors do not work on NetScaler VPX on AWS.
- Issue ID 0340395: While configuring HA between two VPX instances in AWS, if you first configure HA on the VPX instance with a single ENI, HA configuration does not work as expected.

  Workaround: Configure the instance with two or more ENIs before configuring HA on the instance with one ENI.
- Issue ID 0344678: If you remove HA configuration from the primary instance first, HA configuration is not removed and causes the primary instance to reboot.

  Workaround: Remove HA configuration from the secondary instance first before removing HA configuration from the primary instance.
- Issue ID 0346689: In INC mode, HA configuration between two NetScaler VPX instances in AWS does not work properly.

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.
- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.
- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

Build 71.6008.e

Release version: Citrix® NetScaler® release 10.e build 71.6008.e

Replaces build: None

Release date: November 2012

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 71.6. The release notes are available in the Build 71.6 section on Citrix eDocs.
- The enhancements and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Enhancements

NetScaler VPX on AWS

- Issue ID 0248904: You can now launch an instance of Citrix® NetScaler® VPX within Amazon Web Services (AWS). NetScaler VPX is available as an Amazon Machine Image (AMI) from AWS Marketplace. NetScaler VPX on AWS enables customers to leverage AWS Cloud computing capabilities and use NetScaler load balancing and traffic management features for their business needs. NetScaler VPX on AWS supports all the traffic management features of a physical NetScaler appliance. NetScaler VPX instances running in AWS can be deployed in standalone mode or in pairs for High Availability (HA) setup.

  Note: The NetScaler AMI launches on Windows EC2 instance types because it runs as a hardware virtual machine (HVM). HVM is currently available on Windows EC2 instances. The Windows OS is not running and is not used in any way.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0325382: To configure Kerberos-Constrained Delegation (KCD) on a NetScaler appliance with AAA-TM enabled, the appliance must be part of the authentication server's domain. You can add the appliance to that domain by creating a negotiate policy as if a client-side negotiation were intended, or by using the Likewise 'domainjoin' command.

  1. To create a negotiate policy, at the NetScaler command prompt type the following commands:

     > add authentication negotiateAction <negActionName> -domain <domain> -domainUser <domainuse
     > add authentication negotiatePolicy <negPolName> ns_true <negActionName>

     For <negActionName>, substitute a name for the negotiation action. For <domain>, substitute the domain of the authentication server. For <domainuser>, substitute the user name for logging on. For <passwd>, substitute the password for that user name. For <negPolName>, substitute a name for the negotiation policy.
  2. To use the Likewise 'domainjoin' command, at the NetScaler command prompt type the following commands to open a shell and then run domainjoin:

     > shell
     # /opt/likewise/bin/domainjoin-cli join <domain> <domainuser>

     For <domain>, substitute the domain of the authentication server. For <domainuser>, substitute the user name that is used to log on to the domain.

NetScaler VPX on AWS

- Issue ID 0337614: Custom scriptable monitors do not work on NetScaler VPX on AWS.
- Issue ID 0340395: While configuring HA between two VPX instances in AWS, if you first configure HA on the VPX instance with a single ENI, HA configuration does not work as expected.

  Workaround: Configure the instance with two or more ENIs before configuring HA on the instance with one ENI.
- Issue ID 0344678: If you remove HA configuration from the primary instance first, HA configuration is not removed and causes the primary instance to reboot.

  Workaround: Remove HA configuration from the secondary instance first before removing HA configuration from the primary instance.
- Issue ID 0346689: In INC mode, HA configuration between two NetScaler VPX instances in AWS does not work properly.

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.
- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.
- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

Build 70.7012.e

Release version: Citrix® NetScaler® release 10.e build 70.7012.e

Replaces build: None

Release date: November 2012

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Bug Fixes
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 70.7. The release notes are available in the Build 70.7 section on Citrix eDocs.
- The enhancements, bug fixes, and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Enhancements

Kerberos Constrained Delegation (KCD) Support

- Issue ID 0288056: The AAA-TM feature now supports the constrained delegation feature of the Kerberos version 5 authentication protocol (KCD). KCD allows you to configure the list of services that a Kerberos user can access after authentication.

Bug Fixes

AAA Application Traffic

- Issue ID 0327102: On a NetScaler appliance with AAA-TM enabled and Kerberos-constrained delegation (KCD) configured, if the first request after authentication is not a 401-based request, KCD can fail. If KCD fails, the individual resource that the user requested prompts the user to re-enter their credentials. The user can either re-enter the credentials as prompted, or can simply cancel the request and then request the resource a second time. In either case, the user can access the resource.

- Issue ID 0328546: On a NetScaler appliance with AAA-TM enabled and Kerberos-constrained delegation (KCD) configured, under heavy load intermittent failures of KCD can cause individual resources to prompt users to re-enter their credentials.

- Issue ID 0329020: On a NetScaler appliance with AAA-TM enabled and Kerberos-constrained delegatino (KCD) configured, after upgrading the NetScaler operating system to version 10.0.9.45, KCD does not start properly.

- Issue ID 0329280: On a NetScaler appliance with AAA-TM enabled and Kerberos-constrained delegation (KCD) configured, if you change the authentication method on the traffic management virtual server from form-based to 401-based authentication, this might cause intermittent hangs or crashes.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0325382: To configure Kerberos-Constrained Delegation (KCD) on a NetScaler appliance with AAA-TM enabled, the appliance must be part of the authentication server's domain. You can add the appliance to that domain by creating a negotiate policy as if a client-side negotiation were intended, or by using the Likewise "domainjoin" command.

  1. To create a negotiate policy, at the NetScaler command prompt type the following commands:

     > add authentication negotiateAction <negActionName> -domain <domain> -domainUser <domainuse
     > add authentication negotiatePolicy <negPolName> ns_true <negActionName>

     For <negActionName>, substitute a name for the negotiation action. For <domain>, substitute the domain of the authentication server. For <domainuser>, substitute the user name for logging on. For <passwd>, substitute the password for that user name. For <negPolName>, substitute a name for the negotiation policy.
  2. To use the Likewise "domainjoin" command, at the NetScaler command prompt type the following commands to open a shell and then run domainjoin:

     > shell
     # /opt/likewise/bin/domainjoin-cli join <domain> <domainuser>

     For <domain>, substitute the domain of the authentication server. For <domainuser>, substitute the user name that is used to log on to the domain.

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.

- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.

- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

Build 70.7002.e

Release version: Citrix® NetScaler® release 10.e build 70.7002.e

Replaces build: None

Release date: September 2012

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 70.7. The release notes are available in the Build 70.7 section on Citrix eDocs.
- The enhancements and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Enhancements

Stateless NAT46 Translation

- Issue ID 0284926: The stateless NAT46 feature enables the communication between IPv4 and IPv6 networks by way of IPv4 to IPv6 packet translation and vice versa without maintaining any session information on the NetScaler appliance.

  A stateless NAT46 configuration on the NetScaler appliance has the following components:

  - **IPv4-IPv6 INAT entry**. An entry defining a 1:1 relationship between a public IPv4 address and an IPv6 address. In other words, a public IPv4 address on the appliance listens to connection requests on behalf of an IPv6 server

  - **NAT46 IPv6 prefix**. A global IPv6 prefix of length 96 bits (128-32=96) configured on the appliance. During IPv4 packet to IPv6 packet translation, the appliance sets the source IP address of the translated IPv6 packet to a concatenation of the NAT46 IPv6 prefix [96 bits] and the IPv4 source address [32 bits] that was received in the request packet.

  For more information, see Stateless NAT46 Translation.

Known Issues and Workarounds

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.
- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.
- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

FAQs

2015-05-18 16:46:59 UTC

Contents

FAQs

AppFlow

Which build of NetScaler supports AppFlow?

AppFlow is supported on NetScaler appliances running version 9.3 and above with nCore build.

What is the format used by AppFlow to transmit data?

AppFlow transmits information in the Internet Protocol Flow Information eXport (IPFIX) format, which is an open Internet Engineering Task Force (IETF) standard defined in RFC 5101. IPFIX (the standardized version of Cisco's NetFlow) is widely used to monitor network flow information.

What do AppFlow records contain?

AppFlow records contain standard NetFlow or IPFIX information, such as time stamps for the beginning and end of a flow, packet count, and byte count. AppFlow records also contain application-level information (such as HTTP URLs, HTTP request methods and response-status codes, server response time, and latency). IPFIX flow records are based on templates that must be sent before sending flow records.

After an upgrade to NetScaler Version 9.3 Build 48.6 Cl, why does an attempt to open a virtual server from the GUI result in the error message "The AppFlow feature is only available on Citrix Netscaler Ncore"

AppFlow is supported only on nCore appliances. When you open the virtual server configuration tab, clear the **AppFlow** checkbox.

What does the transaction ID in an AppFlow records contain?

A transaction ID is an unsigned 32-bit number identifying an application-level transaction. For HTTP, a transaction corresponds to a request and response pair. All flow records that correspond to this request and response pair have the same transaction ID. A typical transaction has four uniflow records. If the NetScaler generates the response by itself (served from the integrated cache or by a security policy), there might be only two flow records for the transaction.

What is an AppFlow action ?

An Appflow action is a set of collectors to which the flow records are sent if the associated AppFlow policy matches.

What commands can I run on the NetScaler appliance to verify that the AppFlow action is a hit?

The show appflow action. For example:

```
> show appflow action
1)      Name: aFL-act-collector-1
```

Collectors: collector-1
Hits: 0
Action Reference Count: 2

2) Name: apfl-act-collector-2-and-3
Collectors: collector-2, collecter-3
Hits: 0
Action Reference Count: 1

3) Name: apfl-act-collector-1-and-3
Collectors: collector-1, collecter-3
Hits: 0
Action Reference Count: 1

What is an AppFlow collector?

A collector receives flow records generated by the NetScaler appliance. To be able to send flow records, you must specify at least one collector. You can specify up to four. You can remove unused collectors.

What NetScaler verison is required for using AppFlow?

Use NetScaler version 9.3.49.5 or higher, and remember that AppFlow is available in only the nCore builds.

What transport protocol does AppFlow use?

AppFlow uses UDP as the transport protocol.

What ports needs to be opened if I have a firewall in the network?

Port 4739. It is the default UDP port the AppFlow collector uses for listening on IPFIX messages. If the user changes the default port, that port should be opened on the firewall.

How can I change the default port AppFlow uses?

When you add an AppFlow collector by using the add appflowCollector command, you can specify the port to be used.

```
> add appflowCollector coll1 -IPAddress
10.102.29.251 -port 8000
 Done
```

What does setting clientTrafficOnly do?

NetScaler generates AppFlow records only for client-side traffic.

How many collectors can be configured at a time?

You can configure up to four AppFlow collectors at a time on the NetScaler appliance. Please note that the maximum number of collectors that can be configured on a NetScaler appliance is four.

AppFlow

Which build of NetScaler supports AppFlow?

AppFlow is supported on NetScaler appliances running version 9.3 and above with nCore build.

What is the format used by AppFlow to transmit data?

AppFlow transmits information in the Internet Protocol Flow Information eXport (IPFIX) format, which is an open Internet Engineering Task Force (IETF) standard defined in RFC 5101. IPFIX (the standardized version of Cisco's NetFlow) is widely used to monitor network flow information.

What do AppFlow records contain?

AppFlow records contain standard NetFlow or IPFIX information, such as time stamps for the beginning and end of a flow, packet count, and byte count. AppFlow records also contain application-level information (such as HTTP URLs, HTTP request methods and response-status codes, server response time, and latency). IPFIX flow records are based on templates that must be sent before sending flow records.

After an upgrade to NetScaler Version 9.3 Build 48.6 Cl, why does an attempt to open a virtual server from the GUI result in the error message "The AppFlow feature is only available on Citrix Netscaler Ncore"

AppFlow is supported only on nCore appliances. When you open the virtual server configuration tab, clear the **AppFlow** checkbox.

What does the transaction ID in an AppFlow records contain?

A transaction ID is an unsigned 32-bit number identifying an application-level transaction. For HTTP, a transaction corresponds to a request and response pair. All flow records that correspond to this request and response pair have the same transaction ID. A typical transaction has four uniflow records. If the NetScaler generates the response by itself (served from the integrated cache or by a security policy), there might be only two flow records for the transaction.

What is an AppFlow action ?

An Appflow action is a set of collectors to which the flow records are sent if the associated AppFlow policy matches.

What commands can I run on the NetScaler appliance to verify that the AppFlow action is a hit?

The show appflow action. For example:

```
> show appflow action
1)      Name: aFL-act-collector-1
```

Collectors: collector-1
Hits: 0
Action Reference Count: 2

2) Name: apfl-act-collector-2-and-3
Collectors: collector-2, collecter-3
Hits: 0
Action Reference Count: 1

3) Name: apfl-act-collector-1-and-3
Collectors: collector-1, collecter-3
Hits: 0
Action Reference Count: 1

What is an AppFlow collector?

A collector receives flow records generated by the NetScaler appliance. To be able to send flow records, you must specify at least one collector. You can specify up to four. You can remove unused collectors.

What NetScaler verison is required for using AppFlow?

Use NetScaler version 9.3.49.5 or higher, and remember that AppFlow is available in only the nCore builds.

What transport protocol does AppFlow use?

AppFlow uses UDP as the transport protocol.

What ports needs to be opened if I have a firewall in the network?

Port 4739. It is the default UDP port the AppFlow collector uses for listening on IPFIX messages. If the user changes the default port, that port should be opened on the firewall.

How can I change the default port AppFlow uses?

When you add an AppFlow collector by using the add appflowCollector command, you can specify the port to be used.

```
> add appflowCollector coll1 -IPAddress
10.102.29.251 -port 8000
 Done
```

What does setting clientTrafficOnly do?

NetScaler generates AppFlow records only for client-side traffic.

How many collectors can be configured at a time?

You can configure up to four AppFlow collectors at a time on the NetScaler appliance. Please note that the maximum number of collectors that can be configured on a NetScaler appliance is four.

AutoScale

Note: The AutoScale feature is supported only on NetScaler 10.e.

What are the prerequisites for setting up AutoScale?

For prerequisites for setting up AutoScale, see "Prerequisites".

Can the CloudPlatform AutoScale feature be used without a NetScaler appliance?

No. The NetScaler appliance is currently required for the AutoScale feature to work. If the CloudPlatform administrator configures AutoScale in a network that does not include a NetScaler appliance, CloudPlatform throws an error.

What happens if the AutoScale feature is used with a NetScaler release that does not support AutoScale?

If the AutoScale feature is used with a NetScaler release that does not support AutoScale, the CloudPlatform user interface throws an error. CloudPlatform also writes a message to the log file, indicating that the configured NetScaler does not support AutoScale.

What versions of CloudPlatform and NetScaler should I use to implement AutoScale?

For information about NetScaler releases that support AutoScale, see Supported Environment.

In a load balancing rule, can manually provisioned virtual machine instances coexist with instances provisioned by the AutoScale feature?

No. The CloudPlatform virtual machine group in a load balancing rule can contain only manually provisioned instances or only instances provisioned by the AutoScale feature. They cannot coexist.

Is there a limit on the number of virtual machine instances to which we can scale up by using AutoScale?

Yes. The CloudPlatform administrator specifies the maximum number of members to which the configuration can scale up. When the limit is reached, virtual machines are not provisioned even if the scale-up condition is satisfied. The upper limit prevents uncontrolled spawning of VMs due to misconfiguration of the AutoScale feature or unexpected load conditions.

Are AutoScale events observable?

The events generated for deploying or destroying virtual machines are observable. These events are logged in the NetScaler logs (ns.log) and in the CloudPlatform logs (management-server.log). However, you cannot observe the metric values collected by NetScaler monitors.

What metrics can be used in AutoScale policies?

In an AutoScale policy, you can use any metric that is exposed through SNMP, or any NetScaler statistics associated with the load balancing virtual server used in the AutoScale configuration. For example, you can use metrics associated with CPU, memory, or disk usage, and NetScaler metrics such as throughput or response time.

What should a CloudPlatform administrator do before performing maintenance tasks on a CloudPlatform network in which AutoScale is configured?

The CloudPlatform administrator should disable the AutoScale configuration from the CloudPlatform user interface. Disabling the AutoScale configuration temporarily disables any scale-up or scale-down events. However, disabling AutoScale for an application, in CloudPlatform, does not affect the ability of the NetScaler appliance to serve traffic to existing virtual machines.

With AutoScale configured, are any configured VM limits enforced on the user account?

The NetScaler appliance works in the context of an AutoScale user account. Therefore, any limits that the CloudPlatform administrator has imposed on the number of VMs that can be created by the account are automatically enforced when the NetScaler appliance attempts to create more VMs than are permitted.

Is AutoScale supported in a high availability (HA) NetScaler pair?

No. Currently, HA mode is not supported for AutoScale.

Call Home

What is the Call Home feature on a NetScaler appliance?

The Call Home feature registers your NetScaler appliance with the Citrix Technical Support server (TaaS) and monitors the appliance for common error conditions. If your appliance is successfully registered with TaaS server, Call Home automatically uploads system debug data to that server in the event that one of the conditions occurs. The appliance keeps a full log of all upload events. If you are unable to correct the problem after reviewing the appliance's log, you can contact the Citrix Technical Support team and open a service request. The team can analyze the uploaded system data and recommend possible solutions.

Which release of NetScaler Software supports Call Home?

Release 10 and later.

Does Call Home support monitoring of any error conditions in a NetScaler virtual appliance?

No. Call Home does not currently support monitoring of virtual appliances.

Which NetScaler hardware models support Call Home?

Any NetScaler MPX appliance running release 10 or later of the NetScaler software supports Call Home.

Do you need a separate license for Call Home?

No. The Call Home feature does not require a separate license. It is available with all NetScaler platform licenses.

Does Call Home support monitoring of cluster events or error conditions?

No. Call Home does not currently support monitoring of NetScaler clusters.

What error conditions does Call Home monitor in a NetScaler appliance?

Call Home supports monitoring of the following events in a NetScaler appliance:

- Compact flash drive errors
- Hard disk drive errors
- Power supply unit failure
- SSL card failure
- Warm restart

What mechanism does Call Home use to upload the Call Home tar file to TaaS?

Call Home uses the HTTPS protocol to upload the Call Home tar file.

Does Call Home support automatic Technical Support service request creation?

No. You have to contact the Citrix Technical Support team to open a service request.

What is the frequency of Call Home tar file uploads to TaaS?

Call Home creates the Call Home tar file and uploads it to the Citrix Technical Support server (TaaS) upon first occurrence of a particular error condition since the appliance was last started. That is, a reoccurrence of same error condition does not trigger another upload unless the appliance was rebooted after the previous occurrence.

Must I configure SNMP for Call Home to monitor error conditions?

No. Call Home creates and uploads a Call Home tar file for the first occurrence of a monitored error condition since the appliance was last started. If you want to be alerted each time the error condition occurs, you can configure the corresponding SNMP alarm for the error condition.

Clustering FAQs

How many NetScaler appliances can I have in a cluster?

A NetScaler cluster can include as few as 2 or as many as 32 NetScaler nCore hardware or virtual appliances.

Can a cluster have NetScaler appliances from different networks?

No. The current cluster implementation requires that all cluster nodes be in the same network.

Can a NetScaler appliance be a part of multiple clusters?

No. An appliance can belong to only one cluster.

How can I set the hostname for a cluster node?

The hostname of a cluster node must be specified by executing the set ns hostname command through the cluster IP address. For example, to set the hostname of the cluster node with ID 2, the command is:

> set ns hostname hostName1 -ownerNode 2

What is a cluster IP address? What is its subnet mask?

The cluster IP address is the management address of a NetScaler cluster. All cluster configurations must be performed by accessing the cluster through this address. The subnet mask of the cluster IP address is fixed at 255.255.255.255.

Can I automatically detect NetScaler appliances so that I can add them to a cluster?

Yes. The configuration utility allows you to discover appliances that are present in the same subnet as the NSIP address of the configuration coordinator. For more information, see "Discovering NetScaler Appliances".

Why are the network interfaces of a cluster represented in 3-tuple (n/u/c) notation instead of the regular 2-tuple (u/c) notation?

When an appliance is part of a cluster, you must be able to identify the node to which the network interface belongs. Therefore, the network interface naming convention for cluster nodes is modified from u/c to n/u/c, where n denotes the node Id.

I have multiple standalone appliances, each of which has different configurations. Can I add them to a single cluster?

Yes. You can add appliances that have different configurations to a single cluster. However, when the appliance is added to the cluster, the existing configurations are cleared. To use the configurations that are available on each of the individual appliances, you must:

1. Create a single *.conf file for all the configurations.

2. Edit the configuration file to remove features that are not supported in a cluster environment.

3. Update the naming convention of interfaces from 2-tuple (u/c) format to 3-tuple (n/u/c) format.

4. Apply the configurations to the configuration coordinator node of the cluster by using the batch command.

Can I migrate the configurations of a standalone NetScaler appliance or an HA setup to the clustered setup?

No. When a node is added to a clustered setup, its configurations are implicitly cleared by using the clear ns config command (with the extended option). In addition, the SNIP addresses and all VLAN configurations (except default VLAN and NSVLAN) are cleared. Therefore, it is recommended that you back up the configurations before adding the appliance to a cluster. Before using the backed-up configuration file for the cluster, you must:

1. Edit the configuration file to remove features that are not supported in a cluster environment.

2. Update the naming convention of interfaces from two-tuple (x/y) format to three-tuple (x/y/z) format.

3. Apply the configurations to the configuration coordinator node of the cluster by using the batch command.

How can I configure/unconfigure the NSVLAN on a cluster?

- To make the NSVLAN available in a cluster, make sure that each appliance has the same NSVLAN configured before it is added to cluster.

- To remove the NSVLAN from a cluster node, first remove the node from the cluster and then delete the NSVLAN from the appliance.

Can a cluster node that is not connected to the client or server network still serve traffic?

Yes. The cluster supports a traffic distribution mechanism called linksets, which allows unconnected nodes to serve traffic by using the interfaces of connected nodes. The unconnected nodes communicate with the connected nodes through the cluster backplane. For more information, see "Using Linksets".

Can I execute commands from the NSIP address of a cluster node?

No. Access to individual cluster nodes through the NetScaler IP (NSIP) addresses is read-only. Therefore, when you log on to the NSIP address of a cluster node you can only view the configurations and the statistics. You cannot configure anything. However, there are some operations you can execute from the NSIP address of a cluster node. For more information, see "Operations Supported on Individual Nodes".

Can I disable configuration propagation among cluster nodes?

No, you cannot explicitly disable the propagation of cluster configurations among cluster nodes. However, during a software upgrade or downgrade, a version mismatch can

automatically disable configuration propagation.

Can I change the NSIP address or change the NSVLAN of a NetScaler appliance when it is a part of the cluster?

No. To make such changes you must first remove the appliance from the cluster, perform the changes, and then add the appliance to the cluster.

Does the NetScaler cluster support L2 and L3 Virtual Local Area Networks (VLANs)?

Yes. A cluster supports VLANs between cluster nodes. The VLANs must be configured on the cluster IP address.

- **L2 VLAN.** You can create a layer2 VLAN by binding interfaces that belong to different nodes of the cluster.
- **L3 VLAN.** You can create a layer3 VLAN by binding IP addresses that belong to different nodes of the cluster. The IP addresses must belong to the same subnet. Make sure that one of the following criteria is satisfied. Otherwise, the L3 VLAN bindings can fail.
  - All nodes have an IP address on the same subnet as the one bound to the VLAN.
  - The cluster has a striped IP address and the subnet of that IP address is bound to the VLAN.

  When you add a new node to a cluster that has only spotted IPs, the sync happens before spotted IP addresses are assigned to that node. In such cases, L3 VLAN bindings can be lost. To avoid this loss, either add a striped IP or add the L3 VLAN bindings on the NSIP of the newly added node.

How can I configure SNMP on a NetScaler cluster?

SNMP monitors the cluster, and all the nodes of the cluster, in the same way that it monitors a standalone appliance. The only difference is that SNMP on a cluster must be configured through the cluster IP address. When generating hardware specific traps, two additional varbinds are included to identify the node of the cluster: node ID and NSIP address of the node.

For detailed information about configuring SNMP, see "SNMP".

What details must I have available when I contact technical support for cluster-related issues?

The NetScaler provides a `show techsupport -scope cluster` command that extracts configuration data, statistical information, and logs of all the cluster nodes. You must run this command on the cluster IP address.

The output of this command is saved in a file named collector_cluster_<nsip_CCO>_P_<date-timestamp>.tar.gz which is available in the /var/tmp/support/cluster/ directory of the configuration coordinator.

Send this archive to the technical support team to debug the issue.

Can I use striped IP addresses as the default gateway of servers?

In case of cluster deployments, make sure the default gateway of the server points to a striped IP address (if you are using a NetScaler-owned IP address). For example, in case

of LB deployments with USIP enabled, the default gateway must be a striped SNIP address.

Can I view routing configurations of a specific cluster node from the cluster IP address?

Yes. You can view and clear the configurations specific to a node by specifying the owner node while entering the vtysh shell.

For example, to view the output of a command on nodes 0 and 1, the command is as follows:

```
> vtysh
ns# owner-node 0 1
ns(node-0 1)# show cluster state
ns(node-0 1)# exit-cluster-node
ns#
```

How can I specify the node for which I want to set the LACP system priority?

Applicable for NetScaler 10.1 and later releases.

In a cluster, you must set that node as the owner node by using the set lacp command.

For example: To set the LACP system priority for node with ID 2:

```
> set lacp -sysPriority 5 -ownerNode 2
```

How can I configure IP tunnels in a cluster?

Applicable for NetScaler 10.1 and later releases.

Configuring IP tunnels in a cluster is the same as on a standalone appliance. The only difference is that in a cluster setup, the local IP address must be a striped SNIP or MIP address. For more information, see "Configuring IP Tunnels".

How can I add a failover interface set (FIS) on the nodes of a NetScaler cluster?

Applicable for NetScaler 10.5 and later releases.

On the cluster IP address, specify the ID of the cluster node on which the FIS must be added.

add fis <name> -ownerNode <nodeId>

Note:

- The FIS name for each cluster node must be unique.
- A cluster LA channel can be added to a FIS. You must make sure that the cluster LA channel has a local interface as a member interface.

For more information on FIS, see "Configuring FIS".

Are Net Profiles supported on a cluster?

Applicable for NetScaler 10.5 and later releases.

Net profiles are now supported on a NetScaler cluster. You can bind spotted IP addresses to a net profile which can then be bound to spotted lbvserver or service (defined using a node group) with the following recommendations:

Note:

- If the "strict" parameter of the node group is "Yes", the net profile must contain a minimum of one IP address from each node of the node group member.
- If the "strict" parameter of the node group is "No", the net profile must include at least one IP address from each of the cluster nodes.
- If the above recommendations are not followed, the net profile configurations will not be honored and the USIP/USNIP settings will be used.

Configuration Utility - Frequently Asked Questions

Q: I am using a MAC Safari browser to upgrade a NetScaler ADC. On the upgrade wizard, when I click the Browse button to choose the build file from the appliance, the dialog box does not show any files or folders. Also, when I navigate back to the root folder, the dialog box displays the top level folder, but I cannot browse it. What should I do?

A: On the Safari browser, click the Settings icon and navigate to Preferences > Security > Manage Website Settings > Java, and then change value of the When visiting other websites setting to Run in unsafe mode.

Q: After I upgraded the JRE on my appliance to version 7.51, the graphical user interface (GUI) applet does not load when I access the NetScaler configuration utility. The applet download stops at 1%, and Java generates a security error. What should I do?

A: You can use the configuration utility with JRE 7.51 if, in the Java Control Panel, you lower the security level or add the NetScaler appliance's URL to the Exception Site List.

If using a Windows computer, navigate to Control Panel and click Java.

If using a MAC computer, navigate to System Preferences and click Java.

Then, in the Java Control Panel dialog box, do either of the following:

- Click the Security tab, and then set the Security Level to medium.
- Click the Security tab, click the Edit Site List button, and then add the URL of the NetScaler appliance in the Exception Site List box.

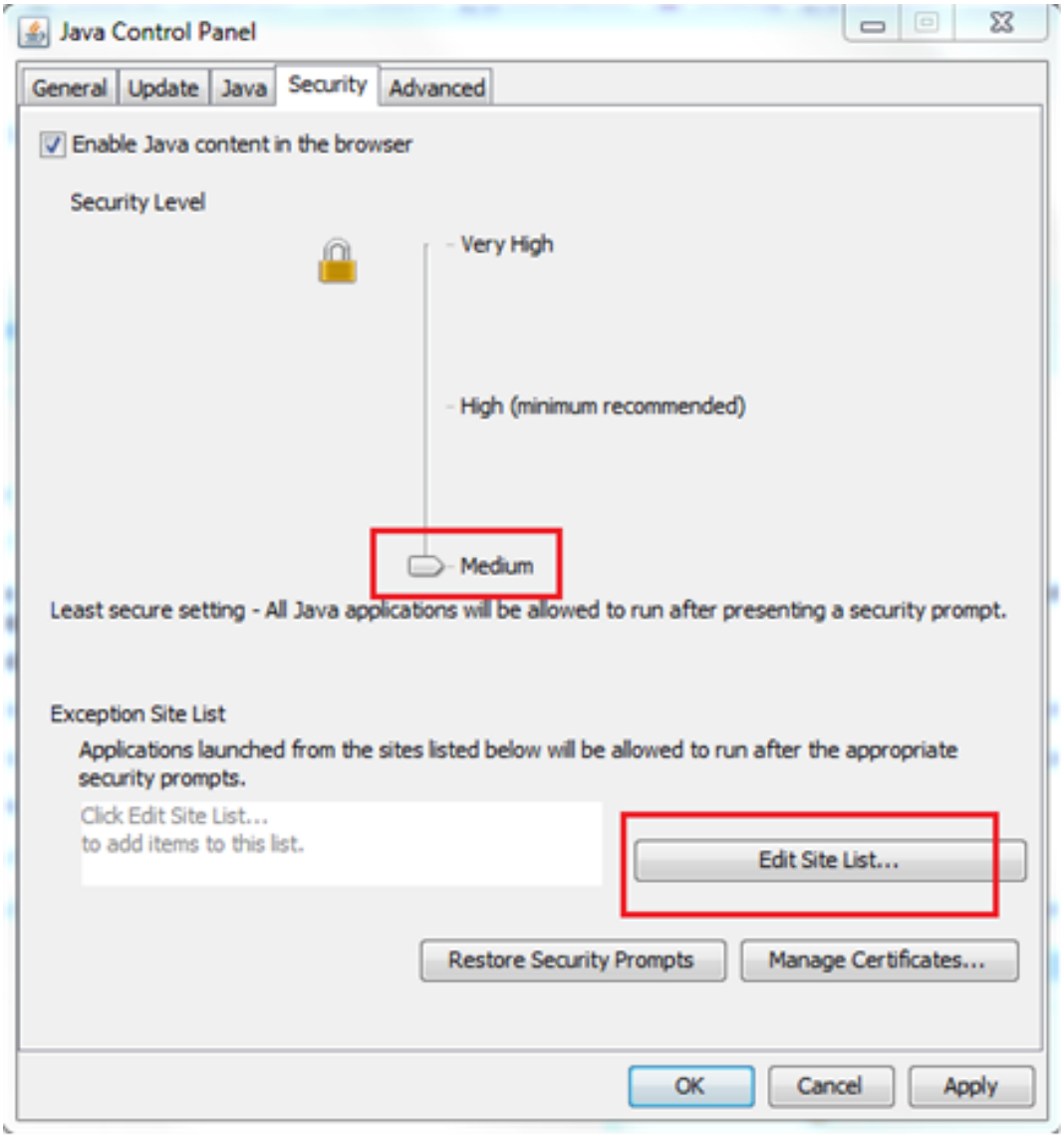


Figure 1. Java Control Panel

Q: After I upgraded the JRE on my appliance to version 7.45, the graphical user interface (GUI) applet does not load when I access the NetScaler configuration utility. The applet download stops at 1%, and Java throws a security error. What should I do?

A: The NetScaler GUI is not compatible with JRE version 7.45. Citrix recommends using a JRE version earlier than 7.45 to access the configuration utility. If you have already upgraded to version 7.45 and do not want to downgrade, you can configure Java to not keep temporary files. However, you will have to download the JAR files every time you access the configuration utility.

To downgrade JRE 7.45 to an earlier version:

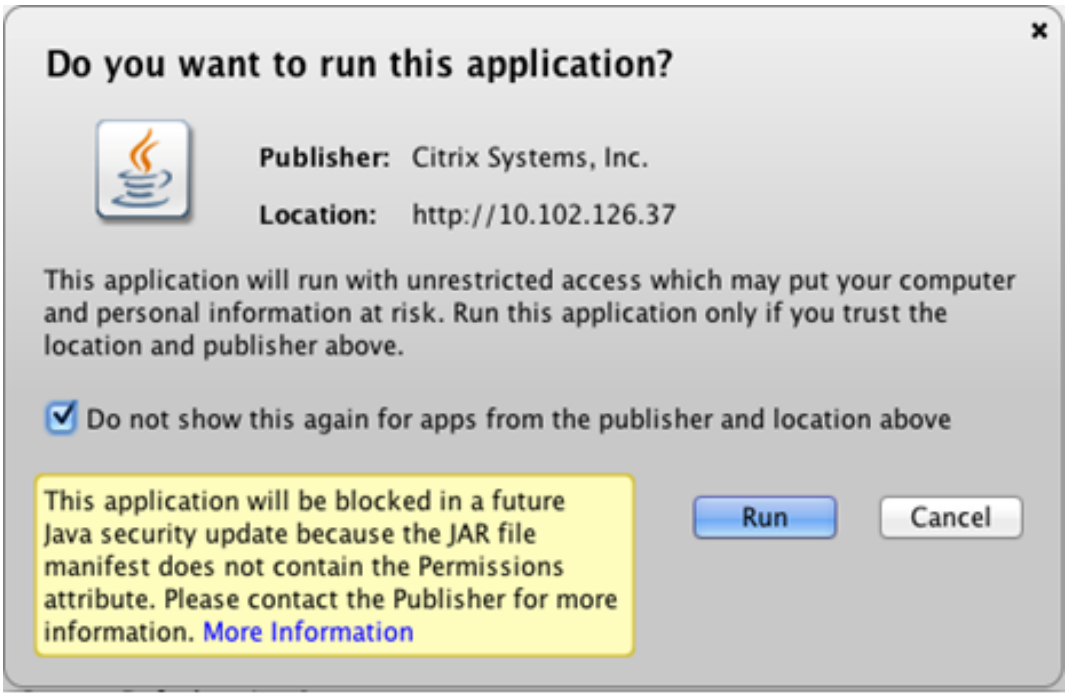
1. Uninstall JRE 7.45 by following the instructions at http://www.java.com/en/download/help/uninstall_java.xml.

2. Download an earlier version of JRE from the following location: http://www.oracle.com/technetwork/java/javase/archive-139210.html.

To continue using JRE 7.45:

If you are using a Windows system, navigate to Control Panel and click Java. The Java Control Panel opens.

If you are using a MAC system, navigate to System Preferences and click Java. The Java Control Panel opens.

1. Click the General tab.
2. Under Temporary Internet Files, click Settings.
3. Clear the Keep temporary files on my computer option.
4. Close the browser and re-launch the GUI.
5. 

Open the configuration utility and click Run and Allow, respectively, when the following warnings appear:

Note:

- The Jar files will not be cached and you will have to download the files every time you access the configuration utility.
- This problem is fixed in the following releases:
  - Release 9.3, build 65.x and later
  - Release 10.0, build 78.x and later
  - Release 10.1, build 122.x and later
  - Release 10.1.e, build 120.13xx.e

Q: What should I do before accessing the NetScaler configuration utility?

A: Before accessing a new version of the NetScaler software:

- Clear your browser cache.
- Make Sure that JavaScript, Java, and plug-ins are enabled in your browser. For help with enabling Java for your browser, see http://java.com/en/download/help/enable_browser.xml.
- Clear the “Temporary internet files” in the Java console.
- On the Java tab of the Java console, in Java Runtime Environment Settings, make sure that the latest version of JRE is present and is enabled.

Q: I am using HTTP to access the configuration utility. Which port should I open?

A: Open TCP port 3010 when using HTTP to access the configuration utility.

Q: I am using HTTPS to access the configuration utility. Which port should I open?

A: Open TCP port 3008 when using HTTPS to access the configuration utility.

Q: After entering the IP address of the NetScaler appliance in the address bar, I get the following error: “Java Applet could not be loaded". What should I do?

A: Verify that Java is installed properly. You can download Java from www.java.com. If you are using a MAC Safari browser, Java is disabled if it is not used for 35 days.

To enable Java plug-in in Safari, follow these steps:

1. In the Safari browser, choose Safari > Preferences or press Command-comma (⌘-,) on your keyboard.

2. 

   Click Security, and then select Enable Java.

3. Close the Safari Preferences window.

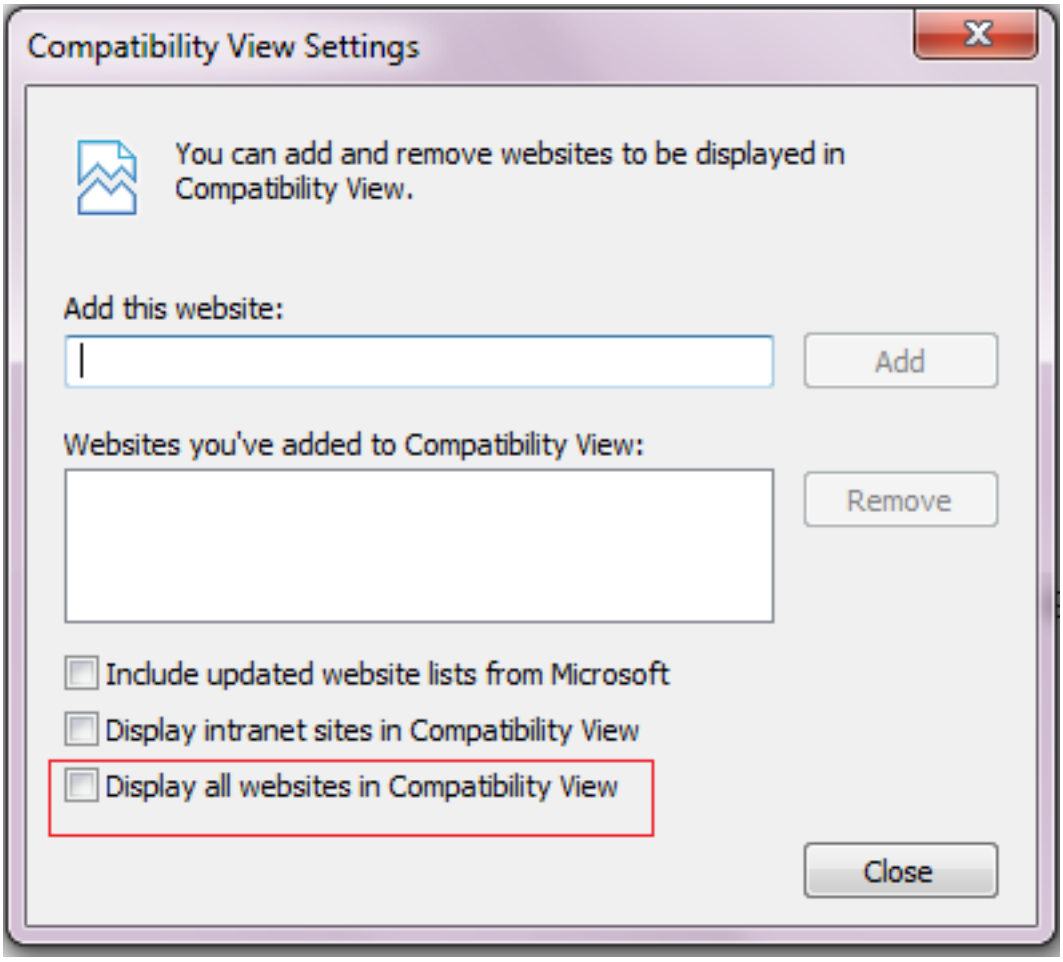
Q: With which browsers is the configuration utility compatible for different operating systems?

A: The following table lists the compatible browsers:

Operating System	Browser	Versions
Windows 7	Internet Explorer	8 and 9
	Mozilla Firefox	3.6.25 and above
	Chrome	15 and above
Windows 64 bit	Internet Explorer	8 and 9
	Chrome	15 and above
MAC OS	Mozilla Firefox	12 and above
	Safari	5.1.3

Q: When I access the NetScaler configuration utility by using Internet Explorer version 8 or 9, the browser displays only a grey bar at the top of the screen. What should I do?

A: The browser might be set in compatibility mode. To disable compatibility mode, go to **Tools** > **Compatibility View Settings** and clear the **Display all websites in Compatibility View** check box.



Q: Even after I disable compatibility mode in Internet Explorer version 8 or 9, the configuration utility does not appear. What should I do?

A: Make sure that the browser mode and document mode in the browser are set to the same version. To view the configuration, press F12. Set the values to either Internet Explorer 8 or Internet Explorer 9.

Q: When I access the NetScaler configuration utility by using Internet Explorer version 9, the utility displays the following error message: "You are not logged in. Please login." What should I do?

A: Make sure that the cookies are not blocked in your Interner Explorer settings. Go to **Tools** > **Internet Options**. Click the **Privacy** tab, and then under **Settings**, make sure that the slider is set to **Medium** or any lower value.

Q: I am using a MAC OS with JRE 1.7. After logging on to the configuration utility, I am not able to enter value in any of the text fields. What should I do?

A: Install Java 7, update 21 or higher.

Q: I am using a MAC OS. When I click outside a dialog window, the screen goes out of focus. Now, my browser looks disabled and hung. What should I do?

A: Click on the Java icon in the system dock, and in the JRE Security Warning window, click **Don't Block**. For details, see

http://www.oracle.com/technetwork/java/javase/7u21-relnotes-1932873.html

Q: Is there any compatibility issue in using JRE version 7_11 with the latest version of browsers?

A: Yes. Internet Explorer 9 and Firefox 18.0.1 block Java on computers running JRE version 7_11. You have to manually activate Java in the browser or upgrade to a later version of JRE (JRE 7_13).

High Availability

What are the various ports used to exchange the HA-related information between the nodes in an HA configuration?

In an HA configuration, both nodes use the following ports to exchange HArelated information:

- UDP Port 3003, to exchange heartbeat packets
- Port 3010, for synchronization and command propagation

What configurations are not synced or propagated in an HA configuration in either INC or non-INC mode?

Configurations implemented with the following commands are neither propagated nor synced to the secondary node:

- All node specific HA configuration commands. For example, add ha node, set ha node, and bind ha node.
- All Interface related configuration commands. For example, set interface and unset interface.
- All channel related configuration commands. For example, add channel, set channel, and bind channel.

Note: For more information about HA Configuration in INC mode, see Configuring High Availability Nodes in Different Subnets.

What configurations are not synced or propagated in an HA configuration in INC mode?

The following configurations are neither synced nor propagated. Each node has its own.

- MIPs
- SNIPs
- VLANs
- Routes (except LLB routes)
- Route monitors
- RNAT rules (except any RNAT rule with VIP as the NAT IP)
- Dynamic routing configurations.

What are the conditions that trigger synchronization?

Synchronization is triggered by any of the following conditions:

- The incarnation number of the primary node, received by the secondary, does not match that of the secondary node.

Note: Both nodes in an HA configuration maintain a counter called *incarnation number*, which counts the number of configurations in the node's configuration file. Each node sends its incarnation number to each other node in the heartbeat messages. The incarnation number is not incremented for the following commands:

- All HA configuration related commands. For example, add ha node, set ha node, and bind ha node.
- All Interface related commands. For example, set interface and unset interface.
- All channel-related commands. For example, add channel, set channel, and bind channel.

- The secondary node comes up after a restart.
- The primary node becomes secondary after a failover.

Does a configuration added to the secondary node get synchronized on the primary?

No, a configuration added to the secondary node is not synchronized to the primary.

What could be the reason for both nodes claiming to be the primary in an HA configuration?

The most likely reason is that the primary and secondary nodes are both healthy but the secondary does not receive the heartbeat packets from the primary. The problem could be with the network between the nodes.

Does an HA configuration run into any issues if you deploy the two nodes with different system clock settings?

Different system-clock settings on the two nodes can cause the following issues:

- The time stamps in the log file entries do not match. This situation makes it difficult to analyze the log entries for any issues.
- After a failover, you might have problems with any type of cookie based persistence for load balancing. A significant difference between the times can cause a cookie to expire sooner than expected, resulting in termination of the persistence session.
- Similar considerations apply to any time related decisions on the nodes.

What are the conditions for failure of the *force HA sync* command?

Forced synchronization fails in any of the following circumstances:

- You force synchronization when synchronization is already in progress.
- The secondary node is disabled.
- HA synchronization is disabled on the current secondary node.
- HA propagation is disabled on the current primary node and you force synchronization from the primary.

What are the conditions for failure of the *sync HA files* command?

Synchronizing configuration files fail if the secondary node is disabled.

In an HA configuration, if the secondary node takes over as the primary, does it switch back to secondary status if the original primary comes back online?

No. After the secondary node takes over as the primary, it remains as primary even if the original primary node comes back online again. To interchange the primary and secondary status of the nodes, run the *force failover* command.

What are the conditions for failure of the *force failover* command?

A forced failover fails in any of the following circumstances:

- The secondary node is disabled.
- The secondary node is configured to remain secondary.
- The primary node is configured to remain primary.
- The state of the peer node is unknown.

Hardware FAQs

Transceivers

Are transceivers shipped with the MPX 8005/8015/8200/8400/8600/8800 appliance?

No. Transceivers are available for purchase separately. Contact your Citrix sales representative to order transceivers for your appliance.

Are transceivers hot-swappable?

The 1G SFP transceiver is hot-swappable with release 9.3 build 42.2 or later on the following NetScaler appliances, which use the Intel e1k interface:

- MPX 7500/9500
- MPX 8005/8015/8200/8400/8600/8800
- MPX 9700/10500/12500/15500
- MPX 11500/13500/14500/16500/18500/20500

The 10G SFP+ transceiver is hot-swappable with release 9.3 build 57.5 or later on the following NetScaler appliances, which use the ixgbe (ix) interface:

- MPX 8005/8015/8200/8400/8600/8800
- MPX 9700/10500/12500/15500
- MPX 11500/13500/14500/16500/18500/20500
- MPX 17500/19500/21500
- MPX 17550/19550/20550/21550

Why does the 10G SFP+ transceiver autonegotiate to 1G speed?

Autonegotiation is enabled by default on the 10G SFP+ ports into which you insert your 10G SFP+ transceiver. When a link is established between the port and the network, the speed is autonegotiated. For example, if you connect the port to a 1G network, the speed is autonegotiated to 1G.

Can I insert a 1G transceiver into a 10G slot?

The 10G slot supports copper 1G transceivers, which can operate at up to 1 Gbps in a 10 Gbps slot.

Note that you cannot insert a 10G transceiver into a 1G slot.

The following table shows the compatibility matrix of transceivers and ports available on the NetScaler appliance.

Ports	Transceivers		
	10G	1G Fiber	1G Copper
10G	Supported	Not Supported	Supported
1G Fiber	Not Supported	Supported	Not Supported
1G Copper	Not Supported	Not Supported	Supported

What is QSFP+?

QSFP+ stands for Quad Small Form-factor Pluggable, which is a small, hot-pluggable transceiver for connecting data devices. This transceiver is used for 40G interfaces.

QSFP+ to Four SFP+ Copper Breakout Cables—These cables connect to four SFP+ 10GE ports of a NetScaler appliance on one end and to a QSFP+ 40G port of a Cisco switch on the other end.

Support for 40G connectivity—NetScaler models that have at least four 10G SFP+ ports connect to Cisco 40G interfaces by aggregating four of the 10G SFP+ ports to form a 40G link aggregation channel. QSFP to Four port SFP+ Copper Breakout Cable **QSFP-4SFP10G-CU3M (reports as L45593-D178-C30)**is used.

Which NetScaler appliances support the QSFP-4SFP10G-CU3M (reports as L45593-D178-C30) Breakout Cable?

NetScaler appliances that have at least four 10G SFP+ ports support this cable. The following appliances have at least four 10G SFP+ ports:

- MPX 11500/13500/14500/16500/18500/20500
- MPX 17550/19550/20550/21550
- MPX 11515/11520/11530/11540/11542
- MPX 22040/22060/22080/22100/22120
- MPX 24100/24150

QSFP-4SFP10G-CU3M breakout cable is supported by NetScaler release 9.3 build 65.8 or later, and release 10.1 build 122.17 or later.

Power Supplies

Is the power supply on the NetScaler MPX 5500 and MPX 5550/5650 appliances field replaceable?

No. The power supply on the NetScaler MPX 5500 and MPX 5550/5650 appliances is fixed.

Does the MPX 8005/8015/8200/8400/8600/8800 appliance ship with two power supplies?

No. The MPX 8005/8015/8200/8400/8600/8800 appliance supports dual power supplies but ships with one power supply. Contact your Citrix sales representative to order a second power supply.

How many power supplies are shipped with each platform?

The following table lists the number of power supplies shipped with each platform:

Platform	Number of Power Supplies shipped
MPX 5500	1
MPX 7500/9500	1 (You can order a second power supply.)
MPX 9700/10500/12500/15500	2
MPX 15000/17000	1 (You can order a second power supply.)
MPX 11500/13500/14500/16500/18500/20500	2
MPX 17500/19500/21500	1 (You can order a second power supply.)
MPX 17550/19550/20550/21550	2

Are power supplies hot-swappable?

Yes. If the appliance has two power supplies, you can replace one power supply without shutting down the appliance, provided the other power supply is working.

Rack and Rail

Do you have different rail kits for 1U and 2U appliances?

No. All MPX and SDX appliances use the same rail kit. The kit contains two pairs of slide rails, of different lengths, for a 1U and a 2U appliance.

Which rail kit should I buy?

The appliance ships with the standard 4-post rail kit that fits racks from 28-38 inches.

The compact 4-post rail kit for racks from 23-33 inches, or the 2-post rail kit for 2-post racks, has to be purchased separately. Contact your Citrix sales representative to order the appropriate kit.

What are the maximum and the minimum lengths of the outer rack rails?

The length of a standard outer rack rail is from 28 to 38 inches. The length of a shorter outer rack rail is from 23 to 33 inches.

What is the space required between the front post and rear post of the rack?

Standard racks require 28–38 inches between the front and rear posts. Shorter racks require from 23 to 33 inches.

How far can an appliance extend from the front post of the rack?

The chassis can extend up to 1.25 inches from the front post for all NetScaler MPX and SDX appliances.

How much space is required for maintaining the front and rear area of an appliance?

Minimum clearance areas of 36 inches for the front area and 24 inches for the rear area are required for maintenance of all NetScaler MPX and SDX appliances.

Lights Out Management (LOM) Port

Which LOM features are supported on the NetScaler MPX Appliance?

The MPX 8005/8015/8200/8400/8600/8800, MPX 11500/13500/14500/16500/18500/20500, and MPX 17550/19550/20550/21550 have an Intelligent Platform Management Interface (IPMI), also known as the Lights out Management (LOM) port, on the front panel of the appliance. The following three LOM features are supported on those platforms:

- Configuring the LOM port
- Power cycling the appliance
- Performing a core dump

Can the LOM interface be configured to accept only encrypted Virtual Network Computer (VNC) sessions on TCP port 5900?

Yes, customers who enable Transport Layer Security (TLS) on their LOM interface will have their VNC connections delivered over TLS as well.

For more information on LOM security guidelines, see Secure Deployment Guide for NetScaler MPX, VPX, and SDX Appliances.

Can the version of SSH used on the LOM interface be upgraded? Is there a patch available?

Individual components of the LOM cannot be upgraded independently. You must upgrade the entire LOM firmware as a package. The latest available LOM package can be found on the Citrix downloads website under LOM Firmware Upgrade.

Is it possible to add a third-party or self-signed SSL certificate to the LOM interface?

Yes, you can enable SSL on the latest binaries for third-party and self-signed SSL certificates, except on the 88XX models. On those models, the current LOM release does not support third-party certificates.

General

What is the recommended terminal emulator?

PuTTY.

Which platforms support Pay-As-You-Grow licenses?

The following platforms support Pay-As-You-Grow licenses:

- MPX 5550 to MPX 5650

- MPX 7500 to MPX 9500
- MPX 8005 to MPX 8015 to MPX 8200 to MPX 8400 to MPX 8600 to MPX 8800
- MPX 11500 to MPX 13500 to MPX 14500 to MPX 16500 to MPX 18500 to MPX 20500
- MPX 17500 to MPX 19500 to MPX 21500
- MPX 17550 to MPX 19550 to MPX 20550 to MPX 21550
- MPX 22040 to MPX 22060 to MPX 22080 to MPX 22100 to MPX 22120

Do you support direct attach cable (DAC)?

Yes, Citrix NetScaler appliances support a passive DAC in the following releases and builds:

- Release 9.3, build 63.4 and later
- Release 9.3.e, build 60.3007.e and later
- Release 10, build 74.2 and later
- Release 10.1, build 112.15 and later

Which port should I insert the DAC into?

DAC is inserted into the 10G port on the appliance.

Does the 1G port support DAC?

No. The DAC might fit into a 1G port but is not supported.

How can I order a DAC?

Contact your Citrix sales representative to order a DAC.

Can I mix DAC and fiber transceivers on the same appliance?

Yes. You can mix DAC and fiber transceivers on the same appliance. Each 10G port supports both options.

Can I mix SFP+ fiber and DAC in ports that are part of the same link aggregation channel (LAC)?

No. There must be symmetry between all elements in the same LAC.

Integrated Caching

Content Groups

How is a DEFAULT content group different from other content groups?

The behavior of the DEFAULT content group is exactly the same as any other group. The only attribute that makes the DEFAULT content group special is that if an object is being cached and no content group has been created, the object is cached in the DEFAULT group.

What is the 'cache-Control' option of the content group level?

You can send any cache-control header the browser. There is a content group level option, -cacheControl, which enables you to specify the cache-control header that you want to be inserted in the response to the browser.

What is the 'Minhit' option in content group level?

Minhit is an integer value specifying the minimum number of hits to a cache policy before the object is cached. This value is configurable at the content group level. Following is the syntax to configure this value from the command line interface.

add/set cache contentGroup <Content_Group_Name> [-minHits <Integer>]

What is the use of the expireAtLastByte option?

The expireAtLastByte option enables the integrated cache to expire the object as soon as it has been downloaded. Only requests that are outstanding requests at that time are served from cache. any new requests are sent to the server. This setting is useful when the object is frequently modified, as in the case of stock quotes. This expiry mechanism works along with the Flash Cache feature. To configure expireAtLastByte option, run the following command from the command line interface:

add cache contentGroup <Group_Name> -expireAtLastByte YES

Cache policy

What is a caching policy?

Policies determine which transactions are cacheable and which are not. Additionally, policies add or override the standard HTTP caching behavior. Policies determine an action, such as CACHE or NOCACHE, depending on the specific characteristics of the request or response. If a response matches policy rules, the object in the response is added to the content group configured in the policy. If you have not configured a content group, the object is added to the DEFAULT content group.

What is a policy hit?

A hit occurs when a request or response matches a cache policy.

What is a miss?

A miss occurs when a request or response does not match any cache policy. A miss can also occur if the request or response matches a cache policy but some override of RFC behavior prevents the object from being stored in the cache.

I have configured Integrated Caching feature of the NetScaler appliance. When adding the following policy, an error message appears. Is there any error in the command?

```
add cache policy image_caching -rule exp1 | ns_ext_not_jpeg –action
cache

> ERROR: No such command
```

In the preceding command, the expression should be within the quotation marks. Without quotation marks, the operator is considered to be the pipe operator.

Memory Requirements

What are the commands that I can run on the NetScaler appliance to check the memory allocated to cache?

To display the memory allocated for cache in the NetScaler appliance, run any of the following commands from the command line interface:

- show cache parameter

  In the output, check the value of the Memory usage limit parameter. This is the maximum memory allocated for cache.
- show cache <Content_Group_Name>

  In the output, check the values of the Memory usage and Memory usage limit parameters indicating the memory used and allocated for the individual content group.

My NetScaler appliance has 2 GB of memory. Is there any recommended memory limit for cache?

For any model of the NetScaler appliance, you can allocate half of the memory to the cache. However, Citrix recommends allocating a little less than half of the memory, because of internal memory dependency. You can run the following command to allocate 1 GB of memory to cache:

```
set cache parameter -memLimit 1024
```

Is it possible to allocate memory for individual content groups?

Yes. Even though you allocate memory for the integrated cache globally by running the set cache parameter –memlimit<Integer>, you can allocate memory to individual content groups by running the set cache <Content_Group_Name> –memLimit <Integer> command. The maximum memory you can allocate to content groups (combined) cannot exceed the memory you have allocated to the integrated cache.

What is the dependency of memory between integrated cache and TCP buffer?

If the NetScaler appliance has 2 GB memory, then the appliance reserves approximately 800 to 900 MB of memory and remaining is allocated to FreeBSD operating system. Therefore, you can allocate up to 512 MB of memory to integrated cache and the rest is allocated to TCP buffer.

Does it affect the caching process if I do not allocate global memory to the integrated cache?

If you do not allocate memory to integrated cache, all requests are sent to the server. To make sure that you have allocated memory to the integrated cache, run the show cache parameter command. Actually no objects will be cached if global memory is 0, so this needs to be set first.

Verification commands

What are the options for displaying cache statistics?

You can use either of the following options to display the statistics for cache:

- stat cache

  To display the summary of the cache statistics.

- stat cache –detail

  To display the full details of the cache statistics.

What are the options for displaying the cached content?

To display the cached content, you can run the show cache object command.

What is the command that I can run to display the characteristics of an object stored in cache?

If the object stored in the cache is, for example, GET //10.102.12.16:80/index.html, you can display the details about the object by running the following command from the command line interface of the appliance:

```
show cache object -url '/index.html' -host 10.102.3.96 -port 80
```

Is it mandatory to specify the group name as a parameter to display the parameterized objects in cache?

Yes. It is mandatory to specify the group name as a parameter to display the parameterized objects in cache. For example, consider that you have added the following policies with the same rule:

add cache policy p2 -rule ns_url_path_cgibin -action CACHE –storeInGroup g1
add cache policy p1 -rule ns_url_path_cgibin -action CACHE -storeInGroup g2

In this case, for the multiple requests, if policy p1 is evaluated, its hit counter is incremented and the policy stores the object in the g1 group, which has hit parameters. Therefore, you have to run the following command to display the objects from the

cache:

show cache object -url "/cgi-bin/setCookie.pl" -host 10.102.18.152 groupName g1

Similarly, for another set of multiple requests, if policy p2 is evaluated, its hit counter is incremented and the policy stores the object in the g2 group, which does not have hit parameters. Therefore, you have to run the following command to display the objects from the cache:

show cache object -url "/cgi-bin/setCookie2.pl" -host 10.102.18.152

I notice that there are some blank entries in the output of the nscachemgr command. What are those entries?

Consider the following sample output of the nscachemgr command. The blank entries in this output are highlighted in bold face for your reference:

root@ns# /netscaler/nscachemgr -a
//10.102.3.89:80/image8.gif
//10.102.3.97:80/staticdynamic.html
//10.102.3.97:80/
//10.102.3.89:80/image1.gif
//10.102.3.89:80/file5.html
//10.102.3.96:80/
//10.102.3.97:80/bg_logo_segue.gif
//10.102.3.89:80/file500.html
//10.102.3.92:80/
//10.102.3.96:80/cgi-bin/rfc/ccProxyReval.pl
Total URLs in IC = 10

The blank entries in the output are due to the default caching properties for GET / HTTP/1.1.

Flushing Objects

How can I flush a selective object from the cache?

You can identify an object uniquely by its complete URL. To flush such object, you can perform any of the following tasks:

- Flush cache
- Flush content group
- Flush the specific object

To flush the specific object, you have to specify the query parameters. You specify the invalParam parameter to flush the object. This parameter applies only to a query.

Does any change in the cache configuration trigger flushing of cache?

Yes. When you make any changes to the cache configuration, all the SET cache commands inherently flush the appropriate content groups.

I have updated the objects on the server. Do I need to flush the cached objects?

Yes. When you update objects on the server, you must flush the cached objects, or at least the relevant objects and content groups. The integrated cache is not affected by an update to the server. It continues to serve the cached objects until they expire.

Flash Cache

What is Flash Cache feature of the NetScaler appliance?

The phenomenon of Flash crowds occurs when a large number of clients access the same content. The result is a sudden surge in traffic toward the server. The Flash Cache feature enables the NetScaler appliance to improve performance in such situation by sending only one request to the server. All other requests are queued on the appliance and the single response is served to all of the requests. You can use either of the following commands to enable the Fast Cache feature:

- add cache contentGroup <Group_Name> -flashCache YES
- set cache contentGroup <Group_Name> -flashCache YES

What is the limit for Flash Cache clients?

The number of Flash Cache clients depends on the availability of resources on the NetScaler appliance.

Default Behaviour

Does the NetScaler appliance proactively receive objects upon expiry?

The NetScaler appliance never proactively receives objects on expiry. This is true even for the negative objects. The first access after expiry triggers a request to the server.

Does the integrated cache add clients to the queue for serving even before it starts receiving the response?

Yes. The integrated cache adds clients to the queue for serving even before it starts receiving the response.

What is the default value for the Verify cached object using parameter of the cache configuration?

HOSTNAME_AND_IP is the default value.

Does the NetScaler appliance create log entries in the log files?

Yes. The NetScaler appliance creates log entries in the log files.

Are compressed objects stored in the cache?

Yes. Compressed objects are stored in the cache.

Interoperability with other features

What happens to objects that are currently stored in cache and are being accessed though SSL VPN?

Objects stored in the cache and accessed regularly are served as cache hits when accessed through SSL VPN.

What happens to objects stored in the cache when accessed through SSL VPN and later accessed through a regular connection?

The objects stored through the SSL VPN access are served as a hit when accessed through the regular connection.

When using weblogging, how do I differentiate entries that indicate response served from cache from those served by the server?

For responses served from the integrated cache, the server log field contains the value IC. For responses served from a server, the server log field contains the value sent by the server. Following is a sample log entry for an integrated caching transaction:

"10.102.1.52 - "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 4.0; .NET CLR 1.0.3705)" "GET /" 200 0 "IC" 10.102.1.45"

Along with a client request, the response logged is the one sent to the client and not necessarily the one sent by the server.

Miscellaneous

What do you mean by configuring relexpiry and absexpiry?

By configuring relexpiry and absexpiry, it means that you are overriding the header irrespective of what appears in the header. You can configure different expiry setting and the content group level. With relexpiry, expiration of the header is based on the time at which the object was received by the NetScaler. With absexpiry, expiration is based on the time configured on the NetScaler. Relexpiry is configured in terms of seconds. Absexpiry is a time of day.

What do you mean by configuring weakpos and heuristic?

The weakpos and heuristic are like fall back values. If there is an expiry header, it is considered only if the last-modified header is present. The NetScaler appliance sets expiry on the basis of the last-modified header and the heuristic parameter. The heuristic expiry calculation determines the time to expiry by checking the last-modified header. Some percentage of the duration since the object was last modified is used as time to expiry. The heuristic of an object that remains unmodified for longer periods of time and is likely to have longer expiry periods. The –heurExpiryParam specifies what percentage value to use in this calculation. Otherwise, the appliance uses the weakpos value.

What should I consider before configuring dynamic caching?

If there is some parameter that is in name-value form and does not have the full URL query, or the appliance receives the parameter in a cookie header or POST body, consider configuring dynamic caching. To configure dynamic caching, you have to configure hitParams parameter.

How is hexadecimal encoding supported in the parameter names?

On the NetScaler appliance, the %HEXHEX encoding is supported in the parameter names. In the names that you specify for hitParams or invalParams, you can specify a name that contains %HEXHEX encoding in the names. For example, name, nam%65, and n%61m%65 are equivalent.

What is the process for selecting a hitParam parameter?

Consider the following excerpt of an HTTP header for a POST request:

How do we select a hitparam?
POST /data2html.asp?param1=value1&param2=&param3&param4=value4
HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, application/x-shockwave-flash, */*
Referer: http://10.102.3.97/forms.html
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: 10.102.3.97
Content-Length: 153
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDQGQGGRNY=NNLLKDADEENOAFLCCDGFGDMO
S1=This+text+is+only+text%2C+not+more+and+not+less%2C+%0D%0Ajust+text+to+be+itself%2C+namely+%2

In the above request, you can use S1 and B1, highlighted in bold face for your reference, as hitParams depending on your requirements. Additionally, if you use -matchCookies YES in the ASPSESSIONIDQGQGGRNY content group, then you can also use these parameters as hitParams.

What happens to the queued clients if the response is not cacheable?

If the response is not cacheable, all of the clients in the queue receive the same response that the first client receives.

Can I enable the Poll every time (PET) and Flash Cache features on the same content group?

No. You cannot enable PET and Flash Cache on the same content group. The integrated cache does not perform AutoPET function on Flash Cache content groups. The PET feature ensures that the integrated cache does not serve a stored object without consulting the server. You can configure PET explicitly for a content group.

When are the log entries created for the queued clients?

The log entries are created for the queued clients soon after the appliance receives the response header. The log entries are created only if the response header does not make the object non-cacheable.

What is the meaning of the DNS, HOSTNAME, and HOSTNAME_AND_IP values of the Verify cached object using parameter of the cache configuration?

The meanings are as follows:

- set cache parameter -verifyUsing HOSTNAME

  This ignores the destination IP address.

- set cache parameter -verifyUsing HOSTNAME_AND_IP

  This matches the destination IP address.

- set cache parameter -verifyUsing DNS

  This uses the DNS server.

I have set weakNegRelExpiry to 600, which is 10 minutes. I noticed that 404 responses are not getting cached. What is the reason ?

This completely depends on your configuration. By default, 404 responses are cached for 10 minutes. If you want all 404 responses to be fetched form the server, specify–weakNegRelExpiry 0. You can fine tune the –weakNegRelExpiry to a desired value, such as higher or lower to get the 404 responses cached appropriately. If you have configured –absExpiry for positive responses, then it might not yield desired results.

When the user accesses the site by using the Mozilla Firefox browser, the updated content is served. However, when the user accesses the site by using the Microsoft Internet Explorer browser, stale content is served. What could be the reason?

The Microsoft Internet Explorer browser might be taking the content from its local cache instead of the NetScaler integrated cache. The reason could be that the Microsoft Internet Explorer browser is not respecting the expiry related header in the response.

To resolve this issue, you can disable the local cache of the Internet Explorer and clear the offline content. After clearing the offline content, the browser should display the updated content

What if Hits are zero?

Check to see if the server time and NS time are in sync. And the weakPosrelexpiry limit set should bear the time difference between NS and server as shown below

root@ns180# date

Tue May 15 18:53:52 IST 2012

Why are policies getting hits but nothing is being cached?

Verify that memory is allocated to the integrated cache and that the allocation is greater than zero.

Is it possible to zero the cache counters?

There is no command line or GUI option for setting the cache counters to zero, and flushing the cache does not do so either. Rebooting the box automatically sets these counters to zero.

SDX

Basic Questions

What is SDX?

SDX is a true service delivery networking platform for enterprises and cloud datacenters. SDX features an advanced virtualization architecture that supports multiple NetScaler instances on a single hardware appliance.

When do I need SDX?

If you have multiple enterprise applications that have independent life cycle needs for L4–L7 networking services, or if you have a need to consolidate multiple underutilized load balancing appliances, you benefit from SDX.

What's unique about SDX?

SDX uniquely delivers key benefits from advancements in server hardware virtualization, hardware-assisted SSL acceleration, and the market-proven, award-winning NetScaler product line. The Management Service features an advanced control plane to unify provisioning, monitoring, and management in the most demanding multitenant environments, while providing full resource isolation for data separation and to meet service level agreement guarantees, such as availability, reliability, and performance.

How will I benefit from SDX?

SDX delivers isolated multitenancy with up to 40:1 consolidation. As a key pillar in Citrix's TriScale technology framework, SDX addresses the growing need to "scale in" within virtual data centers and cloud network infrastructures. The TriScale scale-in factor enables IT to provide the foundation for consolidating L4–L7 network services today, thereby simplifying the build-out of cloud based services down the line, in accordance with business requirements.

Will I need to go outside my normal procurement procedure to purchase SDX?

SDX is a fully contained networking appliance, designed for network deployment. SDX is not designed to be managed through standard hypervisor management tools such as XenCenter.

How do I purchase an SDX?

An SDX order has three basic product components: SDX appliance SKU, SDX support contract SKU, and Add-On Instance Packs. SKUs are also available for platform conversion (MPX-to-SDX) and platform upgrade (SDX-to-SDX). SDX today is available in Platinum Edition only.

Is there SDX-specific documentation?

Yes, please visit
http://support.citrix.com/proddocs/topic/netscaler/sdx-ag-wrapper-con.html.

Do NetScaler editions apply to NetScaler SDX?

The editions do not apply from a packaging perspective. NetScaler SDX appliances and the instance 5-packs are priced the same regardless of the edition. However, when provisioning new instances, the administrator is free to deploy the Standard, Enterprise, or Platinum edition of the NetScaler software.

Configuration

How much memory can I assign to each instance?

There is no maximum limit to the memory that can be assigned to each instance. Minimum memory required per instance is 2GB.

Can we migrate the existing configuration (ns.conf) from the MPX platform to SDX VPX instance?

Yes, but some configuration, such as RBA policies and SNMP community configuration, is deleted.

Features and Functionality

What NetScaler features do I get with SDX?

All NetScaler features are available on SDX.

Does SDX accelerate SSL in hardware like MPX does?

Yes. You can assign SSL cores to an instance during provisioning.

What changes to my network are required for me to deploy SDX?

SDX fits into your network environment through standard Ethernet interfaces. You must disable link aggregation control protocol (LACP) on any external switch ports connected to the appliance.

Is SDX interoperable with my routing and switching infrastructure?

Yes, although link aggregation control protocol (LACP) is currently not supported. However, SDX supports manual link aggregation.

Is SDX interoperable with my existing NetScaler deployment?

Yes, although standard VPX-to-MPX limitations apply. For example, high availability is supported only across homogeneous devices (you cannot pair a virtual device with a physical device), some configuration, such as RBA policies and SNMP configuration, is deleted, and license transfer is not supported.

Can I manage SDX from Command Center?

Yes. You can identify SDX appliances and provision and de-provision VPX instances by using Command Center.

How does SDX deliver multitenancy?

Each instance runs as a separate virtual machine with its own dedicated NetScaler kernel, CPU resources, memory resources, address space, and bandwidth allocation. Network I/O is done in a way that not only maintains aggregate system performance but also enables complete segregation of each tenant's data-plane and management-plane traffic.

Do I need to manage an SDX through XenCenter?

No. XenCenter is not supported. Use the Management Service to manage XenServer.

We are a VMware shop. We have no infrastructure available to support XenServer, do you have a VMware variant of SDX?

No additional XenServer infrastructure is necessary. SDX is a fully contained networking appliance with its own control plane, and the virtualization layer is transparent to the deployment.

Why is the system health monitoring page not showing any data?

You have to install the supplemental pack before you can use this feature. For installation instructions for the supplemental pack, see http://support.citrix.com/article/CTX132877.

How do I verify that the supplemental pack installation was successful?

After installation, a pop up window shows whether installation was successful or if there was an error.

Why is the VPX instance not reachable after interfaces on the appliance are modified?

When you provision a NetScaler VPX instance with L2VLAN configuration, physical interfaces on the SDX appliance are mapped to virtual interfaces on the VPX instance. If you remove an interface, you might change the mapping between the physical interfaces and VPX instances, and therefore you might lose connectivity to the VPX instance.

For example,

1. You provision a VPX instance, by using the Management Service, with interfaces 10/1, 10/2, 10/7, and tag VLAN 512 to interface 10/2. When you log on to that VPX instance, you see that interfaces 10/1, 10/2, and 10/3 are configured.

2. If you later modify the instance and remove interface 10/1, you lose connectivity to the instance, because interface 10/2 is renamed to 10/1 in the VPX instance.

Are IPv6 addresses supported on the NetScaler SDX appliance?

Yes. All NetScaler-supported IPv6 functionality is available on the SDX appliance.

Where are link parameters, such as speed and duplex, configured?

Link parameters are configured from the Management Service.

Should the appliance be restarted if the platform license is upgraded?

No. You do not need to restart the appliance for the new license to apply.

Do I need to restart the appliance to upgrade the device-level firmware?

Yes, this upgrade is handled through the Management Service and requires that the appliance be restarted. This is the only time that the SDX appliance needs a complete restart.

Do I need to restart the appliance when I upgrade it by using a Pay-As-You-Grow license?

No. Upgrading the appliance upgrades the platform license. Restart the Management Service but not the instances running on the SDX appliance. Once upgraded, the Management Service detects the higher throughput available for the instances. If you decide to increase the bandwidth limit for an instance, restart that instance after modifying the bandwidth limit.

What happens to production instances if I remove my platform license?

There is no change to the production instances. However, you cannot add new instances.

How can we readd a gadget to the Home page?

Click the << button in the top-right corner of the Home page. Then, type the name of the gadget, or press Enter for all gadgets. Click "Add to Dashboard".

Should member interfaces in manual link aggregation be part of same VLAN?

Yes. Member interfaces in manual link aggregation should be part of the same VLAN.

How many VLANs are supported per interface with VLAN filtering enabled? What happens if I configure more?

With VLAN filtering enabled, 10G interfaces support up to 63 VLANs, and 1G interfaces suppport up to 31 VLANs. This is a hard limit based on the number of the queues supported by the NIC. An error message appears if the limit is exceeded.

How many instances can be shared on a single NIC?

For a 10G interface, SDX supports up to 63 virtual functions per physical port, which translates to 63 instances per 10G NIC. For 1G interfaces, the maximum number of shared instances per NIC is 7.

Why is the XenServer password the same as the Management Service password?

The XenServer password and the Management Service password are the same to maintain administrative consistency. Changing the XenServer password causes the internal communication between the Management Service and XenServer to fail.

If I have separate management networks, do I need to manually add these networks to the Management Service?

No. Communication is over an external device.

Why can't I modify the default administrator profile?

The default administrator profile enables multiple administrative roles to exist on the SDX. You cannot change the password of the nsroot administrator profile, but you can

create a new administrator profile and make it the default profile.

Why does Core usage show 50% when I'm not passing any traffic through my NetScaler instance?

CPU core usage shows, from the hypervisor perspective, the CPU utilization of one physical CPU, which has two hyperthreads: one for the packet engine and one for the management CPU. For example, assume a single instance with one dedicated core. Even if you are not passing any traffic through your appliance, PE CPU utilization will be 100%, and average core utilization will be 50%.

Will restarting the Management Service interrupt my production instances?

No. Your production instances will continue to pass traffic without interruption while the Management Service restarts. The same applies when you upgrade the Management Service.

Can I configure the Management Service to send syslog?

Syslog through the Management Service is currently not supported.

Am I required to upgrade all VPX instances if I upgrade the Management Service?

No, instance life cycles can be managed independently of one other and of the life cycle of the Management Service.

If my Management Service and VPX instances are on different networks, how can I manage the VPX instance through HTTPS?

The same way as if they are on the same network.

If my Management Service and VPX instances are on different networks, how can I manage the VPX instance through the Management Service?

If the Management Service and the VPX instance are in different networks but the instance can be reached from Management Service, the Management Service shows the instance as UP. If an instance is UP, you can manage it from the Management Service. However, if communication between the two fails, the Management Service shows the instance as "Out of Service".

I forgot the IP address of my Management Service. What can I do?

Log on to XenServer, and then use the default IP address (169.254.0.10) to log on to the Management Service. At the shell prompt, type networkconfig to view or modify the IP address of the Management Service.

Can I specify VLANs on management interfaces?

VLANs on management interfaces are currently not supported.

How do I restart XenServer?

The only supported method for restarting XenServer is from the Management Service. It is equivalent to restarting the appliance.

How many instances can I provision on the SDX appliance? How much aggregate throughput can I expect?

This number is dependent on the hardware and the license that you purchased, as shown below:

- 11500, 13500, 14500, 16500, 18500, 20500—5 to 20 instances. Throughput ranges from 8 to 42 Gbps.
- 17500, 19500, 21500—5 to 20 instances. Throughput ranges from 20 to 50 Gbps.
- 17550, 19550, 20550, 21550—5 to 40 instances. Throughput ranges from 20 to 50 Gbps.
- 8400, 8600—2 to 5 instances. Throughput ranges from 4 to 6 Gbps.

Note: For more information, see the NetScaler datasheet at http://www.citrix.com/content/dam/citrix/en_us/documents/products/netscaler-data-sheet.pdf

Can I restrict functionality on the VPX instances?

Some functionality can be restricted by specifying the license (Standard, Enterprise, or Platinum) when you provision the instance.

Platforms

How many SDX models are there, and how do they differ?

The NetScaler SDX appliance comes in the following variants:

- SDX 11500/13500/14500/16500/18500/20500—8 to 42 Gbps, maximum 20 instances, 8x1G ports, 4x10G ports.
- SDX 17500/19500/21500—20 to 50 Gbps, maximum 20 instances, 8x10G ports.

  Note: This platform is going EOS this year.

- SDX 17550/19550/20550/ 21550—20 to 50 Gbps, maximum 40 instances, 8x10G ports.

What is the minimum NetScaler software version required for SDX instances?

NetScaler VPX instances should run release 9.3 and later to be able to work on SDX.

How many physical interfaces will I need to use?

If you have a single management network, you'll need on an average 1 or 2 physical NICs per instance. For 2 or more management networks (multiple VLANs for NetScaler IP addresses), you'll need a dedicated separate physical NIC for each management VLAN trunk. You can share physical NICs among multiple instances with L2 separation. Therefore, depending on your topology, you can offset the management VLAN trunk count with multiple instances sharing a physical NIC.

Can I upgrade my MPX to an SDX? What about my MPX FIPS platform?

A non-FIPS MPX platform that supports the SDX architecture can be converted to a similar class of SDX platform. The MPX platform must have a platinum license to be eligible for

this upgrade. This is a one way upgrade, and it wipes out the entire configuration on that MPX platform. For more information about this upgrade, see http://support.citrix.com/article/CTX129423.

How many SSL cards (cores) are supported on a NetScaler SDX appliance?

The number of SSL cards supported varies by the platform as follows:

- SDX 17500/19500/21500—16 cards.
- SDX 11500/13500/14500/16500/18500/20500—16 cards.
- SDX 17550/19550/20550/21550—36 cards.

Note: Instances cannot share SSL cores. Any SSL cores that are allocated at the time of provisioning an instance are dedicated to that instance.

Can I apply my VPX license to SDX?

No. NetScaler SDX and NetScaler VPX have different licensing models. One license cannot be used for the other.

Why are the hardware sensors not displayed on the NetScaler SDX 17500/19500/21500 appliance?

The NetScaler SDX 17500/19500/21500 is built on the MPX 17500/19500/21500 hardware platform. These appliance configurations do not support monitoring of hardware components.

When I upgraded my MPX to an SDX, the LCD panel went dark. Is that expected?

Yes, that is normal behavior. SDX does not support the LCD panel.

What are RX and TX errors on the NetScaler SDX appliance?

RX and TX errors include cyclic redundancy check (CRC) errors and small or runt packet errors.

What happens if a hardware component is removed from the SDX appliance?

If a hardware component is physically removed from the appliance, it no longer appears in the Management Service user interface.

Do I need to restart my appliance after I reconfigure VLAN filtering?

No. However, you need to restart the VPX instances that are affected by this change. The Management Service restarts the affected instances if you select "Reboot associated Instances" in the Enable/Disable VLAN Filter dialog box.

What is the NMI button for on the SDX appliance?

The NMI button is not operational on the SDX appliance.

SSL

Basic Questions

HTTPS access to the NetScaler configuration utility fails on a VPX instance. How do I gain access?

A certificate-key pair is required for HTTPS access to the NetScaler configuration utility. On a NetScaler ADC, a certificate-key pair is automatically bound to the internal services. On an MPX or SDX appliance, the default key size is 1024 bytes, and on a VPX instance, the default key size is 512 bytes. However, most browsers today do not accept a key that is less than 1024 bytes. As a result, HTTPS access to the VPX configuration utility is blocked.

Citrix recommends that you install a certificate-key pair of at least 1024 bytes and bind it to the internal service for HTTPS access to the configuration utility or update the ns-server-certificate to 1024 bytes. You can use HTTP access to the configuration utility or the NetScaler command line to install the certificate.

If I add a license to an MPX appliance, the certificate-key pair binding is lost. How do I resolve this problem?

If a license is not present on an MPX appliance when it starts, and you add a license later and restart the appliance, you might lose the certificate binding. You must reinstall the certificate and bind it to the internal service

Citrix recommends that you install an appropriate license before starting the appliance.

What are the various steps involved in setting up a secure channel for an SSL transaction?

Setting up a secure channel for an SSL transaction involves the following steps:

1. The client sends an HTTPS request for a secure channel to the server.
2. After selecting the protocol and cipher, the server sends its certificate to the client.
3. The client checks the authenticity of the server certificate.
4. If any of the checks fail, the client displays the corresponding feedback.
5. If the checks pass or the client decides to continue even if a check fails, the client creates a temporary, disposable key called the *pre-master secret* and encrypts it by using the public key of the server certificate.
6. The server, upon receiving the pre-master secret, decrypts it by using the server's private key and generates the session keys. The client also generates the session keys from the pre-master secret. Thus both client and server now have a common session key, which is used for encryption and decryption of application data.

I understand that SSL is a CPU-intensive process. What is the CPU cost associated with the SSL process?

The following two stages are associated with the SSL process:

- The initial handshake and secure channel setup by using the public and private key technology.
- Bulk data encryption by using the asymmetric key technology.

Both of the preceding stages can affect server performance, and they require intensive CPU processing for of the following reasons:

1. The initial handshake involves public-private key cryptography, which is very CPU intensive because of large key sizes (1024bit, 2048bit, 4096bit).
2. Encryption/decryption of data is also computationally expensive, depending on the amount of data that needs to be encrypted or decrypted.

What are the various entities of an SSL configuration?

An SSL configuration has the following entities:

- Server certificate
- Certificate Authority (CA) certificate
- Cipher suite that specifies the protocols for the following tasks:
  - Initial key exchange
  - Server and client authentication
  - Bulk encryption algorithm
  - Message authentication
- Client authentication
- CRL
- SSL Certificate Key Generation Tool that enables you to create the following files:
  - Certificate request
  - Self signed certificate
  - RSA and DSA keys
  - DH parameters

I want to use the SSL offloading feature of the Citrix NetScaler appliance. What are the various options for receiving an SSL certificate?

You must receive an SSL certificate before you can configure the SSL setup on the Citrix NetScaler appliance. You can use any of the following methods to receive an SSL certificate:

- Request a certificate from an authorized CA.
- Use the existing server certificate.
- Create a certificate-key pair on the Citrix NetScaler appliance.

Note: This is a test certificate signed by the test Root-CA generated by the NetScaler. Test certificates signed by this Root-CA are not accepted by browsers. The browser throws a warning message stating that the server's certificate cannot be authenticated.

- For anything other than test purposes, you must provide a valid CA certificate and CA key to sign the server certificate.

What are the minimum requirements for an SSL setup?

The minimum requirements for configuring an SSL setup are as follows:

- Obtain the certificates and keys.
- Create a load balancing SSL virtual server.
- Bind HTTP or SSL services to the SSL virtual server.
- Bind certificate-key pair to the SSL virtual server.

What are the limits for the various components of SSL?

SSL components have the following limits:

- Bit size of SSL certificates: 4096.
- Number of SSL certificates: Depends on the available memory on the appliance.
- Maximum linked intermediate CA SSL certificates: 9 per chain.
- CRL revocations: Depends on the available memory on the appliance.

What are the various steps involved in the end-to-end data encryption on a Citrix NetScaler appliance?

The steps involved in the server-side encryption process on a Citrix NetScaler appliance are as follows:

1. The client connects to the SSL VIP configured on the Citrix NetScaler appliance at the secure site.
2. After receiving the secure request, the appliance decrypts the request, applies layer 4-7 content switching techniques and load balancing policies, and selects the best available backend Web server for the request.
3. The Citrix NetScaler appliance creates an SSL session with the selected server.
4. After establishing the SSL session, the appliance encrypts the client request and sends it to the Web server by using the secure SSL session.
5. When the appliance receives the encrypted response from the server, it decrypts and re-encrypts the data, and sends the data to the client by using the client side SSL session.

The multiplexing technique of the Citrix NetScaler appliance enables the appliance to reuse SSL sessions that have been established with the Web servers. Therefore, the appliance avoids the CPU intensive key exchange, known as *full handshake*. This process reduces the overall number of SSL sessions on the server and maintains end-to-end security.

Certificates and Keys

Can I place the certificate and key files at any location? Is there any recommended location to store these files?

You can store the certificate and key files on the Citrix NetScaler appliance or a local computer. However, Citrix recommends that you store the certificate and key files in the /nsconfig/ssl directory of the Citrix NetScaler appliance. The /etc directory exists in the flash memory of the Citrix NetScaler appliance. This provides portability and facilitates backup and restoration of the certificate files on the appliance.

Note: Make sure that the certificate and the key files are stored in the same directory.

What is the maximum size of the certificate key supported on the Citrix NetScaler appliance?

A Citrix NetScaler appliance running a software release earlier than release 9.0 supports a maximum certificate key size of 2048 bits. Release 9.0 and later support a maximum certificate key size of 4096 bits. This limit is applicable to both RSA and DSA certificates.

An MPX appliance supports certificates from 512-bits up to the following sizes:

- 4096-bit server certificate on the virtual server
- 4096-bit client certificate on the service
- 4096-bit CA certificate (includes intermediate and root certificates)
- 4096-bit certificate on the back end server
- 4096-bit client certificate (if client authentication is enabled on the virtual server)

A virtual appliance supports certificates from 512-bits up to the following sizes:

- 4096-bit server certificate on the virtual server
- 4096-bit client certificate on the service
- 4096-bit CA certificate (includes intermediate and root certificates)
- 2048-bit certificate on the back end server
- 2048-bit client certificate (if client authentication is enabled on the virtual server)

What is the maximum size of the DH parameter supported on the Citrix NetScaler appliance?

The Citrix NetScaler appliance supports a DH parameter of maximum 2048 bits.

What is the maximum certificate-chain length, that is, the maximum number of certificates in a chain, supported on a Citrix NetScaler appliance?

A Citrix NetScaler appliance can send a maximum of 10 certificates in a chain when sending a server certificate message. A chain of the maximum length includes the server certificate and nine intermediate CA certificates.

What are the various certificate and key formats supported on the Citrix NetScaler appliance?

The Citrix NetScaler appliance supports the following certificate and key formats:

- Privacy Enhanced Mail (PEM)
- Distinguished Encoding Rule (DER)

Is there a limit for the number of certificates and keys that I can install on the Citrix NetScaler appliance?

No. The number of certificates and keys that can be installed is limited only by the available memory on the Citrix NetScaler appliance.

I have saved the certificate and key files on the local computer. I want to transfer these files to the Citrix NetScaler appliance by using the FTP protocol. Is there any preferred mode for transfering these files to the Citrix NetScaler appliance?

Yes. If using the FTP protocol, you should use binary mode to transfer the certificate and key files to the Citrix NetScaler appliance.

Note: By default, FTP is disabled. Citrix recommends using the SCP protocol for transferring certificate and key files. The configuration utility implicitly uses SCP to connect to the appliance.

What is the default directory path for the certificate and key?

The default directory path for the certificate and key is /nsconfig/ssl.

When adding a certificate and key pair, what happens if I do not specify an absolute path to the certificate and key files?

When adding a certificate and key pair, if you do not specify an absolute path to the certificate and key files, the Citrix NetScaler appliance searches the default directory, /nsconfig/ssl, for the specified files and attempts to load them to the kernel. For example, if the cert1024.pem and rsa1024.pem files are available in the /nsconfig/ssl directory of the appliance, both of the following commands are successful:

```
add ssl certKey cert1 -cert cert1204.pem -key rsa1024.pem

add ssl certKey cert1 -cert /nsconfig/ssl/cert1204.pem -key
/nsconfig/ssl/rsa1024.pem
```

I have configured a high availability setup. I want to implement the SSL feature on the setup. How should I handle the certificate and key files in a high availability setup?

In a high availability setup, you must store the certificate and key files on both the primary and the secondary Citrix NetScaler appliance. The directory path for the certificate and key files must be the same on both appliances before you add an SSL certificate-key pair on the primary appliance.

Ciphers

What is a NULL-Cipher?

Ciphers with no encryption are known as NULL-Ciphers. For example, NULL-MD5 is a NULL-Cipher.

Are the NULL-Ciphers enabled by default for an SSL VIP or an SSL service?

No. NULL-Ciphers are not enabled by default for an SSL VIP or an SSL service.

What is the procedure to remove NULL-Ciphers?

To remove the NULL-Ciphers from an SSL VIP, run the following command:

bind ssl cipher <SSL_VIP> REM NULL

To remove the NULL-Ciphers from an SSL Service, run the following command:

```
bind ssl cipher <SSL_Service> REM NULL -service
```

What are the various cipher aliases supported on the Citrix NetScaler appliance?

The Citrix NetScaler appliance supports the following cipher aliases:

1. Alias Name: ALL

   Description: All NetScaler-supported ciphers, excluding NULL ciphers

2. Alias Name: DEFAULT

   Description: Default cipher list with encryption strength >= 128bit

3. Alias Name: kRSA

   Description: Ciphers with RSA key exchange algorithm

4. Alias Name: kEDH

   Description: Ciphers with Ephemeral-DH key exchange algorithm

5. Alias Name: DH

   Description: Ciphers with DH key exchange algorithm

6. Alias Name: EDH

   Description: Ciphers with DH key exchange algorithm and authentication algorithm

7. Alias Name: aRSA

   Description: Ciphers with RSA authentication algorithm

8. Alias Name: aDSS

   Description: Ciphers with DSS authentication algorithm

9. Alias Name: aNULL

   Description: Ciphers with NULL authentication algorithm

10. Alias Name: DSS

    Description: Ciphers with DSS authentication algorithm

11. Alias Name: DES

    Description: Ciphers with DES encryption algorithm

12. Alias Name: 3DES

    Description: Ciphers with 3DES encryption algorithm

13. Alias Name: RC4

    Description: Ciphers with RC4 encryption algorithm

14. Alias Name: RC2

    Description: Ciphers with RC2 encryption algorithm

15. Alias Name: eNULL

    Description: Ciphers with NULL encryption algorithm

16. Alias Name: MD5

    Description: Ciphers with MD5 message authentication code (MAC) algorithm

17. Alias Name: SHA1

    Description: Ciphers with SHA-1 MAC algorithm

18. Alias Name: SHA

    Description: Ciphers with SHA MAC algorithm

19. Alias Name: NULL

    Description: Ciphers with NULL encryption algorithm

20. Alias Name: RSA

    Description: Ciphers with RSA key exchange algorithm and authentication algorithm

21. Alias Name: ADH

    Description: Ciphers with DH key exchange algorithm, and NULL authentication algorithm

22. Alias Name: SSLv2

    Description: SSLv2 protocol ciphers

23. Alias Name: SSLv3

    Description: SSLv3 protocol ciphers

24. Alias Name: TLSv1

    Description: SSLv3/TLSv1 protocol ciphers

25. Alias Name: TLSv1_ONLY

    Description: TLSv1 protocol ciphers

26. Alias Name: EXP

    Description: Export ciphers

27. Alias Name: EXPORT

    Description: Export ciphers

28. Alias Name: EXPORT40

    Description: Export ciphers with 40-bit encryption

29. Alias Name: EXPORT56

    Description: Export ciphers with 56-bit encryption

30. Alias Name: LOW

    Description: Low strength ciphers (56-bit encryption)

31. Alias Name: MEDIUM

    Description: Medium strength ciphers (128-bit encryption)

32. Alias Name: HIGH

    Description: High strength ciphers (168-bit encryption)

33. Alias Name: AES

    Description: AES ciphers

34. Alias Name: FIPS

    Description: FIPS-approved ciphers

What is the command to display all the predefined ciphers of the Citrix NetScaler appliance?

To display all the predefined ciphers of the Citrix NetScaler appliance, at the NetScaler command line, type:

show ssl cipher

What is the command to display the details of an individual cipher of the Citrix NetScaler appliance?

To display the details of an individual cipher of the Citrix NetScaler appliance, at the NetScaler command line, type:

show ssl cipher <Cipher_Name/Cipher_Alias_Name/Cipher_Group_Name>

Example:

```
 > show cipher SSL3-RC4-SHA
 1) Cipher Name: SSL3-RC4-SHA
 Description: SSLv3 Kx=RSA Au=RSA Enc=RC4(128)
Mac=SHA1
 Done
```

What is the significance of adding the predefined ciphers of the Citrix NetScaler appliance?

Adding the predefined ciphers of the Citrix NetScaler appliance causes the NULL-Ciphers to get added to an SSL VIP or an SSL service.

Certificates

Why do I need to bind the server certificate?

Binding the server certificates is the basic requirement for enabling the SSL configuration to process SSL transactions.

To bind the server certificate to an SSL VIP, at the NetScaler command line, type:

bind ssl vserver <vServerName> -certkeyName <cert_name>

To bind the server certificate to an SSL service, at the NetScaler command line, type:

bind ssl service <serviceName> -certkeyName <cert_name>

How many certificates can I bind to an SSL VIP or an SSL service?

On a NetScaler virtual appliance, you can bind a maximum of two certificates to an SSL VIP or an SSL service, one each of type RSA and type DSA. On a NetScaler MPX or MPX-FIPS appliance, if SNI is enabled, you can bind multiple server certificates of type RSA. If SNI is disabled, you can bind a maximum of one certificate of type RSA.

Note: DSA certificates are not supported on MPX or MPX-FIPS platforms.

Does SNI support Subject Alternative Name (SAN) certificates?

No. On a NetScaler appliance, SNI is not supported with a SAN extension certificate.

What happens if I unbind or overwrite a server certificate?

When you unbind or overwrite a server certificate, all the connections and SSL sessions created by using the existing certificate are terminated. When you overwrite an existing certificate, the following message appears:

```
ERROR:

Warning: Current certificate replaces the previous binding.
```

How do I install an intermediate certificate on Citrix NetScaler and link to a server certificate?

See the article at http://support.citrix.com/article/ctx114146 for information about installing an intermediate certificate.

Why am I am getting a "resource already exists" error when I try to install a certificate on the Citrix NetScaler?

See the article athttp://support.citrix.com/article/CTX117284 for instructions for resolving the "resource already exists" error.

I want to create a server certificate on a Citrix NetScaler appliance to test and evaluate the product. What is the procedure to create a server certificate?

Perform the following procedure to create a test certificate.

Note: A certificate created with this procedure cannot be used to authenticate all the users and browsers. After using the certificate for testing, you should obtain a server certificate signed by an authorized Root CA.

To create a self-signed server certificate:

1. To create a Root CA certificate, at the NetScaler command line, type:

   create ssl rsakey /nsconfig/ssl/test-ca.key 1024

   create ssl certreq /nsconfig/ssl/test-ca.csr -keyfile /nsconfig/ssl/test-ca.key

   Enter the required information when prompted, and then type the following command:

   create ssl cert /nsconfig/ssl/test-ca.cer /nsconfig/ssl/test-ca.csr ROOT_CERT -keyfile /nsconfig/ssl/test-ca.key

2. Perform the following procedure to create a server certificate and sign it with the root CA certificate that you just created

   a. To create the request and the key, at the NetScaler command line, type:

      create ssl rsakey /nsconfig/ssl/test-server.key 1024

      create ssl certreq /nsconfig/ssl/test-server.csr -keyfile /nsconfig/ssl/test-server.key

   b. Enter the required information when prompted.

   c. To create a serial-number file, at the NetScaler command line, type:

      shell
      # echo '01' > /nsconfig/ssl/serial.txt

```
# exit
```

3. To create a server certificate signed by the root CA certificate created in step 1, at the NetScaler command line, type:

   create ssl cert /nsconfig/ssl/test-server.cer /nsconfig/ssl/test-server.csr SRVR_CERT -CAcert /nsconfig/ssl/test-ca.cer -CAkey /nsconfig/ssl/test-ca.key -CAserial /nsconfig/ssl/serial.txt

4. To create a Citrix NetScaler certkey, which is the in-memory object that holds the server certificate information for SSL handshakes and bulk encryption, at the NetScaler command line, type:

   add ssl certkey test-certkey -cert /nsconfig/ssl/test-server.cer -key /nsconfig/ssl/test-server.key

5. To bind the certkey object to the SSL virtual server, at the NetScaler command line, type:

   bind ssl vserver <vServerName> -certkeyName <cert_name>

I have received a Citrix NetScaler appliance on which Citrix NetScaler software release 9.0 is installed. I have noticed an additional license file on the appliance. Is there any change in the licensing policy starting with Citrix NetScaler software release 9.0?

Yes. Starting with Citrix NetScaler software release 9.0, the appliance might not have a single license file. The number of license files depends on the Citrix NetScaler software release edition. For example, if you have installed the Enterprise edition, you might need additional license files for the full functionality of the various features. However, if you have installed the Platinum edition, the appliance has only one license file.

How do I export the certificate from Internet Information Service (IIS)?

There are many ways to do this, but by using the following method the appropriate certificate and private key for the Web site are exported. This procedure **must** be performed on the actual IIS server.

1. Open the Internet Information Services (IIS) Manager administration tool.
2. Expand the Web Sites node and locate the SSL-enabled Web site that you want to serve through the Citrix NetScaler.
3. Right-click this Web site and click Properties.
4. Click the Directory Security tab and, in the Secure Communications section of the window, select the View Certificate box.
5. Click the Details tab, and then click Copy to File.
6. On the Welcome to the Certificate Export Wizard page, click Next.
7. Select Yes, export the private key and click Next.

   Note: The private key MUST be exported for SSL Offload to work on the Citrix NetScaler

8. Make sure that the Personal Information Exchange -PKCS #12 radio button is selected, and select *only* the Include all certificates in the certification path if possible check box. Click Next.

9. Enter a password and click Next.

10. Enter a file name and location, and then click Next. Give the file an extension of .PFX.

11. Click Finish.

How do I convert the PKCS#12 certificate and install it on the Citrix NetScaler?

1. Move the exported .PFX certificate file to a location from where it may be copied to the Citrix NetScaler (that is, to a machine that permits SSH access to the management interface of a Citrix NetScaler appliance). Copy the certificate to the appliance by using a secure copy utility such as SCP.

2. Access the BSD shell and convert the certificate (for example, cert.PFX) to .PEM format:

   ```
   root@ns# openssl pkcs12 -in cert.PFX -out cert.PEM
   ```

3. To make sure that the converted certificate is in correct x509 format, verify that the following command produces no error:

   ```
   root@ns# openssl x509 -in cert.PEM -text
   ```

4. Verify that the certificate file contains a private key. Begin by issuing the following command:

   ```
   root@ns# cat cert.PEM
   ```

   Verify that the output file includes an RSA PRIVATE KEY section.

   ```
   -----BEGIN RSA PRIVATE KEY-----
    Mkm^s9KMs9023pz/s...
    -----END RSA PRIVATE KEY-----
   ```

   The following is another example of an RSA PRIVATE KEY section:

   ```
    Bag Attributes
   1.3.6.1.4.1.311.17.2: <No Values>
   localKeyID: 01 00 00 00
   Microsoft CSP Name: Microsoft RSA SChannel Cryptographic
   Provider
   friendlyName:
   4b9cef4cc8c9b849ff5c662fd3e0ef7e_76267e3e-6183-4d45-886e-6e067297b38f

   Key Attributes
   X509v3 Key Usage: 10
   -----BEGIN RSA PRIVATE KEY-----
   Proc-Type: 4,ENCRYPTED
   DEK-Info: DES-EDE3-CBC,43E7ACA5F4423968
   ```

pZJ2SfsSVqMbRRf6ug37Clua5gY0Wld4frPIxFXyJquUHr31dilW5ta3hbIaQ+Rg

... (more random characters)
v8dMugeRplkaH2Uwt/mWBk4t71Yv7GeHmcmjafK8H8iW80ooPO3D/ENV8X4U/tlh

5eU6ky3WYZ1BTy6thxxLlwAullynVXZEflNLxq1oX+ZYl6djgjE3qg==
-----END RSA PRIVATE KEY-----

The following is a SERVER CERTIFICATE section:

Bag Attributes
localKeyID: 01 00 00 00
friendlyName: AG Certificate
subject=/C=AU/ST=NSW/L=Wanniassa/O=Dave Mother Asiapacific/OU=Support/CN=davemother.food.lan
issuer=/DC=lan/DC=food/CN=hotdog
-----BEGIN CERTIFICATE-----
MIIFiTCCBHGgAwIBAgIKCGryDgAAAAAHzANBgkqhkiG9w0BAQUFADA8MRMwEQYK

... (more random characters) 5pLDWYVHhLkA1pSxvFjNJHRSIydWHc5ltGyKqIUcBezVaXyel94pNSUYx07N

MY2ovQyQZM8gGe3+lGFum0VHbv/y/gB9HhFesog=
-----END CERTIFICATE-----

The following is an INTERMEDIATE CA CERTIFICATE section:

Bag Attributes: <Empty Attributes>
subject=/DC=lan/DC=food/CN=hotdog
issuer=/DC=lan/DC=food/CN=hotdog
-----BEGIN CERTIFICATE-----
MIIESDCCAzCgAwIBAgIQah20fCRYTY9LRXYMIRaKGjANBgkqhkiG9w0BAQUFADA8

... (more random characters) Nt0nksawDnbKo86rQcNnY5xUs7c7pj2zxj/IOsgNHUp5W6dDI9pQoqFFaDk=

-----END CERTIFICATE-----

Further Intermediate CA certificates may follow, depending on the certification path of the exported certificate.

5. Open the .PEM file in a text editor
6. Locate the first line of the .PEM file and the first instance of the following line, and copy those two lines and all the lines between them:

   ```
   -----END CERTIFICATE-----
   ```

   Note: Make sure that last copied line is the first `-----END CERTIFICATE-----` line in the .PEM file.

7. Paste the copied lines into a new file. Call the new file something intuitive, such as `cert-key.pem`. This is the certificate-key pair for the server hosting the HTTPS service. This file should contain both the section labeled `RSA PRIVATE KEY` and the section labeled `SERVER CERTIFICATE` in the example above.

Note: The certificate-key pair file contains the private key and must therefore be kept secure.

8. Locate any subsequent sections beginning with `-----BEGIN CERTIFICATE-----` and ending with `---END CERTIFICATE-----`, and copy each such section to a separate new file.

   These sections correspond to certificates of trusted CAs that have been included in the certification path. These sections should be copied and pasted into new individual files for these certificates. For example, the INTERMEDIATE CA CERTIFICATE section of the example above should be copied and pasted into a new file).

   For multiple intermediate CA certificates in the original file, create new files for each intermediate CA certificate in the order in which they appear in the file. Keep track (using appropriate filenames) of the order in which the certificates appear, as they need to be linked together in the correct order in a later step.

9. Copy the certificate-key file (`cert-key.pem`) and any additional CA certificate files into the /nsconfig/ssl directory on the Citrix NetScaler.

10. Exit the BSD shell and access the Citrix NetScaler prompt.

11. Follow the steps in "Install the certificate-key files on the appliance" to install the key/certificate once uploaded on the device.

How do I convert the PKCS#7 certificate and install it on the NetScaler appliance?

You can use OpenSSL to convert a PKCS #7 Certificate to a format recognizable by the NetScaler appliance. The procedure is identical to the procedure for PKCS #12 certificates, except that you invoke OpenSSL with different parameters. The steps for converting PKCS #7 certificates are as follows:

1. Copy the certificate to the appliance by using a secure copy utility, such as SCP.

2. Convert the certificate (for example, cert.P7B) to PEM format:

   ```
   > openssl pkcs7 -inform DER -in cert.p7b -print_certs -text -out
   cert.pem
   ```

3. Follow steps 3 through 7 as described in the answer to Q32 for PKCS #12 certificates.

Note: Before loading the converted PKCS #7 certificate to the appliance, be sure to verify that it contains a private key, exactly as described in step 3 for the PKCS #12 procedure. PKCS #7 certificates, particularly those exported from IIS, do not typically contain a private key.

When I bind a cipher to a virtual server or service by using the bind cipher command, I see the error message "Command deprecated."

The command for binding a cipher to a virtual server or service has changed.

Use the bind ssl vserver <vsername> -ciphername <ciphername> command to bind an SSL cipher to an SSL virtual server.

Use the bind ssl service <serviceName> -ciphername <ciphername> command to bind an SSL cipher to an SSL service.

Note: New ciphers and cipher groups are added to the existing list and not replaced.

Why can't I create a new cipher group and bind ciphers to it by using the add cipher command?

The add cipher command functionality has changed in release 10. The command only creates a cipher group. To add ciphers to the group, use the bind cipher command.

OpenSSL

How do I install the OpenSSL toolkit?

See the article at http://support.citrix.com/article/ctx106627.

How do I use OpenSSL to convert certificates between PEM and DER?

To use OpenSSL, you must have a working installation of the OpenSSL software and be able to execute Openssl from the command line.

x509 certificates and RSA keys can be stored in a number of different formats.

Two common formats are DER (a binary format used primarily by Java and Macintosh platforms) and PEM (a base64 representation of DER with header and footer information, which is used primarily by UNIX and Linux platforms). There is also an obsolete NET (Netscape server) format that was used by earlier versions of IIS (up to and including 4.0) and various other less common formats that are not covered in this article.

A key and the corresponding certificate, as well as the root and any intermediate certificates, can also be stored in a single PKCS#12 (.P12, .PFX) file.

Procedure

Use the Openssl command to convert between formats as follows:

1. To convert a certificate from PEM to DER:

   ```
   x509 -in input.crt -inform PEM -out output.crt -outform DER
   ```

2. To convert a certificate from DER to PEM:

   ```
   x509 -in input.crt -inform DER -out output.crt -outform PEM
   ```

3. To convert a key from PEM to DER:

   ```
   rsa -in input.key -inform PEM -out output.key -outform DER
   ```

4. To convert a key from DER to PEM:

   ```
   rsa -in input.key -inform DER -out output.key -outform PEM
   ```

Note: If the key you are importing is encrypted with a supported symmetric cipher, you are prompted to enter the pass-phrase.

Note: To convert a key to or from the obsolete NET (Netscape server) format, substitute NET for PEM or DER as appropriate. The stored key is encrypted in a weak unsalted RC4 symmetric cipher, so a pass-phrase will be requested. A blank pass-phrase is acceptable.

System Limits

What are the important numbers to remember?

1. Create Certificate Request:
    - Request File Name: Maximum 63 characters
    - Key File Name: Maximum 63 characters
    - PEM Passphrase (For Encrypted Key): Maximum 31 characters
    - Common Name: Maximum 63 characters
    - City: Maximum 127 characters
    - Organization Name: Maximum 63 characters
    - State/Province Name: Maximum 63 characters
    - Email Address: Maximum 39 Characters
    - Organization Unit: Maximum 63 characters
    - Challenge Password: Maximum 20 characters
    - Company Name: Maximum 127 characters
2. Create Certificate:
    - Certificate File Name: Maximum 63 characters
    - Certificate Request File Name: Maximum 63 characters
    - Key File Name: Maximum 63 characters
    - PEM Passphrase: Maximum 31 characters
    - Validity Period: Maximum 3650 days
    - CA Certificate File Name: Maximum 63 characters
    - CA Key File Name: Maximum 63 characters
    - PEM Passphrase: Maximum 31 characters
    - CA Serial Number File: Maximum 63 characters

3. Create and Install a Server Test Certificate:
    - Certificate File Name: Maximum 31 characters
    - Fully Qualified Domain Name: Maximum 63 characters
4. Create Diffie-Hellman (DH) key:
    - DH Filename (with path): Maximum 63 characters
    - DH Parameter Size: Maximum 2048 bits
5. Import PKCS12 key:
    - Output File Name: Maximum 63 characters
    - PKCS12 File Name: Maximum 63 characters
    - Import Password: Maximum 31 characters
    - PEM Passphrase: Maximum 31 characters
    - Verify PEM Passphrase: Maximum 31 characters
6. Export PKCS12
    - PKCS12 File Name: Maximum 63 characters
    - Certificate File Name: Maximum 63 characters
    - Key File Name: Maximum 63 characters
    - Export Password: Maximum 31 characters
    - PEM Passphrase: Maximum 31 characters
7. CRL Management:
    - CA Certificate File Name: Maximum 63 characters
    - CA Key File Name: Maximum 63 characters
    - CA Key File Password: Maximum 31 characters
    - Index File Name: Maximum 63 characters
    - Certificate File Name: Maximum 63 characters
8. Create RSA Key:
    - Key Filename: Maximum 63 characters
    - Key Size: Maximum 4096 bits
    - PEM Passphrase: Maximum 31 characters
    - Verify Passphrase: Maximum 31 characters
9. Create DSA Key:
    - Key Filename: Maximum 63 characters

- Key Size: Maximum 4096 bits
- PEM Passphrase: Maximum 31 characters
- Verify Passphrase: Maximum 31 characters

10. Change advanced SSL settings:
    - Maximum CRL memory size: Maximum 1024 Mbytes
    - Encryption trigger timeout (10 mS ticks): Maximum 200
    - Encryption trigger packet count: Maximum 50
    - OCSP cache size: Maximum 512 Mbytes
11. Install Certificate:
    - Certificate-Key pair Name: Maximum 31 characters
    - Certificate File Name: Maximum 63 characters
    - Private Key File Name: Maximum 63 characters
    - Password: Maximum 31 characters
    - Notification Period: Maximum 100
12. Create Cipher Group:
    - Cipher Group Name: Maximum 39 characters
13. Create CRL:
    - CRL Name: Maximum 31 characters
    - CRL File: Maximum 63 characters
    - URL: Maximum 127 characters
    - Base DN: Maximum 127 characters
    - Bind DN: Maximum 127 characters
    - Password: Maximum 31 characters
    - Day(s): Maximum 31
14. Create SSL Policy:
    - Name: Maximum 127 characters
15. Create SSL Action:
    - Name: Maximum 127 characters
16. Create OCSP Responder:
    - Name: Maximum 32 characters
    - URL: Maximum 128 characters

- Batching Depth: Maximum 8
- Batching Delay: Maximum 10000
- Produced At Time Skew: Maximum 86400
- Request Time-out: Maximum120000

17. Create Virtual Server:
    - Name: Maximum 127 characters
    - Redirect URL: Maximum 127 characters
    - Client Time-out: Maximum 31536000 secs
18. Create Service:
    - Name: Maximum 127 characters
    - Idle Time-out (secs):

      Client: Maximum 31536000

      Server: Maximum 31536000
19. Create Service Group:
    - Service Group Name: Maximum 127 characters
    - Server ID: Maximum 4294967295
    - Idle Time-out (secs):

      Client: Maximum value 31536000

      Server: Maximum 31536000
20. Create Monitor:
    - Name: Maximum 31 characters
21. Create Server:
    - Server Name: Maximum 127 characters
    - Domain Name: Maximum 255 characters
    - Resolve Retry: Maximum 20939 secs

CITRIX®

Getting Started 10

Understanding the NetScaler

The Citrix NetScaler product is an application switch that performs application-specific traffic analysis to intelligently distribute, optimize, and secure Layer 4-Layer 7 (L4–L7) network traffic for web applications. For example, a NetScaler bases load balancing decisions on individual HTTP requests instead of on long-lived TCP connections, so that the failure or slowdown of a server is managed much more quickly and with less disruption to clients. The NetScaler feature set can be broadly categorized as consisting of switching features, security and protection features, and server-farm optimization features.

Switching Features

When deployed in front of application servers, a NetScaler ensures optimal distribution of traffic by the way in which it directs client requests. Administrators can segment application traffic according to information in the body of an HTTP or TCP request, and on the basis of L4–L7 header information such as URL, application data type, or cookie. Numerous load balancing algorithms and extensive server health checks improve application availability by ensuring that client requests are directed to the appropriate servers.

Security and Protection Features

NetScaler security and protection features protect web applications from Application Layer attacks. A NetScaler allows legitimate client requests and can block malicious requests. It provides built-in defenses against denial-of-service (DoS) attacks and supports features that protect against legitimate surges in application traffic that would otherwise overwhelm the servers. An available built-in firewall protects web applications from Application Layer attacks, including buffer overflow exploits, SQL injection attempts, cross-site scripting attacks, and more. In addition, the firewall provides identity theft protection by securing confidential corporate information and sensitive customer data.

Optimization Features

Optimization features offload resource-intensive operations, such as Secure Sockets Layer (SSL) processing, data compression, client keep-alive, TCP buffering, and the caching of static and dynamic content from servers. This improves the performance of the servers in the server farm and therefore speeds up applications. A NetScaler supports several transparent TCP optimizations, which mitigate problems caused by high latency and congested network links, accelerating the delivery of applications while requiring no configuration changes to clients or servers.

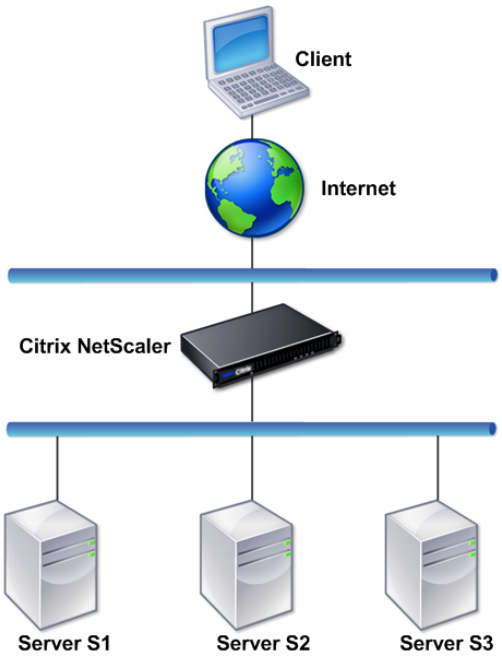
Where Does a NetScaler Appliance Fit in the Network?

A NetScaler appliance resides between the clients and the servers, so that client requests and server responses pass through it. In a typical installation, virtual servers configured on the appliance provide connection points that clients use to access the applications behind the appliance. In this case, the appliance owns public IP addresses that are associated with its virtual servers, while the real servers are isolated in a private network. It is also possible to operate the appliance in a transparent mode as an L2 bridge or L3 router, or even to combine aspects of these and other modes.

Physical Deployment Modes

A NetScaler appliance logically residing between clients and servers can be deployed in either of two physical modes: inline and one-arm. In inline mode, multiple network interfaces are connected to different Ethernet segments, and the appliance is placed between the clients and the servers. The appliance has a separate network interface to each client network and a separate network interface to each server network. The appliance and the servers can exist on different subnets in this configuration. It is possible for the servers to be in a public network and the clients to directly access the servers through the appliance, with the appliance transparently applying the L4-L7 features. Usually, virtual servers (described later) are configured to provide an abstraction of the real servers. The following figure shows a typical inline deployment.

Figure 1. Inline Deployment



In one-arm mode, only one network interface of the appliance is connected to an Ethernet segment. The appliance in this case does not isolate the client and server sides of the network, but provides access to applications through configured virtual servers. One-arm mode can simplify network changes needed for NetScaler installation in some environments.

For examples of inline (two-arm) and one-arm deployment, see "Understanding Common Network Topologies."

Citrix NetScaler as an L2 Device

A NetScaler functioning as an L2 device is said to operate in L2 mode. In L2 mode, the NetScaler forwards packets between network interfaces when all of the following conditions are met:

- The packets are destined to another device's media access control (MAC) address.
- The destination MAC address is on a different network interface.
- The network interface is a member of the same virtual LAN (VLAN).

By default, all network interfaces are members of a pre-defined VLAN, VLAN 1. Address Resolution Protocol (ARP) requests and responses are forwarded to all network

interfaces that are members of the same VLAN. To avoid bridging loops, L2 mode must be disabled if another L2 device is working in parallel with the NetScaler.

For information about how the L2 and L3 modes interact, see "Configuring Modes of Packet Forwarding."

For information about configuring L2 mode, see "Enabling and Disabling Layer 2 Mode."

Citrix NetScaler as a Packet Forwarding Device

A NetScaler appliance can function as a packet forwarding device, and this mode of operation is called *L3 mode*. With L3 mode enabled, the appliance forwards any received unicast packets that are destined for an IP address that does not belong to the appliance, if there is a route to the destination. The appliance can also route packets between VLANs.

In both modes of operation, L2 and L3, the appliance generally drops packets that are in:

- Multicast frames
- Unknown protocol frames destined for an appliance's MAC address (non-IP and non-ARP)
- Spanning Tree protocol (unless BridgeBPDUs is ON)

For information about how the L2 and L3 modes interact, see "Configuring Modes of Packet Forwarding."

For information about configuring the L3 mode, see "Enabling and Disabling Layer 3 Mode."

How a NetScaler Communicates with Clients and Servers

A NetScaler appliance is usually deployed in front of a server farm and functions as a transparent TCP proxy between clients and servers, without requiring any client-side configuration. This basic mode of operation is called Request Switching technology and is the core of NetScaler functionality. Request Switching enables an appliance to multiplex and offload the TCP connections, maintain persistent connections, and manage traffic at the request (application layer) level. This is possible because the appliance can separate the HTTP request from the TCP connection on which the request is delivered.

Depending on the configuration, an appliance might process the traffic before forwarding the request to a server. For example, if the client attempts to access a secure application on the server, the appliance might perform the necessary SSL processing before sending traffic to the server.

To facilitate efficient and secure access to server resources, an appliance uses a set of IP addresses collectively known as *NetScaler-owned IP addresses*. To manage your network traffic, you assign NetScaler-owned IP addresses to virtual entities that

become the building blocks of your configuration. For example, to configure load balancing, you create virtual servers to receive client requests and distribute them to services, which are entities representing the applications on your servers.

Understanding NetScaler-Owned IP Addresses

To function as a proxy, a NetScaler appliance uses a variety of IP addresses. The key NetScaler-owned IP addresses are:

NetScaler IP (NSIP) address
The NSIP address is the IP address for management and general system access to the appliance itself, and for communication between appliances in a high availability configuration.

Mapped IP (MIP) address
A MIP address is used for server-side connections. It is not the IP address of the appliance. In most cases, when the appliance receives a packet, it replaces the source IP address with a MIP address before sending the packet to the server. With the servers abstracted from the clients, the appliance manages connections more efficiently.

Virtual server IP (VIP) address
A VIP address is the IP address associated with a virtual server. It is the public IP address to which clients connect. An appliance managing a wide range of traffic may have many VIPs configured.

Subnet IP (SNIP) address
A SNIP address is used in connection management and server monitoring. You can specify multiple SNIP addresses for each subnet. SNIP addresses can be bound to a VLAN.

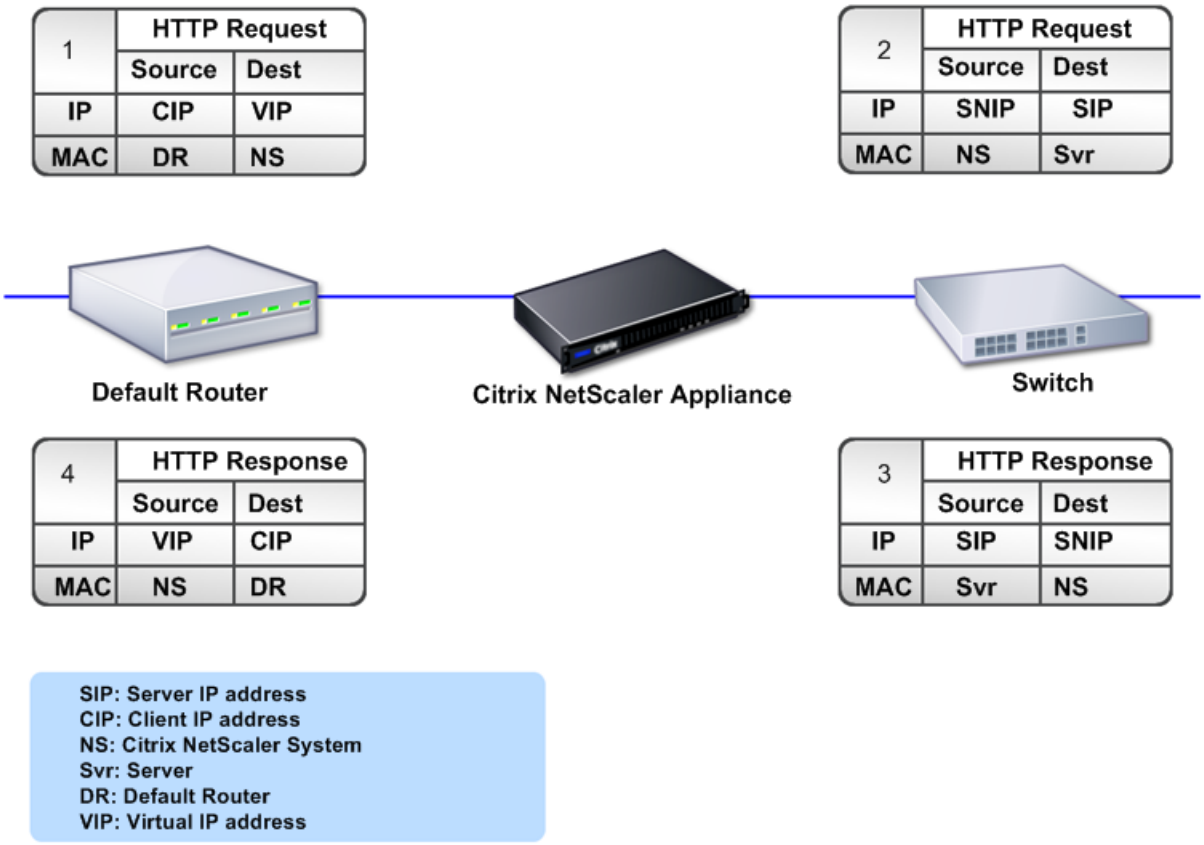
IP Set
An IP set is a set of IP addresses, which are configured on the appliance as SNIP . An IP set is identified with a meaningful name that helps in identifying the usage of the IP addresses contained in it.

Net Profile
A net profile (or network profile) contains an IP address or an IP set. A net profile can be bound to load balancing or content switching virtual servers, services, service groups, or monitors. During communication with physical servers or peers, the appliance uses the addresses specified in the profile as source IP addresses.

How Traffic Flows Are Managed

Because a NetScaler appliance functions as a TCP proxy, it translates IP addresses before sending packets to a server. When you configure a virtual server, clients connect to a VIP address on the NetScaler instead of directly connecting to a server. As determined by the settings on the virtual server, the appliance selects an appropriate server and sends the client's request to that server. By default, the appliance uses a SNIP address to establish connections with the server, as shown in the following figure.

Figure 2. Virtual Server Based Connections



In the absence of a virtual server, when an appliance receives a request, it transparently forwards the request to the server. This is called the transparent mode of operation. When operating in transparent mode, an appliance translates the source IP addresses of incoming client requests to the SNIP address but does not change the destination IP address. For this mode to work, L2 or L3 mode has to be configured appropriately.

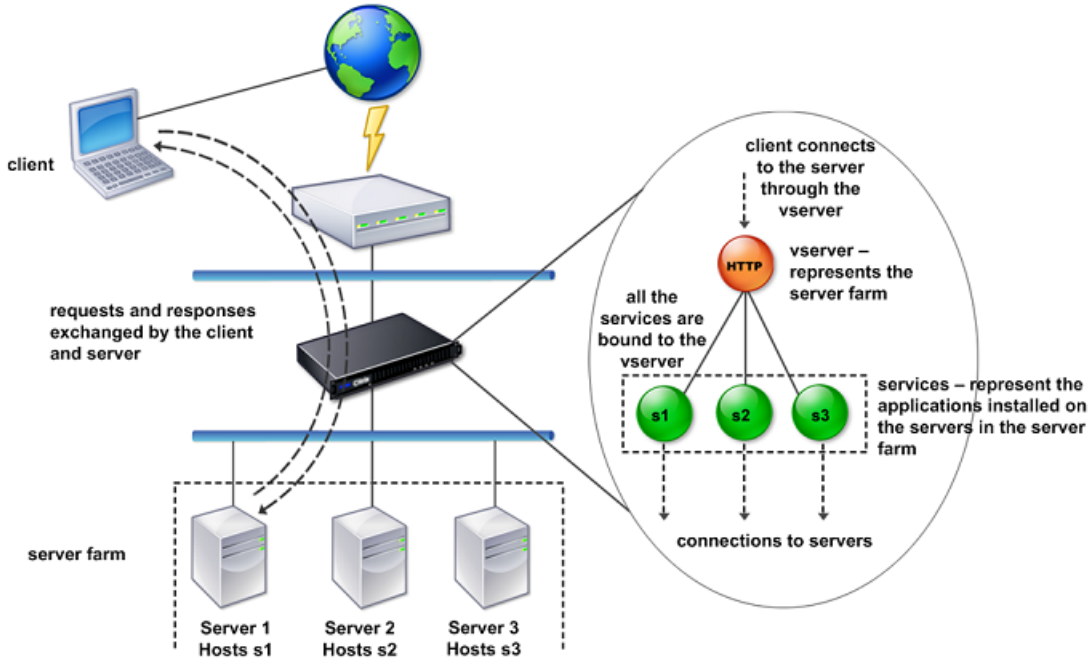
For cases in which the servers need the actual client IP address, the appliance can be configured to modify the HTTP header by inserting the client IP address as an additional field, or configured to use the client IP address instead of a SNIP address for connections to the servers.

Traffic Management Building Blocks

The configuration of a NetScaler appliance is typically built up with a series of virtual entities that serve as building blocks for traffic management. The building block approach helps separate traffic flows. Virtual entities are abstractions, typically representing IP addresses, ports, and protocol handlers for processing traffic. Clients access applications and resources through these virtual entities. The most commonly used entities are virtual servers and services. Virtual servers represent groups of servers in a server farm or remote network, and services represent specific applications on each server.

Most features and traffic settings are enabled through virtual entities. For example, you can configure an appliance to compress all server responses to a client that is connected to the server farm through a particular virtual server. To configure the appliance for a particular environment, you need to identify the appropriate features and then choose the right mix of virtual entities to deliver them. Most features are delivered through a cascade of virtual entities that are bound to each other. In this case, the virtual entities are like blocks being assembled into the final structure of a delivered application. You can add, remove, modify, bind, enable, and disable the virtual entities to configure the features. The following figure shows the concepts covered in this section.

Figure 3. How Traffic Management Building Blocks Work



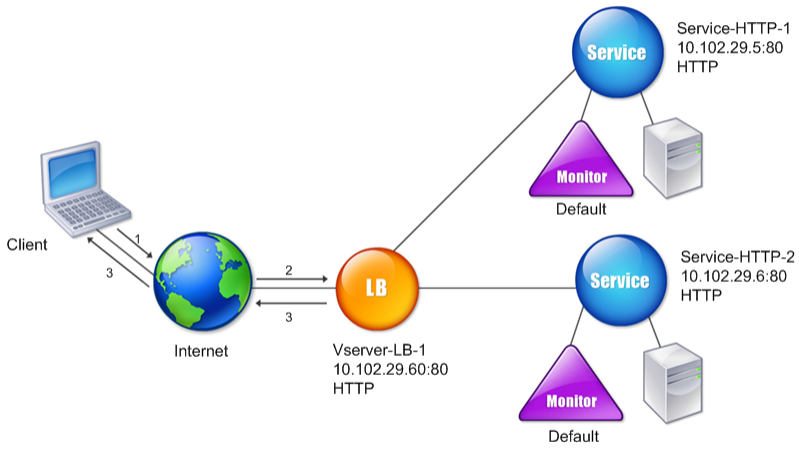
A Simple Load Balancing Configuration

In the example shown in the following figure, the NetScaler appliance is configured to function as a load balancer. For this configuration, you need to configure virtual

entities specific to load balancing and bind them in a specific order. As a load balancer, an appliance distributes client requests across several servers and thus optimizes the utilization of resources.

The basic building blocks of a typical load balancing configuration are services and load balancing virtual servers. The services represent the applications on the servers. The virtual servers abstract the servers by providing a single IP address to which the clients connect. To ensure that client requests are sent to a server, you need to bind each service to a virtual server. That is, you must create services for every server and bind the services to a virtual server. Clients use the VIP address to connect to a NetScaler appliance. When the appliance receives client requests sent to the VIP address, it sends them to a server determined by the load balancing algorithm. Load balancing uses a virtual entity called a *monitor* to track whether a specific configured service (server plus application) is available to receive requests.

Figure 4. Load Balancing Virtual Server, Services, and Monitors



In addition to configuring the load balancing algorithm, you can configure several parameters that affect the behavior and performance of the load balancing configuration. For example, you can configure the virtual server to maintain persistence based on source IP address. The appliance then directs all requests from any specific IP address to the same server.

Understanding Virtual Servers

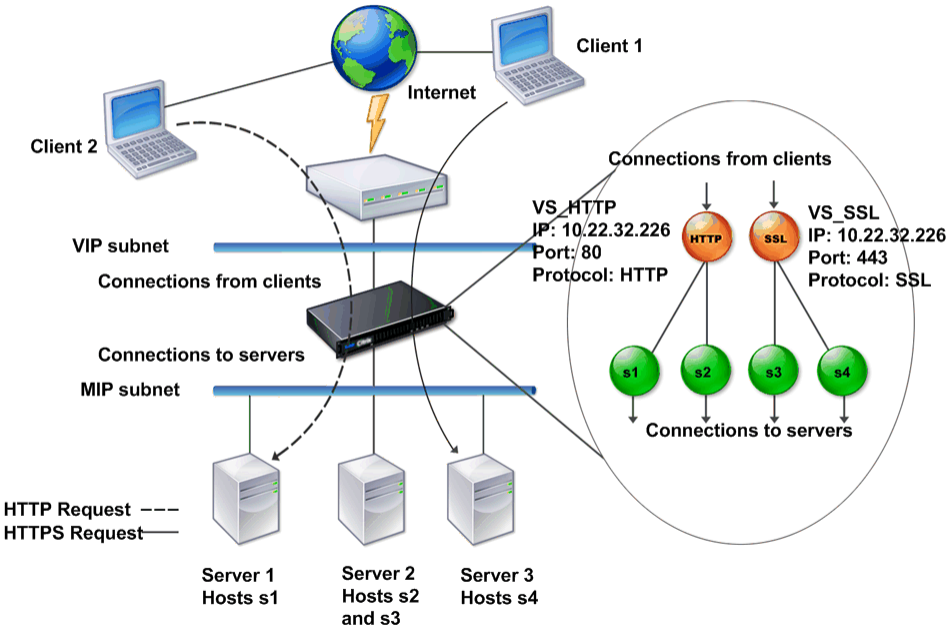
A virtual server is a named NetScaler entity that external clients can use to access applications hosted on the servers. It is represented by an alphanumeric name, virtual

IP (VIP) address, port, and protocol. The name of the virtual server is of only local significance and is designed to make the virtual server easier to identify. When a client attempts to access applications on a server, it sends a request to the VIP instead of the IP address of the physical server. When the appliance receives a request at the VIP address, it terminates the connection at the virtual server and uses its own connection with the server on behalf of the client. The port and protocol settings of the virtual server determine the applications that the virtual server represents. For example, a web server can be represented by a virtual server and a service whose port and protocol are set to 80 and HTTP, respectively. Multiple virtual servers can use the same VIP address but different protocols and ports.

Virtual servers are points for delivering features. Most features, like compression, caching, and SSL offload, are normally enabled on a virtual server. When the appliance receives a request at a VIP address, it chooses the appropriate virtual server by the port on which the request was received and its protocol. The appliance then processes the request as appropriate for the features configured on the virtual server.

In most cases, virtual servers work in tandem with services. You can bind multiple services to a virtual server. These services represent the applications running on physical servers in a server farm. After the appliance processes requests received at a VIP address, it forwards them to the servers as determined by the load balancing algorithm configured on the virtual server. The following figure illustrates these concepts.

Figure 5. Multiple Virtual Servers with a Single VIP Address



The preceding figure shows a configuration consisting of two virtual servers with a common VIP address but different ports and protocols. Each of the virtual servers has two services bound to it. The services s1 and s2 are bound to VS_HTTP and represent the HTTP applications on Server 1 and Server 2. The services s3 and s4 are bound to VS_SSL and represent the SSL applications on Server 2 and Server 3 (Server 2 provides both HTTP and SSL applications). When the appliance receives an HTTP request at the VIP address, it processes the request as specified by the settings of VS_HTTP and sends it to either Server 1 or Server 2. Similarly, when the appliance receives an HTTPS request at the VIP address, it processes it as specified by the settings of VS_SSL and it sends it to either Server 2 or Server 3.

Virtual servers are not always represented by specific IP addresses, port numbers, or protocols. They can be represented by wildcards, in which case they are known as *wildcard* virtual servers. For example, when you configure a virtual server with a wildcard instead of a VIP, but with a specific port number, the appliance intercepts and processes all traffic conforming to that protocol and destined for the predefined port. For virtual servers with wildcards instead of VIPs and port numbers, the appliance intercepts and processes all traffic conforming to the protocol.

Virtual servers can be grouped into the following categories:

Load balancing virtual server
Receives and redirects requests to an appropriate server. Choice of the appropriate server is based on which of the various load balancing methods the user configures.

Cache redirection virtual server
Redirects client requests for dynamic content to origin servers, and requests for static content to cache servers. Cache redirection virtual servers often work in conjunction with load balancing virtual servers.

Content switching virtual server
Directs traffic to a server on the basis of the content that the client has requested. For example, you can create a content switching virtual server that directs all client requests for images to a server that serves images only. Content switching virtual servers often work in conjunction with load balancing virtual servers.

Virtual private network (VPN) virtual server
Decrypts tunneled traffic and sends it to intranet applications.

SSL virtual server
Receives and decrypts SSL traffic, and then redirects to an appropriate server. Choosing the appropriate server is similar to choosing a load balancing virtual server.

Understanding Services

Services represent applications on a server. While services are normally combined with virtual servers, in the absence of a virtual server, a service can still manage application-specific traffic. For example, you can create an HTTP service on a NetScaler appliance to represent a web server application. When the client attempts to access a web site hosted on the web server, the appliance intercepts the HTTP requests and creates a transparent connection with the web server.

In service-only mode, an appliance functions as a proxy. It terminates client connections, uses a SNIP address to establish a connection to the server, and translates the destination IP addresses of incoming client requests to a SNIP address. Although the clients send requests directly to the IP address of the server, the server sees them as coming from the SNIP address. The appliance translates the IP addresses, port numbers, and sequence numbers.

A service is also a point for applying features. Consider the example of SSL acceleration. To use this feature, you must create an SSL service and bind an SSL certificate to the service. When the appliance receives an HTTPS request, it decrypts the traffic and sends it, in clear text, to the server. Only a limited set of features can be configured in the service-only case.

Services use entities called monitors to track the health of applications. Every service has a default monitor, which is based on the service type, bound to it. As specified by the settings configured on the monitor, the appliance sends probes to the application at regular intervals to determine its state. If the probes fail, the appliance marks the service as down. In such cases, the appliance responds to client requests with an appropriate error message or re-routes the request as determined by the configured load balancing policies.

Understanding Policies and Expressions

A policy defines specific details of traffic filtering and management on a NetScaler. It consists of two parts: the expression and the action. The expression defines the types of requests that the policy matches. The action tells the NetScaler what to do when a request matches the expression. As an example, the expression might be to match a specific URL pattern to a type of security attack, with the action being to drop or reset the connection. Each policy has a priority, and the priorities determine the order in which the policies are evaluated.

When a NetScaler receives traffic, the appropriate policy list determines how to process the traffic. Each policy on the list contains one or more expressions, which together define the criteria that a connection must meet to match the policy.

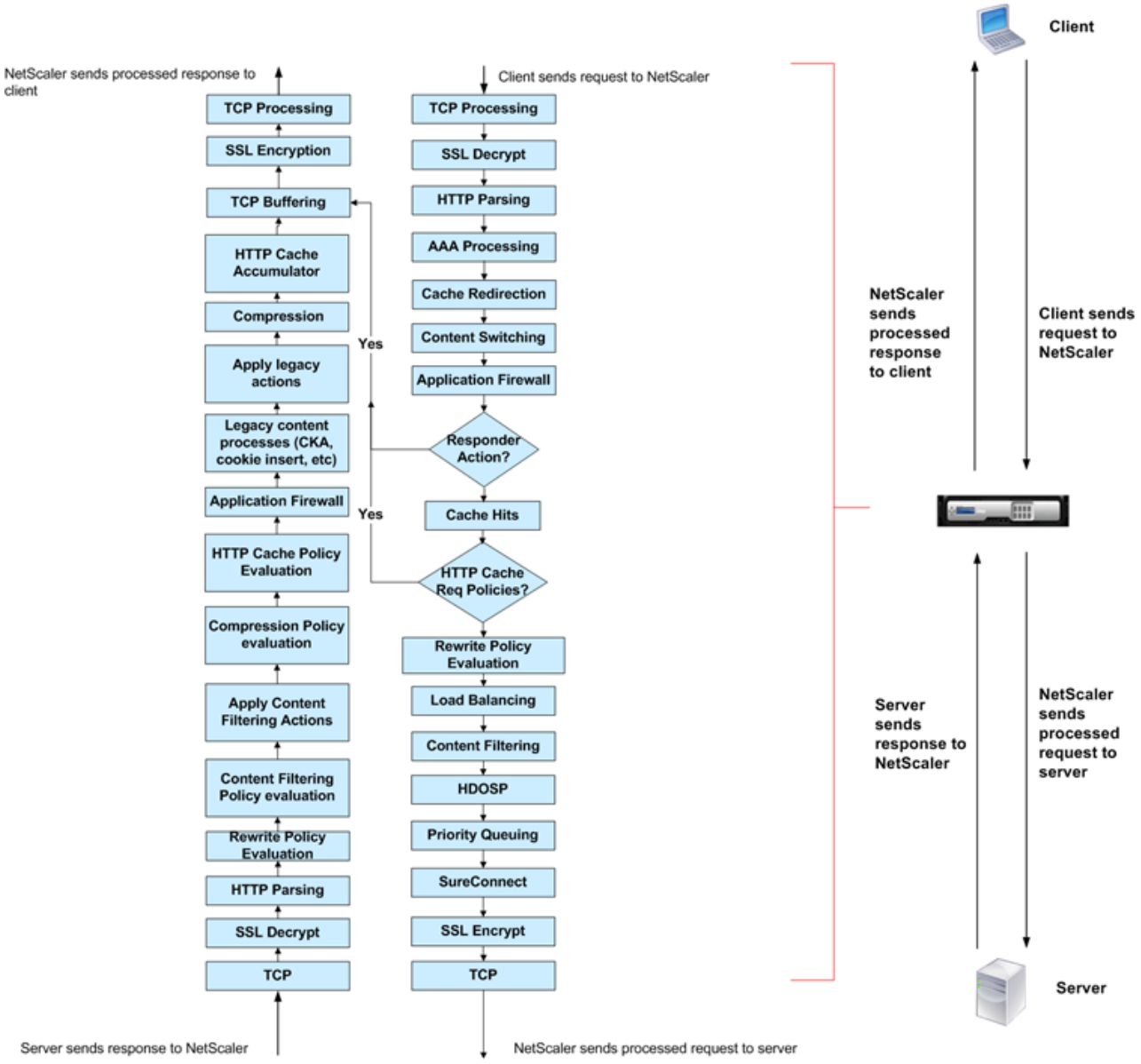
For all policy types except Rewrite policies, a NetScaler implements only the first policy that a request matches, not any additional policies that it might also match. For Rewrite policies, the NetScaler evaluates the policies in order and, in the case of multiple matches, performs the associated actions in that order. Policy priority is important for getting the results you want.

Processing Order of Features

Depending on requirements, you can choose to configure multiple features. For example, you might choose to configure both compression and SSL offload. As a result, an outgoing packet might be compressed and then encrypted before being sent to the client.

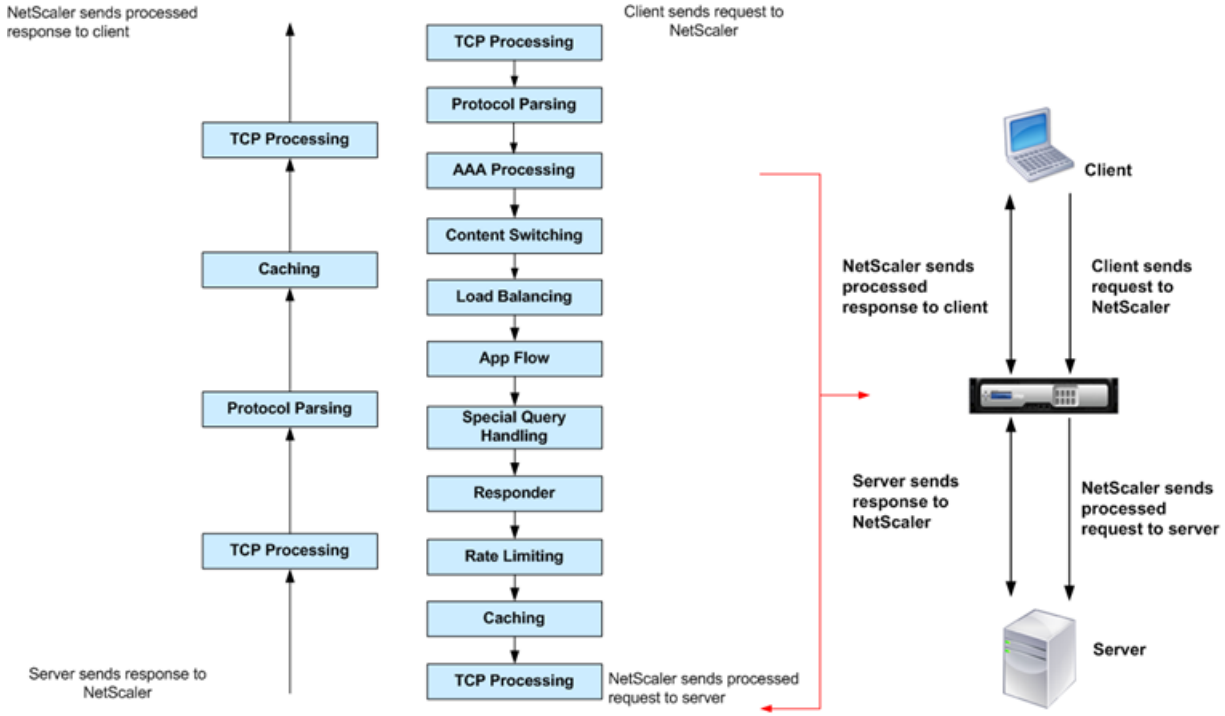
The following figure shows the L7 packet flow in the NetScaler.

Figure 6. L7 Packet Flow Diagram



The following figure shows the DataStream packet flow in the NetScaler. DataStream is supported for MySQL and MS SQL databases. For information about the DataStream feature, see "DataStream."

Figure 7. DataStream Packet Flow Diagram



Introduction to the Citrix NetScaler Product Line

The Citrix NetScaler product line optimizes delivery of applications over the Internet and private networks, combining application-level security, optimization, and traffic management into a single, integrated appliance. You install a NetScaler appliance in your server room and route all connections to your managed servers through it. The NetScaler features that you enable and the policies you set are then applied to incoming and outgoing traffic.

A NetScaler can be integrated into any network as a complement to existing load balancers, servers, caches, and firewalls. It requires no additional client or server side software, and can be configured using the NetScaler web-based GUI and CLI configuration utilities.

NetScaler appliances are available in a variety of hardware platforms that have a range of specifications, including multicore processors.

The NetScaler operating system is the base operating system for all NetScaler hardware platforms. The NetScaler operating system is available in three editions: Standard, Enterprise, and Platinum.

Citrix NetScaler Hardware Platforms

NetScaler hardware is available in a variety of platforms that have a range of hardware specifications, including multicore processors. All hardware platforms support some combination of Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet interfaces.

The following platforms are available for NetScaler 10.

- Citrix NetScaler MPX 5500
- Citrix NetScaler MPX 5550/5650
- Citrix NetScaler MPX 7500/9500
- Citrix NetScaler MPX 8200/8400/8600
- Citrix NetScaler MPX 9700/10500/12500/15500
- Citrix NetScaler MPX 11500/13500/14500/16500/18500/20500
- Citrix NetScaler MPX 15000
- Citrix NetScaler MPX 17000
- Citrix NetScaler MPX 17500/19500/21500

- Citrix NetScaler MPX 17550/19550/20550/21550

For more information about the hardware platform specifications, see "Introduction to the Hardware Platforms."

The following tables list different editions of the NetScaler and the hardware platforms on which they are available.

Table 1. Product Editions and MPX Hardware Platforms

Hardware	MPX 5500	MPX 5550/5650	MPX 7500/9500	MPX 8200/8400/8600	MPX 15000	MPX 17000
Platinum Edition	Yes	Yes	Yes	Yes	Yes	Yes
Enterprise Edition	Yes	Yes	Yes	Yes	Yes	Yes
Standard Edition	Yes	Yes	Yes	Yes	Yes	Yes

Table 2. Product Editions and MPX Hardware Platforms (contd.)

Hardware	MPX 9700/10500/12500/15500	MPX 11500/13500/14500/16500/18500/20500	MPX 17500/19500/21500	MPX 17550/19550/20550/21550
Platinum Edition	Yes	Yes	Yes	Yes
Enterprise Edition	Yes	Yes	Yes	Yes
Standard Edition	Yes	Yes	Yes	Yes

Citrix NetScaler Editions

The NetScaler operating system is available in Standard, Enterprise, and Platinum editions. The Enterprise and Standard editions have limited features available. Feature licenses are required for all editions.

For instructions on how to obtain and install licenses, see "http://support.citrix.com/article/ctx121062."

The Citrix NetScaler editions are described as follows:

- *Citrix NetScaler, Standard Edition*. Provides small and medium enterprises with comprehensive Layer 4- Layer 7 (L4-L7) traffic management, enabling increased web application availability.
- *Citrix NetScaler, Enterprise Edition*. Provides web application acceleration and advanced L4-L7 traffic management, enabling enterprises to increase web application performance and availability and reduce datacenter costs.
- *Citrix NetScaler, Platinum Edition*. Provides a web application delivery solution that reduces data center costs and accelerates application performance, with end-to-end visibility of application performance, and provides advanced application security.

The following table summarizes the features supported by each edition in the Citrix NetScaler product line:

Table 3. Citrix NetScaler Application Delivery Product Line Features

Key Features	Platinum Edition	Enterprise Edition	Standard Edition
Application availability			
Layer 4 load balancing	Yes	Yes	Yes
Layer 7 content switching	Yes	Yes	Yes
AppExpert rate controls	Yes	Yes	Yes
IPv6 support	Yes	Yes	Yes
Global server load balancing (GSLB)	Yes	Yes	Optional
Dynamic routing protocols	Yes	Yes	No
Surge protection	Yes	Yes	No
Priority queuing	Yes	Yes	No
Application acceleration			
Client and server TCP optimizations	Yes	Yes	Yes
Citrix AppCompress for HTTP	Yes	Yes	Optional
Citrix AppCache	Yes	Optional	No
Citrix Branch Repeater client	Yes	No	No
Application security			
Layer 4 DoS defenses	Yes	Yes	Yes
Layer 7 content filtering	Yes	Yes	Yes

Key Features	Platinum Edition	Enterprise Edition	Standard Edition
HTTP/URL Rewrite	Yes	Yes	Yes
Access Gateway, EE SSL VPN	Yes	Yes	Yes
Layer 7 DoS Defenses	Yes	Yes	No
AAA security	Yes	Yes	No
Application firewall with XML security	Yes	Optional	No
Simple manageability			
AppExpert visual policy builder	Yes	Yes	Yes
AppExpert service callouts	Yes	Yes	Yes
AppExpert templates	Yes	Yes	Yes
Role-based administration	Yes	Yes	Yes
Configuration wizards	Yes	Yes	Yes
Citrix Command Center	Yes	Yes	No
Citrix EdgeSight for NetScaler	Yes	Optional	No
Web 2.0 optimization			
Rich Internet application support	Yes	Yes	Yes
Advanced server offload	Yes	Yes	No
Lower total cost of ownership (TCO)			
TCP buffering	Yes	Yes	Yes
TCP multiplexing	Yes	Yes	Yes
SSL offload and acceleration	Yes	Yes	Yes
Cache redirection	Yes	Yes	No
Citrix EasyCall	Yes	No	No

Note: While we have taken care to ensure absolute accuracy when compiling this information, it might change. For the latest information, see Citrix Support at "http://www.citrix.com."

Supported Releases on NetScaler Hardware

The following table lists the earliest NetScaler builds for releases that are supported on the NetScaler MPX platforms.

Hardware	Software Release	Software Build #
MPX 5500	10.5	All
	10.1	All
	10.0	All
	9.3	All
MPX 5550/5650	10.5	All
	10.1	All
	10.0	71.6.nc and later
	9.3	59.5.nc and later
MPX 7500/9500	10.5	All
	10.1	All
	10.0	All
	9.3	All
MPX 8005/8015	10.5	All
	10.1	122.17.nc and later
	9.3	65.8.nc and later
MPX 8200/8400/8600	10.5	All
	10.1	All
	10.0	70.7.nc and later
	9.3	58.5.nc and later
MPX 9700/10500/12500	10.5	All

Hardware	Software Release	Software Build #
	10.1	All
	10.0	All
	9.3	All
MPX 9700/10500/12500 10G	10.5	All
	10.1	All
	10.0	All
	9.3	All
MPX 15500	10.5	All
	10.1	All
	10.0	All
	9.3	All
MPX 15500 10G	10.5	All
	10.1	All
	10.0	All
	9.3	All
MPX 11500/13500/14500/16500/18500/20500	10.5	All
	10.1	All
	10.0	All
	9.3	52.3.nc and later
MPX 11515/11520/11530/11540/11542	10.5	All
	10.1	123.11.nc and later
	9.3	65.8.nc and later
MPX 15000	10.5	All
	10.1	All
	10.0	All
	9.3	All

Hardware	Software Release	Software Build #
MPX 17000	10.5	All
	10.1	All
	10.0	All
	9.3	All
MPX 17500/19500/21500	10.5	All
	10.1	All
	10.0	All
	9.3	All
MPX 17550/19550/20550/21550	10.5	All
	10.1	All
	10.0	All
	9.3	53.5.nc and later
MPX 22040/22060/22080/22100/22120	10.5	51.10.nc and later
	10.1	123.11.nc and later
	9.3	65.8.nc and later
MPX 24100/24150	10.5	51.10.nc and later
	10.1	129.11.nc and later

Installing the NetScaler Hardware

Before installing a NetScaler appliance, review the pre-installation checklist. A NetScaler is typically mounted in a rack, and all models ship with rack-rail hardware. All models except the 7000 support small form factor pluggable SFP, XFP, or SFP+ transceivers. After mounting the appliance and installing the transceivers, connect the NetScaler to your network. Use a console cable to connect the NetScaler to a personal computer so that you can perform an initial configuration. After connecting everything else, connect the NetScaler to a power source.

Unpacking the Appliance

The hardware accessories for your particular appliance, such as cables, adapters, and rail kit, vary depending on the hardware platform you ordered. Unpack the box that contains your new appliance on a sturdy table with plenty of space and inspect the contents.

Use the following list to verify that you received everything that should have been included in the box.

- The appliance you ordered
- One RJ-45 to DB-9 adapter
- One 6 ft RJ-45/DB-9 cable
- Two power cables
- One fiber patch cable
- The following list specifies the number of power cables included for each appliance model:
  - One power cable for the MPX 5500, MPX 5550/5650, MPX 7500/9500, and MPX 8200/8400/8600/8800 appliances
  - Two power cables for the MPX 15000, MPX 17000, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 25100T/25160T, and MPX 17550/19550/20550/21550 appliances

  Note: For Brazilian customers, Citrix does not ship a power cable. Use a cable that conforms to the **ABNT NBR 14136:2002** standard.
- One standard 4-post rail kit

  Note: If the kit that you received does not fit your rack, contact your Citrix sales representative to order the appropriate kit.

In addition to the items included in the box with your new appliance, you will need the following items to complete the installation and initial configuration process.

- Ethernet cables for each additional Ethernet port that you will connect to your network
- One available Ethernet port on your network switch or hub for each NetScaler Ethernet port you want to connect to your network

> **Note:** Transceiver modules are sold separately. Contact your Citrix sales representative to order transceiver modules for your appliance. Only transceivers supplied by Citrix are supported on the appliance.

- A computer to serve as a management workstation

Rack Mounting the Appliance

Most appliances can be installed in standard server racks that conform to EIA-310-D specification. The appliances ship with a set of rails, which you must install before you mount the appliance. The only tools that you need for installing an appliance are a Phillips screwdriver and a flathead screwdriver.

> ⚠ **Caution:** If you are installing the appliance as the only unit in the rack, mount it at the bottom. If the rack contains other units, make sure that the heaviest unit is at the bottom. If the rack has stabilizing devices available, install them before mounting the appliance.

The following table lists the different hardware platforms and the rack units required for each platform.

Table 1. ***Height Requirements For Each Platform***

Platform	Number of rack units
MPX 5500	One rack unit
MPX 5550/5650	One rack unit
MPX 7500/9500	One rack unit
MPX 8200/8400/8600/8800	One rack unit
MPX 9700/10500/12500/15500	Two rack units
MPX 15000, MPX 17000	Two rack units

MPX 11500/13500/14500/16500/18500/20500	Two rack units
MPX 17500/19500/21500	Two rack units
MPX 17550/19550/20550/21550	Two rack units

Each appliance ships with a mounting rail kit that contains two rail assemblies, one for the left side and the other for the right side of the appliance, and screws to attach the rails. An assembly consists of an inner rail and a rack rail. The supplied rail kit is 28 inches long (38 inches extended). Contact your Citrix sales representative to order a 23-inch (33 inches extended) rail kit.

Note: The same rail kit is used for both square-hole and round-hole racks. See "Installing the Rail Assembly to the Rack" for specific instructions for threaded, round-hole racks.

To mount the appliance, you must first install the rails and then install the appliance in the rack.

Perform the following tasks to mount the appliance:

- Remove the inner rails from the rail assembly.
- Attach the inner rails to the appliance.
- Install the rack rails on the rack.
- Install the appliance in the rack.

The appliance is shipped with rack-rail hardware. This hardware consists of including two inner rails that you attach to the appliance, one on each side, and a rack-rail assembly that you attach to the rack. The following figure illustrates The following figure shows the steps involved in mounting the Citrix NetScaler how to mount the appliance to a rack.

To remove the inner rails from the rail assembly

1. Place the rail assembly on a flat surface.
2. Slide out the inner rail toward the front of the assembly.
3. Depress the latch until the inner rail comes all the way out of the rail assembly.
4. Repeat steps 1 through 3 to remove the second inner rail.

To attach the inner rails to the appliance

1. Position the right inner rail behind the handle on the right side of the appliance.

2. Align the holes on the rail with the corresponding holes on the side of the appliance.
3. Attach the rail to the appliance with the provided screws: 4 per side for a 1U appliance and 5 per side for a 2U appliance, as shown in the following figure.

Figure 1. Attaching inner rails

4. Repeat steps 1 through 3 to install the left inner rail on the other side of the appliance.

To install the rack rails on the rack

1. If you have a round-hole, threaded rack, skip to step 3.
2. Install square nut retainers into the front post and back post of the rack as shown in the following figures. Before inserting a screw, be sure to align the square nut with the correct hole for your 1U or 2U appliance. The three holes are not evenly spaced.

Figure 2. Installing Retainers into the Front Rack Posts

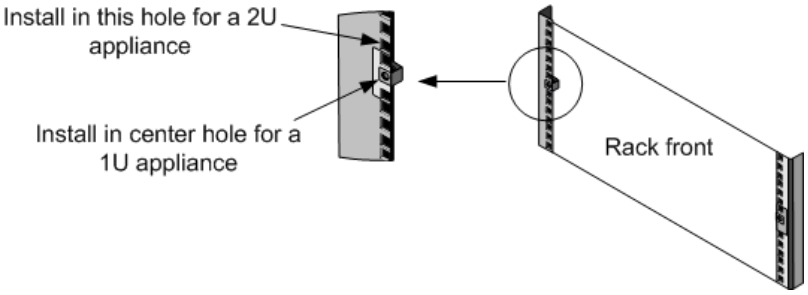
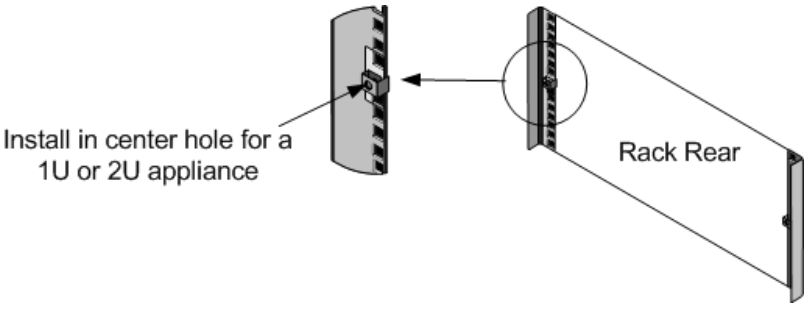
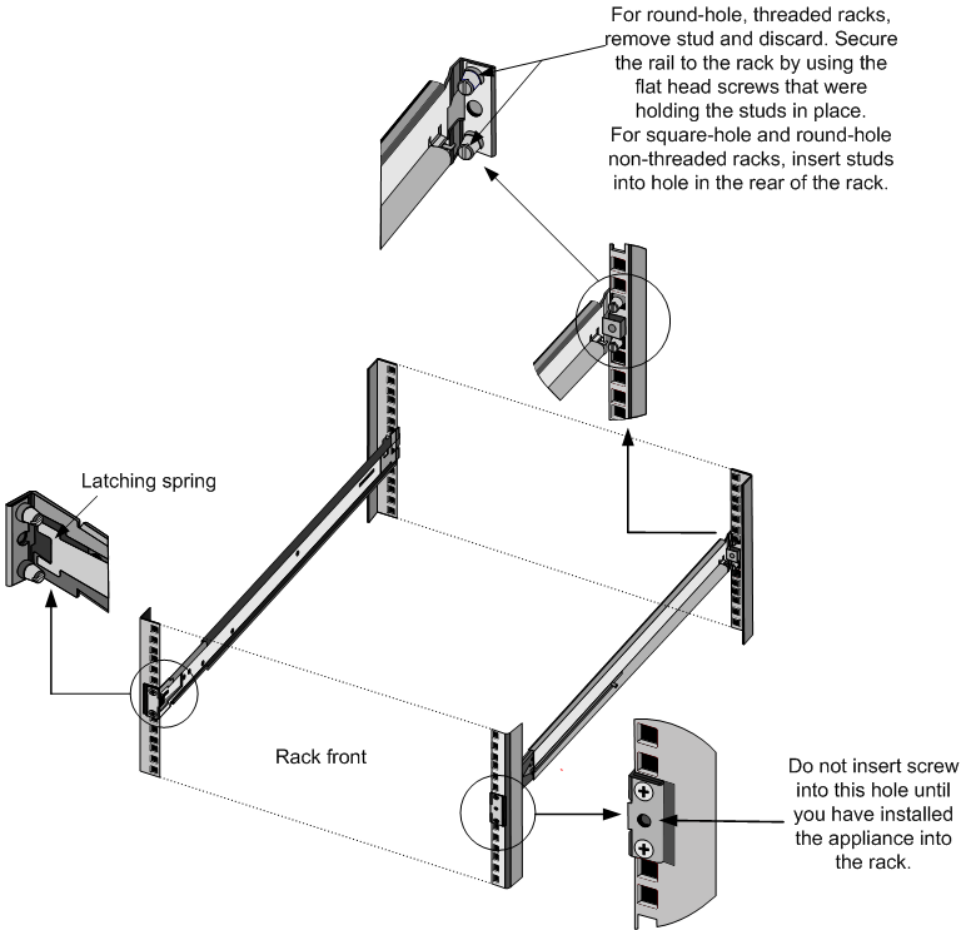


Figure 3. Installing Retainers into the Rear Rack Posts



3. Install the adjustable rail assembly into the rack as shown in the following figures. Use a screw to lock the rear rail flange into the rack. With the screw securing the rail in place, you can optionally remove the latching spring.

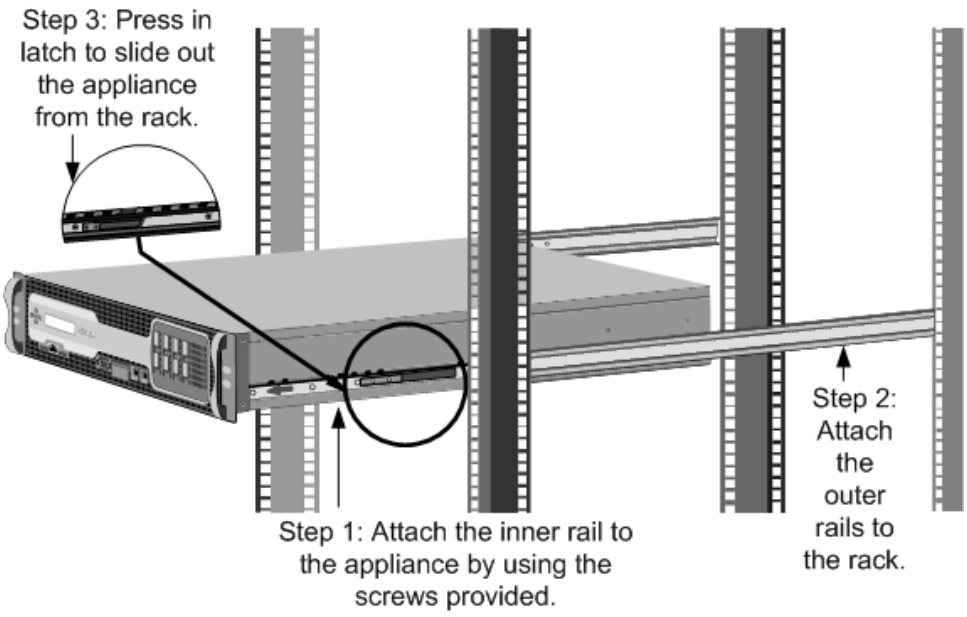
Figure 4. Installing the Rail Assembly to the Rack



To install the appliance in the rack

1. Align the inner rails, attached to the appliance, with the rack rails.
2. Slide the appliance into the rack rails, keeping the pressure even on both sides.
3. Verify that the appliance is locked in place by pulling it all the way out from the rack.

Figure 5. Rack Mounting the Appliance



Installing and Removing 1G SFP Transceivers

Note: This section applies to the MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, and MPX 11500/13500/14500/16500/18500/20500 appliances.

Note: Some CloudBridge 4000/5000Repeater on SDX appliances do not require SFP transceivers.

A Small Form-Factor Pluggable (SFP) is a compact transceiver that can operate at speeds of up to 1 gigabit per second and is available in both copper and fiber types. Inserting a 1G SFP copper transceiver converts the 1G SFP port to a 1000BASE-T port. Inserting a 1G SFP fiber transceiver converts the 1G SFP port to a 1000BASE-X port. Auto-negotiation is enabled by default on the 1G SFP port into which you insert your 1G SFP transceiver. As soon as a link between the port and the network is established, the speed and mode are matched on both ends of the cable.

Note: The 1G SFP transceiver is hot-swappable from release 9.3 build 47.5 and later on the NetScaler appliances that use the e1k interface. The following platforms support 1G SPF transceivers:

- MPX 7500/9500
- MPX 8200/8400/8600/8800
- MPX 9700/10500/12500/15500

- MPX 11500/13500/14500/16500/18500/20500

⚠ **Caution:** NetScalerCloudBridge 4000/5000Repeater on SDX appliances do not support 1G SFP transceivers from vendors other than Citrix Systems. Attempting to install third-party 1G SFP transceivers on your NetScalerCloudBridge 4000/5000Repeater on SDX appliance voids the warranty.

Insert 1G SFP transceivers into the 1G SFP ports on the front panel of the appliance. Frequent installation and removal of transceivers shortens their life span. Follow the removal procedure carefully to avoid damaging the 1G SFP transceiver or the appliance.

⚠ **Caution:** Do not install the transceivers with the cables attached. Doing so can damage the cable, the connector, or the optical interface of the transceiver.

To install a 1G SFP transceiver

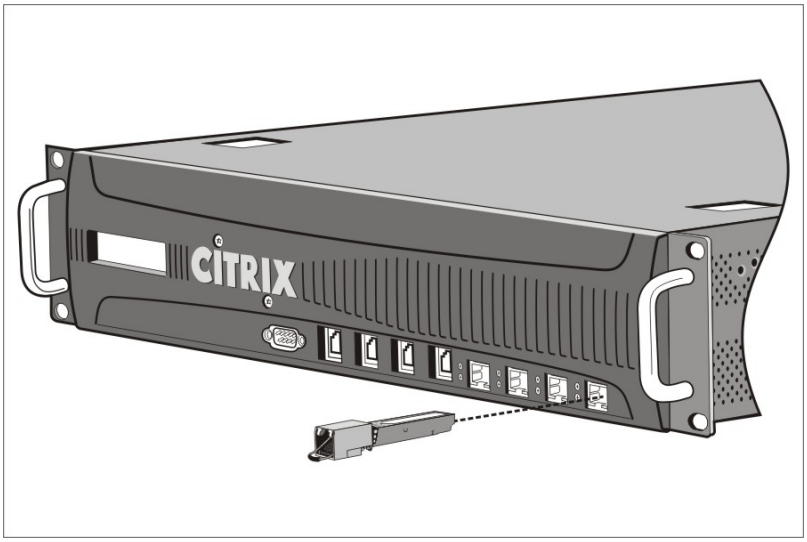
1. Remove the 1G SFP transceiver carefully from its box.

   👉 **Danger:** Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.

2. Align the 1G SFP transceiver to the front of the 1G SFP transceiver port on the front panel of the appliance, as shown in the following figure.

   Note: The illustration in the following figures might not represent your actual appliance.

   Figure 6. Installing a 1G SFP transceiver



3. Hold the 1G SFP transceiver between your thumb and index finger and insert it into the 1G SFP transceiver port, pressing it in until you hear the transceiver snap into place.
4. Lock the transceiver.
5. Verify that the LED is green and blinks twice, which indicates that the transceiver is functioning correctly.
6. If you are using a fiber 1G SFP transceiver, do not remove the dust caps attached to the transceiver and the cable until you are ready to insert the cable.

To remove a 1G SFP transceiver

1. Disconnect the cable from the 1G SFP transceiver. If you are using a fiber optic cable, replace the dust cap on the cable before putting it away.

   👉 **Danger:** Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.

2. Unlock the 1G SFP transceiver.
3. Hold the 1G SFP transceiver between your thumb and index finger and slowly pull it out of the port.
4. If you are removing a fiber 1G SFP transceiver, replace the dust cap before putting it away.
5. Put the 1G SFP transceiver into its original box or another appropriate container.

Installing and Removing XFP and 10G SFP+ Transceivers

Note: This section applies to the MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, MPX 15000, MPX 17000, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances.

Note: Some CloudBridge 4000/5000Repeater on SDX appliances do not require SFP+ transceivers.

A 10-Gigabit Small Form-Factor Pluggable (XFP or SFP+) is a compact optical transceiver that can operate at speeds of up to 10 gigabits per second. The MPX 15000 and MPX 17000 appliances use XFP transceivers and the MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances use 10G SFP+ transceivers. Autonegotiation is enabled by default on the XFP/10G SFP+ ports into which you insert your XFP/10G SFP+ transceiver. As soon as a link between the port and

the network is established, the mode is matched on both ends of the cable and for 10G SFP+ transceivers, the speed is also autonegotiated.

Note: An XFP transceiver is **not hot-swappable** on the NetScaler appliances. You must restart a NetScaler appliance after you insert an XFP transceiver.

However, the 10G SFP+ transceiver is hot-swappable from release 9.3 build 57.5 and later on the NetScaler appliances that use the ixgbe (ix) interface. The following platforms support 10G SPF+ transceivers:

- MPX 8200/8400/8600/8800
- MPX 9700/10500/12500/15500 10G and 10G FIPS
- MPX 11500/13500/14500/16500/18500/20500
- MPX 17500/19500/21500
- MPX 17550/19550/20550/21550

The following platforms support XFP transceivers:

- MPX 15000
- MPX 17000

⚠ **Caution:** NetScalerCloudBridge 4000/5000Repeater on SDX appliances do not support XFP/10G SFP+ transceivers provided by vendors other than Citrix Systems. Attempting to install third-party XFP/10G SFP+ transceivers on your NetScalerCloudBridge 4000/5000Repeater on SDX appliance voids the warranty.

Insert the XFP/10G SFP+ transceivers into the XFP/10G SFP+ ports on the front panel of the appliance. Frequent installation and removal of transceivers shortens their life span. Follow the removal procedure carefully to avoid damaging the transceiver or the appliance.

⚠ **Caution:** Do not install the transceivers with the cables attached. Doing so can damage the cable, the connector, or the optical interface of the transceiver.

To install an XFP/a 10G SFP+ transceiver

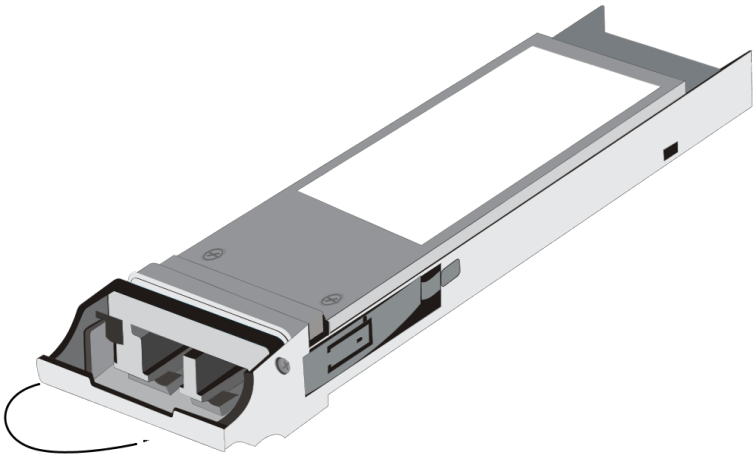
1. Remove the XFP/10G SFP+ transceiver carefully from its box.

   👉 **Danger:** Do not look directly into fiber optic transceivers and cables. They emit laser beams that can damage your eyes.

2. Align the XFP/10G SFP+ transceiver to the front of the XFP/10G SFP+ transceiver port on the front panel of the appliance.

3. Hold the XFP/10G SFP+ transceiver between your thumb and index finger and insert it into the XFP/10G SFP+ transceiver port, pressing it in until you hear the transceiver snap into place.
4. Move the locking hinge to the DOWN position as shown in the following figure.

Figure 7. Locking an XFP transceiver



5. Verify that the LED is green and blinks twice, which indicates that the transceiver is functioning correctly.
6. Do not remove the dust caps attached to the transceiver and cable until you are ready to insert the cable.

To remove an XFP/a 10G SFP+ transceiver

1. Disconnect the cable from the XFP/10G SFP+ transceiver. Replace the dust cap on the cable before putting it away.

> 👉 **Danger:** Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.

2. Unlock the XFP/10G SFP+ transceiver by moving the locking hinge to the UP position.
3. Hold the XFP/10G SFP+ transceiver between your thumb and index finger and slowly pull it out of the port.
4. Replace the dust cap on the transceiver before putting it away.
5. Put the XFP/10G SFP+ transceiver into its original box or another appropriate container.

Connecting the Cables

When the appliance is securely mounted on the rack, you are ready to connect the cables. Ethernet cables and the optional console cable are connected first. Connect the power cable last.

> **Danger:** Before installing or repairing the appliance, remove all jewelry and other metal objects that might come in contact with power sources or wires. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.

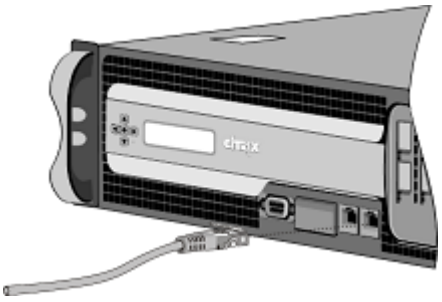
Connecting the Ethernet CablesConnecting the Appliance to the Network

Ethernet cables connect your appliance to the network. The type of cable you need depends on the type of port used to connect to the network. Use a category 5e or category 6 Ethernet cable with a standard RJ-45 connector on a 10/100/1000BASE-T port or 1G SFP copper transceiver. Use a fiber optic cable with an LC duplex connector with a 1G SFP fiber transceiver, or 10G SFP+, or XFP transceiver. The type of connector at the other end of the fiber optic cable depends on the port of the device that you are connecting to.

To connect an Ethernet cable to a 10/100/1000BASE-T port or 1G SFP copper transceiver

1. Insert the RJ-45 connector on one end of your Ethernet cable into an appropriate port on the front panel of the appliance, as shown in the following figure.

   Figure 8. Inserting an Ethernet cable

2. Insert the RJ-45 connector on the other end into the target device, such as a router or switch.
3. Verify that the LED glows amber when the connection is established.

To connect the Ethernet cable to a 1G SFP fiber, or 10G SFP +, or XFP transceiver

1. Remove the dust caps from the transceiver and cable.
2. Insert the LC connector on one end of the fiber optic cable into the appropriate port on the front panel of the appliance.
3. Insert the connector on the other end into the target device, such as a router or switch.
4. Verify that the LED glows amber when the connection is established.

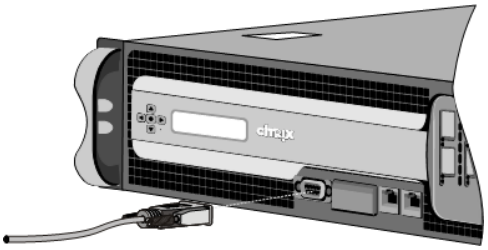
Connecting the Console Cable

You can use the console cable to connect your appliance to a computer or terminal, from which you can configure the appliance. Alternatively, you can use a computer connected to the network. Before connecting the console cable, configure the computer or terminal to support VT100 terminal emulation, 9600 baud, 8 data bits, 1 stop bit, parity, and flow control set to NONE. Then connect one end of the console cable to the RS232 serial port on the appliance and the other end to the computer or terminal.

To connect the console cable to a computer or terminal

1. Insert the DB-9 connector at the end of the cable into the console port that is located on the front panel of the appliance, as shown in the following figure.

   Figure 9. Inserting a console cable

   Note: To use a cable with an RJ-45 converter, insert the optional converter provided into the console port and attach the cable to it.

2. Insert the RJ-45 connector at the other end of the cable into the serial port of the computer or terminal.

Connecting the Power CableConnecting the Appliance to a Power Source

An MPX 5500, MPX 5550/5650, MPX 7500/9500, and MPX 8200/8400/8600/8800 appliance has one power cable. All the other appliances come with two power cables,

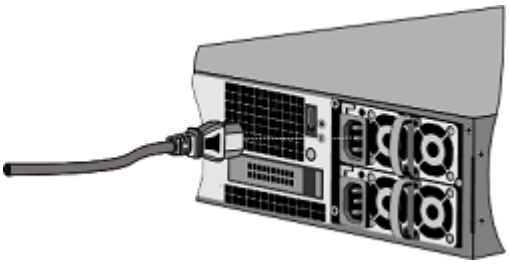
but they can also operate if only one power cable is connected. A separate ground cable is not required, because the three-prong plug provides grounding.

The CloudBridge 4000/5000Repeater on SDX appliance has two power supplies, with one serving as a backup. A separate ground cable is not required, because the three-prong plug provides grounding. Power up the appliance by installing one or both power cords.

To connect the appliance to the power source

1. Connect one end of the power cable to the power outlet on the back panel of the appliance, next to the power supply, as shown in the following figure.

   Figure 10. Inserting a power cable

2. Connect the other end of the power cable to a standard 110V/220V power outlet.
3. If a second power supply is provided, rRepeat steps 1 and 2 to connect the second power supply.

Note: The MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliance emit a high-pitched alert if one power supply fails or if you connect only one power cable to the appliance. To silence the alarm, you can press the small red button located on the back panel of the appliance. The appliance emits a high-pitched alert if one power supply fails or if you connect only one power cable to the appliance. To silence the alarm, you can press the small red button located on the back panel of the appliance.

Accessing a Citrix NetScaler

A NetScaler appliance has both a command line interface (CLI) and a graphical user interface (GUI). The GUI includes a configuration utility for configuring the appliance and a statistical utility, called Dashboard. For initial access, all appliances ship with the default NetScaler IP address (NSIP) of 192.168.100.1 and default subnet mask of 255.255.0.0. You can assign a new NSIP and an associated subnet mask during initial configuration.

If you encounter an IP address conflict when deploying multiple NetScaler units, check for the following possible causes:

- Did you select an NSIP that is an IP address already assigned to another device on your network?
- Did you assign the same NSIP to multiple NetScaler appliances?
- The NSIP is reachable on all physical ports. The ports on a NetScaler are host ports, not switch ports.

The following table summarizes the available access methods.

Table 1. Methods for Accessing a NetScaler appliance

Access Method	Port	Default IP Address Required? (Y/N)
CLI	Console	N
CLI and GUI	Ethernet	Y

Using the Command Line Interface

You can access the CLI either locally, by connecting a workstation to the console port, or remotely, by connecting through secure shell (SSH) from any workstation on the same network.

Logging on to the Command Line Interface through the Console Port

The appliance has a console port for connecting to a computer workstation. To log on to the appliance, you need a serial crossover cable and a workstation with a terminal emulation program.

To log on to the CLI through the console port

1. Connect the console port to a serial port on the workstation, as described in "Connecting the Console Cable".
2. On the workstation, start HyperTerminal or any other terminal emulation program. If the logon prompt does not appear, you may need to press ENTER one or more times to display it.
3. Log on by using the administrator credentials.
   The command prompt (>) appears on the workstation monitor.

Logging on to the Command Line Interface by using SSH

The SSH protocol is the preferred remote access method for accessing an appliance remotely from any workstation on the same network. You can use either SSH version 1 (SSH1) or SSH version 2 (SSH2.)

If you do not have a working SSH client, you can download and install any of the following SSH client programs:

- PuTTY

  Open Source software supported on multiple platforms. Available at:

  "http://www.chiark.greenend.org.uk/~sgtatham/putty/"

- Vandyke Software SecureCRT

  Commercial software supported on the Windows platform. Available at:

  "http://www.vandyke.com/products/securecrt/"

These programs have been tested by the Citrix NetScaler team, which has verified that they work correctly with a NetScaler appliance. Other programs may also work correctly, but have not been tested.

To verify that the SSH client is installed properly, use it to connect to any device on your network that accepts SSH connections.

To log on to a NetScaler by using an SSH client

1. On your workstation, start the SSH client.
2. For initial configuration, use the default NetScaler IP address (NSIP), which is 192.168.100.1. For subsequent access, use the NSIP that was assigned during initial configuration. Select either SSH1 or SSH2 as the protocol.
3. Log on by using the administrator credentials. For example:

```
login as: nsroot
Using keyboard-interactive authentication.
Password:
```

```
Last login: Tue Jun 16 10:37:28 2009 from 10.102.29.9

 Done
>
```

Using the Graphical User Interface

Important: A certificate-key pair is required for HTTPS access to the NetScaler configuration utility. On a NetScaler ADC, a certificate-key pair is automatically bound to the internal services. On an MPX or SDX appliance, the default key size is 1024 bytes, and on a VPX instance, the default key size is 512 bytes. However, most browsers today do not accept a key that is less than 1024 bytes. As a result, HTTPS access to the VPX configuration utility is blocked.

Additionally, if a license is not present on an MPX appliance when it starts, and you add a license later and restart the appliance, you might lose the certificate binding.

Citrix recommends that you install a certificate-key pair of at least 1024 bytes on a NetScaler ADC for HTTPS access to the configuration utility, and that you install an appropriate license before starting the ADC.

The graphical user interface includes a configuration utility and a statistical utility, called Dashboard, either of which you access through a workstation connected to an Ethernet port on the appliance. If your computer does not have a supported Java plug-in installed, the utility prompts you to download and install the plug-in the first time you log on. If automatic installation fails, you can install the plug-in separately before you attempt to log on to the configuration utility or Dashboard.

The system requirements for the workstation running the GUI are as follows:

- For Windows-based workstations, a Pentium 166 MHz or faster processor with at least 48 MB of RAM is recommended for applets running in a browser using a Java plug-in product. You should have 40 MB free disk space before installing the plug-in.
- For Linux-based workstations, a Pentium platform running Linux kernel v2.2.12 or above, and glibc version 2.12-11 or later. A minimum of 32 MB RAM is required, and 48 MB RAM is recommended. The workstation should support 16-bit color mode, KDE and KWM window managers used in conjunction, with displays set to local hosts.
- For Solaris-based workstations, a Sun running either Solaris 2.6, Solaris 7, or Solaris 8, and the Java 2 Runtime Environment, Standard Edition, version 1.6 or later.

Your workstation must have a supported web browser and version 1.6 or above of the Java applet plug-in installed to access the configuration utility and Dashboard.

The following browsers are supported.

Using the Configuration Utility

Once you log on to the configuration utility, you can configure the appliance through a graphical interface that includes context-sensitive help.

If your computer does not have a supported Java plug-in installed, the first time you log on to the appliance, the configuration utility will prompt you to download and install the plug-in.

Note: Prior to installing the Java 2 Runtime Environment, ensure that you have installed the full set of required operating system patches needed for the current Java release.

To log on to the configuration utility

1. Open your web browser and enter the NetScaler IP (NSIP) as an HTTP address. If you have not yet set up the initial configuration, enter the default NSIP (`http://192.168.100.1`).
   The **Citrix Logon** page appears.

   Note: If you have two NetScaler appliances in a high availability setup, make sure that you do not access the GUI by entering the IP address of the secondary NetScaler. If you do so and use the GUI to configure the secondary NetScaler, your configuration changes will not be applied to the primary NetScaler.

2. In the **User Name** text box, type `nsroot`.
3. In the **Password** text box, type the administrative password you assigned to the nsroot account during initial configuration and click **Login**.
   The **Configuration Utility** page appears.

   Note: If your workstation does not already have a supported version of the Java runtime plug-in installed, the NetScaler prompts you to download the Java Plug-in. After the download is complete, the configuration utility page appears.

   If you need to access the online help, select Help from the Help menu at the top right corner.

4. In the **Start in** list, click **Configuration**, and then click **Login**.
   The **Configuration Utility** page appears.

   Note: If your workstation does not already have a supported version of the Java runtime plug-in installed, the NetScaler prompts you to download the Java Plug-in. After the download is complete, the configuration utility page appears.

   If you need to access the online help, select Help from the Help menu at the top right corner.

Using the Statistical Utility

Dashboard, the statistical utility, is a browser-based application that displays charts and tables on which you can monitor the performance of a NetScaler.

To log on to Dashboard

1. Open your web browser and enter the NSIP as an HTTP address (http://<NSIP>). The **Citrix Logon** page appears.
2. In the **User Name** text box, type `nsroot`.
3. In the **Password** text box, type the administrative password you assigned to the nsroot account during initial configuration.
4. In the **Start in** list, click **Dashboard**, and then click **Login**.

Installing the Java Runtime Plug-in

If automatic installation of the Java plug-in fails, you can install the plug-in separately before you attempt to log on to the configuration utility.

Note: Before installing the Java 2 Runtime Environment, make sure that you have installed the full set of required operating system patches needed for the current Java release.

To install the Java runtime plug-in on your workstation

1. In your web browser, enter the NSIP and port number of your appliance: `http://<NSIP>:80`
   The Java plug-in icon appears.
2. Click the Java plug-in icon and follow the screen prompts to copy the plug-in installer to your workstation hard disk. The Java plug-in setup icon (for example, **j2re-1.6.0**) appears on your computer at the location you specified.
3. Double-click the plug-in setup icon, and follow the screen prompts to install the plug-in.
4. Return to your web browser and click the Java plug-in icon a second time to display the GUI logon screen.

Configuring a NetScaler for the First Time

Your new NetScaler is preconfigured with a default IP address (the NSIP) and associated subnet mask for management access. The default NSIP is 192.168.100.1 and the subnet mask (netmask) is 255.255.0.0. You can change these values to fit the addressing scheme for your network. For your initial configuration, you must also specify at least one SNIP or MIP. Before saving your new configuration, you should change the administrator password.

You can perform the initial configuration of your appliance by using any of the following interfaces:

- LCD Keypad
- Command Line Interface
- Configuration Utility
- XML API

If you are setting up two NetScaler appliances as a high availability pair, you configure one as primary and the other as secondary.

The configuration procedure for a FIPS appliance is slightly different from the procedure for a NetScaler MPX appliance or a NetScaler virtual appliance.

Using the LCD Keypad

When you first install the appliance, you can configure the initial settings by using the LCD keypad on the front panel of the appliance. The keypad interacts with the LCD display module, which is also on the front panel of these appliances.

Note: You can use the LCD keypad for initial configuration on a new appliance with the default configuration. The configuration file (ns.conf) should contain the following command and default values.

set ns config -IPAddress 192.168.100.1 -netmask 255.255.0.0

The functions of the different keys are explained in the following table.

Table 1. LCD Key Functions

Key	Function
<	Moves the cursor one digit to the left.
>	Moves the cursor one digit to the right.

Key	Function
^	Increments the digit under the cursor.
v	Decrements the digit under the cursor.
.	Processes the information, or terminates the configuration, if none of the values are changed. This key is also known as the ENTER key.

To perform the initial configuration by using the LCD keypad press the "<" key.

You are prompted to enter the subnet mask, NetScaler IP address (NSIP), and gateway in that order respectively. The subnet mask is associated with both the NSIP and default gateway IP address. The NSIP is the IPv4 address of the NetScaler appliance. The default gateway is the IPv4 address for the router, which will handle external IP traffic that the NetScaler cannot otherwise route. The NSIP and the default gateway should be on the same subnet.

If you enter a valid value for the subnet mask, such as 255.255.255.224, you are prompted to enter the IP address. Similarly, if you enter a valid value for the IP address, you are prompted to enter the gateway address. If the value you entered is invalid, the following error message appears for three seconds, where xxx.xxx.xxx.xxx is the IP address you entered, followed by a request to re-enter the value.

```
Invalid addr!
xxx.xxx.xxx.xxx
```

If you press the ENTER (.) key without changing any of the digits, the software interprets this as a user exit request. The following message will be displayed for three seconds.

```
Exiting menu...
xxx.xxx.xxx.xxx
```

If all the values entered are valid, when you press the ENTER key, the following message appears.

```
Values accepted,
Rebooting...
```

The subnet mask, NSIP, and gateway values are saved in the configuration file.

Note: For information about deploying a high availability (HA) pair, see "http://support.citrix.com/proddocs/topic/ns-system-10-map/ns-nw-ha-cnfgrng-ha-con.html."

Configuring a NetScaler by Using the Command Line Interface

When you first install the appliance, you can configure the initial settings by using the serial console. Connect a serial cable to the port on the appliance and the other end to a computer. For remote access to the command-line interface (CLI), see Logging on to the Command Line Interface by using SSH. At the CLI, you can setup or change the NSIP, subnet or mapped IP address, advanced network settings, and time zone.

To configure a NetScaler by using the command line interface

1. Connect a workstation to the NetScaler.
2. Run the vt100 terminal emulation program of your choice on your workstation or notebook computer to connect to the appliance.
   - For Microsoft Windows, you can use Hyperterminal, which is installed with all current versions of Windows.
   - For Apple Macintosh OSX, you can use the GUI-based Terminal program or the shell-based telnet client.

     Note: OSX is based on the FreeBSD UNIX platform. Most standard UNIX shell programs are available from the OSX command line.
   - For UNIX-based workstations, you can use the shell-based telnet client or any supported terminal emulation program.
3. Press ENTER.
   The terminal screen displays the Logon prompt.

   Note: You might have to press ENTER two or three times, depending on which terminal program you are using.
4. Log on to the appliance by using the administrator credentials.

   Note: Your sales representative or Citrix Customer Service can provide the administrator credentials.
5. At the NetScaler command prompt, you can type **config ns** and follow the prompts to complete the initial configuration. Alternatively, type the commands shown in the following steps.

   Note: To prevent an attacker from breaching your ability to send packets to the appliance, choose a non-routable IP address on your organization's LAN as your appliance IP address.
6. **set ns config** `-ipaddress <IPAddress> -netmask <Netmask>`
7. **add ns ip** `<IPAddress> <Netmask> -type <Type>`

8. **add route** `<Network> <Netmask> <Gateway>`
9. **set system user nsroot** `<Password>`
10. **save ns config**
11. **reboot**

    Example

```
set ns config - ipaddress 10.102.29.60 - netmask
255.255.255.0
add ns ip 10.102.29.61 255.255.255.0 -type snip
add route 0.0.0.0 0.0.0.0 10.102.29.1
set system user nsroot administrator
save ns config
reboot
```

Configuring a NetScaler by Using the Configuration Utility

The configuration utility is accessed from a web browser. To configure the NetScaler using the Setup Wizard in the configuration utility, you need an administrative workstation or laptop configured on the same network as the appliance. You also need Java RunTime Environment (JRE) version 1.6 or later. You can use the Setup Wizard to configure the following initial settings:

- System IP address and subnet mask
- Subnet or Mapped IP address and subnet mask
- Host name
- Default gateway
- Time zone
- Licenses
- Administrator password

Important: Before running the Setup Wizard, you should download your licenses from the Citrix web site and put them in a location on your workstation or laptop hard drive or another device where you can access them from your web browser during configuration.

To configure initial settings by using the Setup Wizard

1. In a web browser, type `http:// 192.168.100.1`.

Note: The operating system is preconfigured with a default IP address and associated netmask. The default IP address is 192.168.100.1 and the default netmask is 255.255.0.0.

2. In **User Name** and **Password**, type the administrator credentials. You can obtain the initial user name and password from your sales representative or from Citrix Customer Service.
3. In **Start in**, select **Configuration**, and then click **Login**.
4. In the **Setup Wizard**, click **Next**, and then follow the instructions in the wizard.

Note: To prevent an attacker from breaching your ability to send packets to the appliance, choose a non-routable IP address on your organization's LAN as your appliance IP address.

Configuring a NetScaler by Using the XML API

You can use an external Application Programming Interface (API) to configure the NetScaler. The API allows you to create custom client applications to configure and monitor the state of the NetScaler. It is based on Simple Object Access Protocol (SOAP) over HTTP. You can download the API documentation from the Downloads page of the configuration utility.

Configuring a High Availability Pair for the First Time

You can deploy two NetScaler appliances in a high availability configuration, where one unit actively accepts connections and manages servers while the secondary unit monitors the first. The NetScaler that is actively accepting connections and managing the servers is called a primary unit and the other one is called a secondary unit in a high availability configuration. If there is a failure in the primary unit, the secondary unit becomes the primary and begins actively accepting connections.

Each NetScaler in a high availability pair monitors the other by sending periodic messages, called heartbeat messages or health checks, to determine the health or state of the peer node. If a health check for a primary unit fails, the secondary unit retries the connection for a specific time period. For more information about high availability, see "High Availability." If a retry does not succeed by the end of the specified time period, the secondary unit takes over for the primary unit in a process called failover. The following figure shows two high availability configurations, one in one-arm mode and the other in two-arm mode.

Figure 1. High availability in one-arm mode

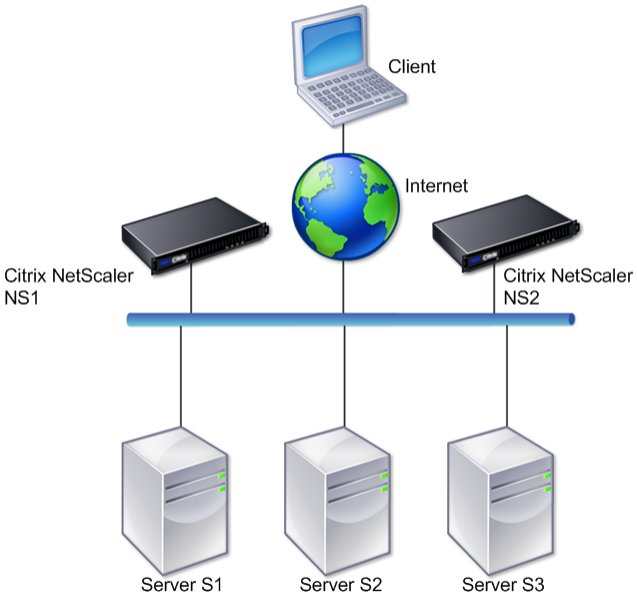
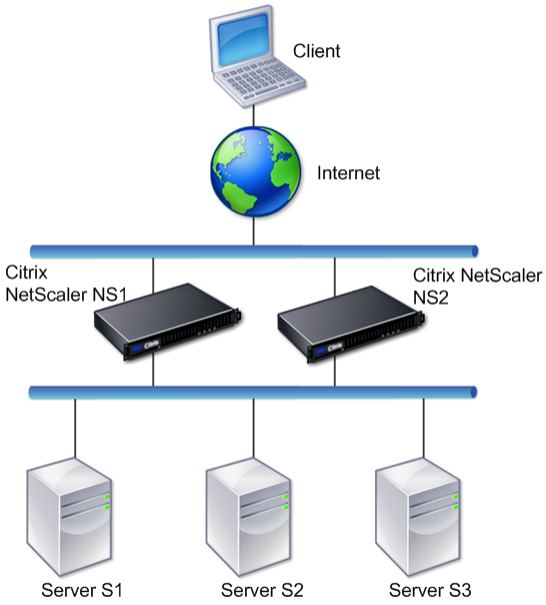


Figure 2. High availability in two-arm mode



In one-arm configuration, both NS1 and NS2 and servers S1, S2, and S3 are connected to the switch.

In two-arm configuration, both NS1 and NS2 are connected to two switches. The servers S1, S2, and S3 are connected to the second switch. The traffic between client and the servers passes through either NS1 or NS2.

To set up a high availability environment, configure one NetScaler as primary and another as secondary. Perform the following tasks on each of the NetScalers:

- Add a node.
- Disable high availability monitoring for unused interfaces.

Adding a Node

A node is a logical representation of a peer NetScaler appliance. It identifies the peer unit by ID and NSIP. An appliance uses these parameters to communicate with the peer and track its state. When you add a node, the primary and secondary units exchange heartbeat messages asynchronously. The node ID is an integer that must not be greater than 64.

To add a node by using the command line interface

At the command prompt, type the following commands to add a node and verify that the node has been added:

- **add HA node** `<id> <IPAddress>`
- **show HA node** `<id>`

  Example

```
add HA node 0 10.102.29.170
 Done
> show HA node 0
1)      Node ID:      0
        IP:   10.102.29.200 (NS200)
        Node State: UP
        Master State: Primary
        SSL Card Status: UP
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 1:0:41:50
(days:hrs:min:sec)
```

To add a node by using the configuration utility

1. In the navigation pane, expand **System** and click **High Availability**.
   The **High Availability** page appears.
2. On the **High Availability** page, select the **Nodes** tab.
3. Click **Add**.
   The **High Availability Setup** dialog box appears.
4. In the **High Availability Setup** dialog box, in the **Remote Node IP Address** text box, type an IP Address (for example, `10.102.29.170`).
5. Ensure that the **Configure remote system to participate in High Availability setup** check box is selected.

   By default, this check box is selected.
6. Select the **Turn off HA monitor on interfaces/channels that are down** check box to disable the HA monitor on interfaces that are down.

   By default, this check box is selected.
7. Verify that the node you added appears in the list of nodes under the **Nodes** tab.

Disabling High Availability Monitoring for Unused Interfaces

The high availability monitor is a virtual entity that monitors an interface. You must disable the monitor for interfaces that are not connected or being used for traffic. When the monitor is enabled on an interface whose status is DOWN, the state of the node becomes NOT UP. In a high availability configuration, a primary node entering a NOT UP state might cause a high availability failover. An interface is marked DOWN under the following conditions:

- The interface is not connected

- The interface is not working properly
- The cable connecting the interface is not working properly

To disable the high availability monitor for an unused interface by using the command line interface

At the command prompt, type the following commands to disable the high availability monitor for an unused interface and verify that it is disabled:

- **set interface** `<id> -haMonitor OFF`
- **show interface** `<id>`

  Example

```
> set interface 1/8 -haMonitor OFF
 Done
> show interface 1/8
        Interface 1/8 (Gig Ethernet 10/100/1000 MBits) #2
        flags=0x4000 <ENABLED, DOWN, down, autoneg, 802.1q>
        MTU=1514, native vlan=1, MAC=00:d0:68:15:fd:3d,
downtime 238h55m44s
        Requested: media AUTO, speed AUTO, duplex AUTO, fctl
OFF,
                  throughput 0

        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0)
Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
```

  When the high availability monitor is disabled for an unused interface, the output of the **show interface** command for that interface does not include "HAMON."

To disable the high availability monitor for unused interfaces by using the configuration utility

1. In the navigation pane, expand **Network** and click **Interfaces**.
   The **Interfaces** page appears.
2. Select the interface for which the monitor must be disabled.
3. Click **Open**.
   The **Modify Interface** dialog box appears.
4. In **HA Monitoring**, select the **OFF** option.
5. Click **OK**.
6. Verify that, when the interface is selected, "HA Monitoring: OFF" appears in the details at the bottom of the page.

Configuring a FIPS Appliance for the First Time

A certificate-key pair is required for HTTPS access to the configuration utility and for secure remote procedure calls. RPC nodes are internal system entities used for system-to-system communication of configuration and session information. One RPC node exists on each appliance. This node stores the password, which is checked against the one provided by the contacting appliance. To communicate with other NetScaler appliances, each appliance requires knowledge of the other appliances, including how to authenticate on the other appliance. RPC nodes maintain this information, which includes the IP addresses of the other NetScaler appliances and the passwords used to authenticate on each.

On a NetScaler MPX appliance virtual appliance, a certificate-key pair is automatically bound to the internal services. On a FIPS appliance, a certificate-key pair must be imported into the hardware security module (HSM) of a FIPS card. To do so, you must configure the FIPS card, create a certificate-key pair, and bind it to the internal services.

To configure secure HTTPS by using the command line interface

1. Initialize the hardware security module (HSM) on the FIPS card of the appliance. For information about initializing the HSM, see "Configuring the HSM."
2. If the appliance is part of a high availability setup, enable the SIM. For information about enabling the SIM on the primary and secondary appliances, see " Configuring FIPS Appliances in a High Availability Setup."
3. Import the FIPS key into the HSM of the FIPS card of the appliance. At the command prompt, type:

   import ssl fipskey *serverkey* -key *ns-server.key* -inform `PEM`
4. Add a certificate-key pair. At the command prompt, type:

   add certkey server -cert *ns-server.cert* -fipskey *serverkey*
5. Bind the certificate-key created in the previous step to the following internal services. At the command prompt, type:

   bind ssl service `nshttps-127.0.0.1-443` -certkeyname server

   bind ssl service `nshttps-::11-443` -certkeyname server

To configure secure HTTPS by using the configuration utility

1. Initialize the hardware security module (HSM) on the FIPS card of the appliance. For information about initializing the HSM, see "Configuring the HSM."

2. If the appliance is part of a high availability setup, enable the secure information system (SIM). For information about enabling the SIM on the primary and secondary appliances, see " Configuring FIPS Appliances in a High Availability Setup."
3. Import the FIPS key into the HSM of the FIPS card of the appliance. For more information about importing a FIPS key, see "Importing an Existing FIPS Key."
4. In the navigation pane, expand **SSL**, and then click **Certificates**.
5. In the details pane, click **Install**.
6. In the **Install Certificate** dialog box, type the certificate details.
7. Click **Create**, and then click **Close**.
8. In the navigation pane, expand **Load Balancing**, and then click **Services**.
9. In the details pane, click **Internal Services**.
10. Select **nshttps-127.0.0.1-443** from the list, and then click **Open**.
11. On the **SSL Settings** tab, in the **Available** pane, select the certificate created in step 7, click **Add**, and then click **OK**.
12. Select **nshttps-::11-443** from the list, and then click **Open**.
13. On the **SSL Settings** tab, in the **Available** pane, select the certificate created in step 7, click **Add**, and then click **OK**.
14. Click **OK**.

To configure secure RPC by using the command line interface

1. Initialize the hardware security module (HSM) on the FIPS card of the appliance. For information about initializing the HSM, see "Configuring the HSM."
2. Enable the secure information system (SIM). For information about enabling the SIM on the primary and secondary appliances, see " Configuring FIPS Appliances in a High Availability Setup."
3. Import the FIPS key into the HSM of the FIPS card of the appliance. At the command prompt, type:

   import ssl fipskey *serverkey* -key *ns-server.key* -inform `PEM`
4. Add a certificate-key pair. At the command prompt, type:

   add certkey server -cert *ns-server.cert* -fipskey *serverkey*
5. Bind the certificate-key pair to the following internal services. At the command prompt, type:

   bind ssl service `nsrpcs-127.0.0.1-3008` -certkeyname server

   bind ssl service `nskrpcs-127.0.0.1-3009` -certkeyname server

   bind ssl service `nsrpcs-::11-3008` -certkeyname server

6. Enable secure RPC mode. At the command prompt, type:

   set ns rpcnode <IP address> -secure `YES`

To configure secure RPC by using the configuration utility

1. Initialize the hardware security module (HSM) on the FIPS card of the appliance. For information about initializing the HSM, see "Configuring the HSM."
2. Enable the secure information system (SIM). For information about enabling the SIM on the primary and secondary appliances, see " Configuring FIPS Appliances in a High Availability Setup."
3. Import the FIPS key into the HSM of the FIPS card of the appliance. For more information about importing a FIPS key, see "Importing an Existing FIPS Key."
4. In the navigation pane, expand **SSL**, and then click **Certificates**.
5. In the details pane, click **Install**.
6. In the **Install Certificate** dialog box, type the certificate details.
7. Click **Create**, and then click **Close**.
8. In the navigation pane, expand **Load Balancing**, and then click **Services**.
9. In the details pane, click **Internal Services**.
10. Select **nsrpcs-127.0.0.1-3008** from the list, and then click **Open**.
11. On the **SSL Settings** tab, in the **Available** pane, select the certificate created in step 7, click **Add**, and then click **OK**.
12. Select **nskrpcs-127.0.0.1-3009** from the list, and then click **Open**.
13. On the **SSL Settings** tab, in the **Available** pane, select the certificate created in step 7, click **Add**, and then click **OK**.
14. Select **nsrpcs-::11-3008** from the list, and then click **Open**.
15. On the **SSL Settings** tab, in the **Available** pane, select the certificate created in step 7, click **Add**, and then click **OK**.
16. Click **OK**.
17. In the navigation pane, expand **Network**, and then click **RPC**.
18. In the details pane, select the IP address, and click **Open**.
19. In the **Configure RPC Node** dialog box, select **Secure**.
20. Click **OK**.

Understanding Common Network Topologies

As described in "Physical Deployment Modes," you can deploy the Citrix NetScaler appliance either inline between the clients and servers or in one-arm mode. Inline mode uses a two-arm topology, which is the most common type of deployment.

Setting Up Common Two-Arm Topologies

In a two-arm topology, one network interface is connected to the client network and another network interface is connected to the server network, ensuring that all traffic flows through the appliance. This topology might require you to reconnect your hardware and also might result in a momentary downtime. The basic variations of two-arm topology are multiple subnets, typically with the appliance on a public subnet and the servers on a private subnet, and transparent mode, with both the appliance and the servers on the public network.

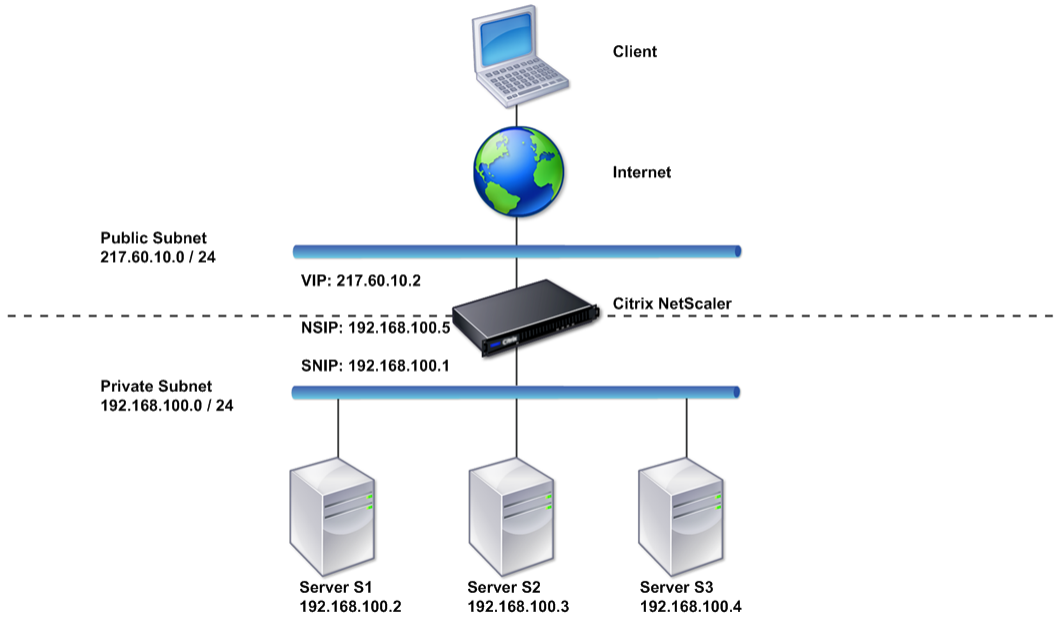
Setting Up a Simple Two-Arm Multiple Subnet Topology

One of the most commonly used topologies has the NetScaler appliance inline between the clients and the servers, with a virtual server configured to handle the client requests. This configuration is used when the clients and servers reside on different subnets. In most cases, the clients and servers reside on public and private subnets, respectively.

For example, consider an appliance deployed in two-arm mode for managing servers S1, S2, and S3, with a virtual server of type HTTP configured on the appliance, and with HTTP services running on the servers. The servers are on a private subnet and a SNIP is configured on the appliance to communicate with the servers. The Use SNIP (USNIP) option must be enabled on the appliance so that it uses the SNIP instead of the MIP.

As shown in the following figure, the VIP is on public subnet 217.60.10.0, and the NSIP, the servers, and the SNIP are on private subnet 192.168.100.0/24.

Figure 1. Topology Diagram for Two-Arm Mode, Multiple Subnets



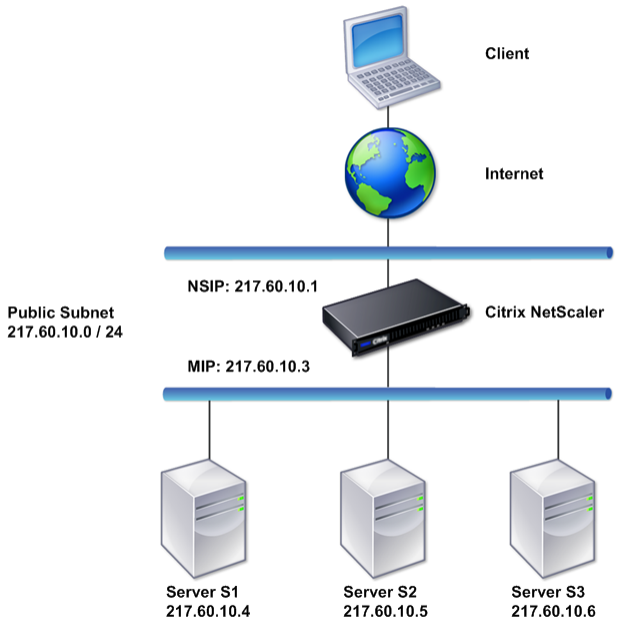
Task overview: To deploy a NetScaler appliance in two-arm mode with multiple subnets

1. Configure the NSIP and default gateway, as described in "Configuring the NetScaler IP Address (NSIP)."
2. Configure the SNIP, as described in "Configuring Subnet IP Addresses."
3. Enable the USNIP option, as described in "To enable or disable USNIP mode."
4. Configure the virtual server and the services, as described in "Creating a Virtual Server" and "Configuring Services."
5. Connect one of the network interfaces to a private subnet and the other interface to a public subnet.

Setting Up a Simple Two-Arm Transparent Topology

Use transparent mode if the clients need to access the servers directly, with no intervening virtual server. The server IP addresses must be public because the clients need to be able to access them. In the example shown in the following figure, a NetScaler appliance is placed between the client and the server, so the traffic must pass through the appliance. You must enable L2 mode for bridging the packets. The NSIP and MIP are on the same public subnet, 217.60.10.0/24.

Figure 2. Topology Diagram for Two-Arm, Transparent Mode



Task overview: To deploy a NetScaler in two-arm, transparent mode

1. Configure the NSIP, MIP, and default gateway, as described in "Configuring a NetScaler by Using the Command Line Interface."
2. Enable L2 mode, as described in "Enabling and Disabling Layer 2 Mode."
3. Configure the default gateway of the managed servers as the MIP.
4. Connect the network interfaces to the appropriate ports on the switch.

Setting Up Common One-Arm Topologies

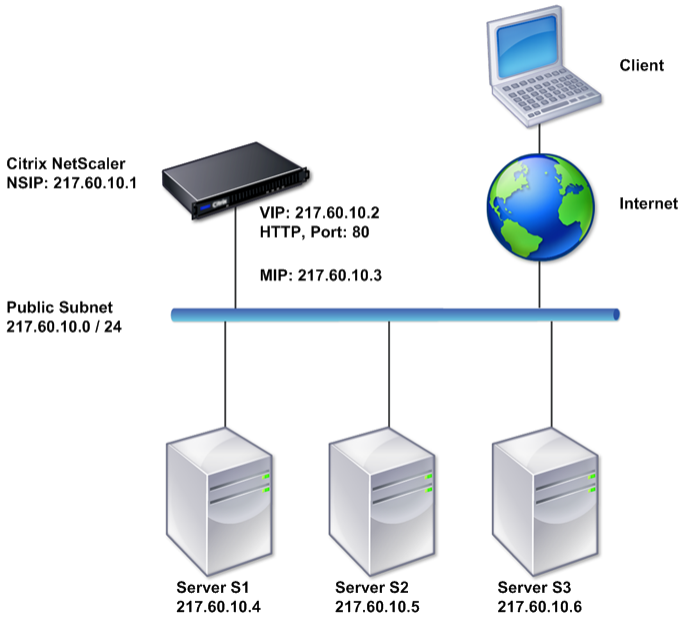
The two basic variations of one-arm topology are with a single subnet and with multiple subnets.

Setting Up a Simple One-Arm Single Subnet Topology

You can use a one-arm topology with a single subnet when the clients and servers reside on the same subnet. For example, consider a NetScaler deployed in one-arm mode for managing servers S1, S2, and S3. A virtual server of type HTTP is configured on a NetScaler, and HTTP services are running on the servers. As shown in the following

figure, the NetScaler IP address (NSIP), the Mapped IP address (MIP), and the server IP addresses are on the same public subnet, 217.60.10.0/24.

Figure 3. Topology Diagram for One-Arm Mode, Single Subnet



Task overview: To deploy a NetScaler in one-arm mode with a single subnet

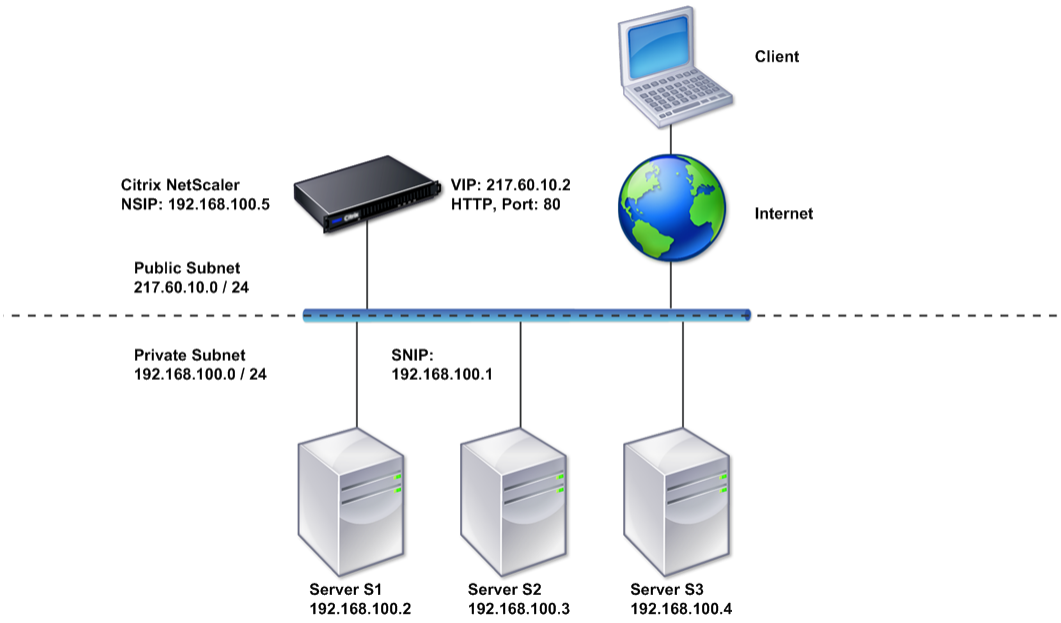
1. Configure the NSIP, MIP, and the default gateway, as described in "Configuring the NetScaler IP Address (NSIP)".
2. Configure the virtual server and the services, as described in "Creating a Virtual Server" and "Configuring Services".
3. Connect one of the network interfaces to the switch.

Setting Up a Simple One-Arm Multiple Subnet Topology

You can use a one-arm topology with multiple subnets when the clients and servers reside on the different subnets. For example, consider a NetScaler appliance deployed in one-arm mode for managing servers S1, S2, and S3, with the servers connected to switch SW1 on the network. A virtual server of type HTTP is configured on the appliance, and HTTP services are running on the servers. These three servers are on the private subnet, so a subnet IP address (SNIP) is configured to communicate with them. The Use Subnet IP address (USNIP) option must be enabled so that the appliance uses the SNIP instead of a MIP. As shown in the following figure, the virtual IP address

(VIP) is on public subnet 217.60.10.0/24; the NSIP, SNIP, and the server IP addresses are on private subnet 192.168.100.0/24.

Figure 4. Topology Diagram for One-Arm Mode, Multiple Subnets



Task overview: To deploy a NetScaler appliance in one-arm mode with multiple subnets

1. Configure the NSIP and the default gateway, as described in "Configuring the NetScaler IP Address (NSIP)".
2. Configure the SNIP and enable the USNIP option, as described in "Configuring Subnet IP Addresses".
3. Configure the virtual server and the services, as described in "Creating a Virtual Server" and "Configuring Services".
4. Connect one of the network interfaces to the switch.

Configuring System Management Settings

Once your initial configuration is in place, you can configure settings to define the behavior of the Citrix NetScaler appliance and facilitate connection management. You have a number of options for handling HTTP requests and responses. Routing, bridging, and MAC based forwarding modes are available for handling packets not addressed to the NetScaler. You can define the characteristics of your network interfaces and can aggregate the interfaces. To prevent timing problems, you can synchronize the NetScaler clock with a Network Time Protocol (NTP) server. The NetScaler can operate in various DNS modes, including as an authoritative domain name server (ADNS). You can set up SNMP for system management and customize syslog logging of system events. Before deployment, verify that your configuration is complete and correct.

Configuring System Settings

Configuration of system settings includes basic tasks such as configuring HTTP ports to enable connection keep-alive and server offload, setting the maximum number of connections for each server, and setting the maximum number of requests per connection. You can enable client IP address insertion for situations in which a proxy IP address is not suitable, and you can change the HTTP cookie version.

You can also configure a NetScaler appliance to open FTP connections on a controlled range of ports instead of ephemeral ports for data connections. This improves security, because opening all ports on the firewall is insecure. You can set the range anywhere from 1,024 to 64,000.

Before deployment, go through the verification checklists to verify your configuration. To configure HTTP parameters and the FTP port range, use the NetScaler configuration utility.

You can modify the types of HTTP parameters described in the following table.

Table 1. HTTP Parameters

Parameter Type	Specifies
HTTP Port Information	The web server HTTP ports used by your managed servers. If you specify the ports, the appliance performs request switching for any client request that has a destination port matching a specified port.

Parameter Type	Specifies
	Note: If an incoming client request is not destined for a service or a virtual server that is specifically configured on the appliance, the destination port in the request must match one of the globally configured HTTP ports. This allows the appliance to perform connection keep-alive and server off-load.
Limits	The maximum number of connections to each managed server, and the maximum number of requests sent over each connection. For example, if you set **Max Connections** to 500, and the appliance is managing three servers, it can open a maximum of 500 connections to each of the three servers. By default, the appliance can create an unlimited number of connections to any of the servers it manages. To specify an unlimited number of requests per connection, set **Max Requests** to 0. **Note:** If you are using the Apache HTTP server, you must set **Max Connections** equal to the value of the MaxClients parameter in the Apache httpd.conf file. Setting this

Parameter Type	Specifies
	parameter is optional for other web servers.
Client IP Insertion	Enable/disable insertion of the client's IP address into the HTTP request header. You can specify a name for the header field in the adjacent text box. When a web server managed by an appliance receives a mapped IP address or a subnet IP address, the server identifies it as the client’s IP address. Some applications need the client’s IP address for logging purposes or to dynamically determine the content to be served by the web server. You can enable insertion of the actual client IP address into the HTTP header request sent from the client to one, some, or all servers managed by the appliance. You can then access the inserted address through a minor modification to the server (using an Apache module, ISAPI interface, or NSAPI interface).
Cookie Version	The HTTP cookie version to use when COOKIEINSERT persistence is configured on a virtual server. The default, version 0, is the most common type on the Internet. Alternatively, you can specify version 1.

Parameter Type	Specifies
Requests/Responses	Options for handling certain types of requests, and enable/disable logging of HTTP error responses.
Server Header Insertion	Insert a server header in NetScaler-generated HTTP responses.

To configure HTTP parameters by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.
2. In the details pane, under **Settings**, click **Change HTTP parameters**.
3. In the **Configure HTTP parameters** dialog box, specify values for some or all of the parameters that appear under the headings listed in the table above.
4. Click **OK**.

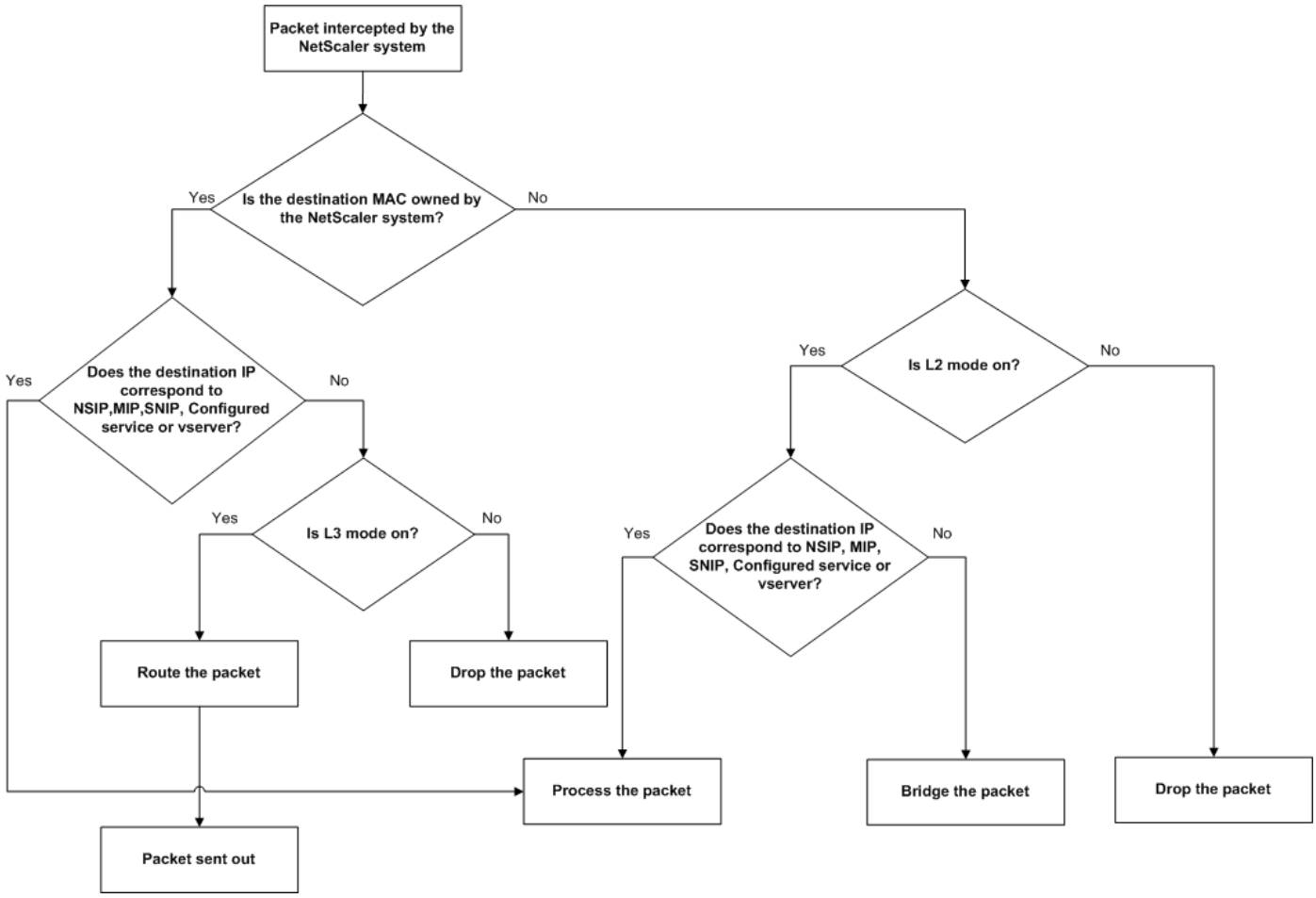
To set the FTP port range by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.
2. In the details pane, under **Settings**, click **Change global system settings**.
3. Under **FTP Port Range**, in the **Start Port** and **End Port** text boxes, type the lowest and highest port numbers, respectively, for the range you want to specify (for example, 5000 and 6000).
4. Click **OK**.

Configuring Modes of Packet Forwarding

The NetScaler appliance can either route or bridge packets that are not destined for an IP address owned by the appliance (that is, the IP address is not the NSIP, a MIP, a SNIP, a configured service, or a configured virtual server). By default, L3 mode (routing) is enabled and L2 mode (bridging) is disabled, but you can change the configuration. The following flow chart shows how the appliance evaluates packets and either processes, routes, bridges, or drops them.

Figure 1. Interaction between Layer 2 and Layer 3 Modes



An appliance can use the following modes to forward the packets it receives:

- Layer 2 (L2) Mode
- Layer 3 (L3) Mode
- MAC-Based Forwarding Mode

Enabling and Disabling Layer 2 Mode

Layer 2 mode controls the Layer 2 forwarding (bridging) function. You can use this mode to configure a NetScaler appliance to behave as a Layer 2 device and bridge the packets that are not destined for it. When this mode is enabled, packets are not forwarded to any of the MAC addresses, because the packets can arrive on any interface of the appliance and each interface has its own MAC address.

With Layer 2 mode disabled (which is the default), the appliance drops packets that are not destined for one of its MAC address. If another Layer 2 device is installed in parallel with the appliance, Layer 2 mode must be disabled to prevent bridging (Layer

2) loops. You can use the configuration utility or the command line to enable Layer 2 mode.

Note: The appliance does not support spanning tree protocol. To avoid loops, if you enable L2 mode, do not connect two interfaces on the appliance to the same broadcast domain.

To enable or disable Layer 2 mode by using the command line interface

At the command prompt, type the following commands to enable/disable Layer 2 mode and verify that it has been enabled/disabled:

- **enable ns mode** <Mode>
- **disable ns mode** <Mode>
- **show ns mode**

  Examples

```
> enable ns mode l2
 Done
> show ns mode

      Mode                    Acronym          Status
      -------                 -------          ------
 1)   Fast Ramp               FR               ON
 2)   Layer 2 mode            L2               ON
 .
 .
 .
 Done
>

> disable ns mode l2
 Done
> show ns mode

      Mode                      Acronym          Status
      -------                   -------          ------
 1)   Fast Ramp                 FR               ON
 2)   Layer 2 mode              L2               OFF
 .
 .
 .
 Done
>
```

To enable or disable Layer 2 mode by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.
2. In the details pane, under **Modes and Features**, click **Configure modes**.

3. In the **Configure Modes** dialog box, to enable Layer 2 mode, select the **Layer 2 Mode** check box. To disable Layer 2 mode, clear the check box.
4. Click **OK**.
   The **Enable/Disable Mode(s)?** message appears in the details pane.
5. Click **Yes**.

Enabling and Disabling Layer 3 Mode

Layer 3 mode controls the Layer 3 forwarding function. You can use this mode to configure a NetScaler appliance to look at its routing table and forward packets that are not destined for it. With Layer 3 mode enabled (which is the default), the appliance performs route table lookups and forwards all packets that are not destined for any appliance-owned IP address. If you disable Layer 3 mode, the appliance drops these packets.

To enable or disable Layer 3 mode by using the command line interface

At the command prompt, type the following commands to enable/disable Layer 3 mode and verify that it has been enabled/disabled:

- **enable ns mode** <Mode>
- **disable ns mode** <Mode>
- **show ns mode**

  Examples

```
> enable ns mode l3
 Done
> show ns mode

     Mode                          Acronym          Status
     -------                       -------          ------
 1)  Fast Ramp                     FR               ON
 2)  Layer 2 mode                  L2               OFF
 .
 .
 .
 9)  Layer 3 mode (ip forwarding)  L3               ON
 .
 .
 .
 Done
>

> disable ns mode l3
 Done
> show ns mode

     Mode                          Acronym          Status
     -------                       -------          ------
 1)  Fast Ramp                     FR               ON
```

```
 2)  Layer 2 mode                  L2               OFF
 .
 .
 .
 9)  Layer 3 mode (ip forwarding)  L3               OFF
 .
 .
 .
 Done
>
```

To enable or disable Layer 3 mode by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.
2. In the details pane, under **Modes and Features**, click **Configure modes**.
3. In the **Configure Modes** dialog box, to enable Layer 3 mode, select the **Layer 3 Mode (IP Forwarding)** check box. To disable Layer 3 mode, clear the check box.
4. Click **OK**.
   The **Enable/Disable Mode(s)?** message appears in the details pane.
5. Click **Yes**.

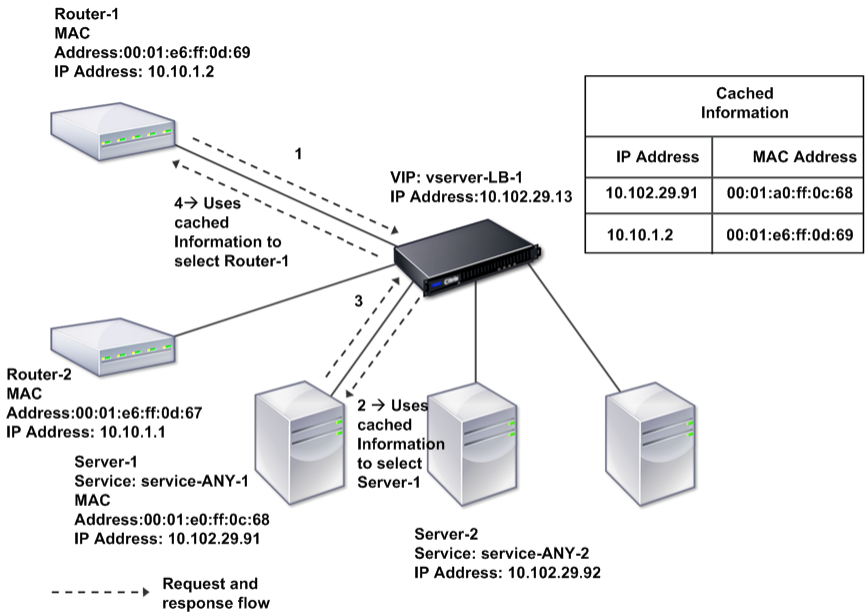
Enabling and Disabling MAC-Based Forwarding Mode

You can use MAC-based forwarding to process traffic more efficiently and avoid multiple-route or ARP lookups when forwarding packets, because the NetScaler appliance remembers the MAC address of the source. To avoid multiple lookups, the appliance caches the source MAC address of every connection for which it performs an ARP lookup, and it returns the data to the same MAC address.

MAC-based forwarding is useful when you use VPN devices because the appliance ensures that all traffic flowing through a particular VPN passes through the same VPN device.

The following figure shows the process of MAC-based forwarding.

Figure 2. MAC-Based Forwarding Process



When MAC-based forwarding is enabled, the appliance caches the MAC address of:

- The source (a transmitting device such as router, firewall, or VPN device) of the inbound connection.
- The server that responds to the requests.

When a server responds through an appliance, the appliance sets the destination MAC address of the response packet to the cached address, ensuring that the traffic flows in a symmetric manner, and then forwards the response to the client. The process bypasses the route table lookup and ARP lookup functions. However, when an appliance initiates a connection, it uses the route and ARP tables for the lookup function. To enable MAC-based forwarding, use the configuration utility or the command line.

Some deployments require the incoming and outgoing paths to flow through different routers. In these situations, MAC-based forwarding breaks the topology design. For a global server load balancing (GSLB) site that requires the incoming and outgoing paths to flow through different routers, you must disable MAC-based forwarding and use the appliance's default router as the outgoing router.

With MAC-based forwarding disabled and Layer 2 or Layer 3 connectivity enabled, a route table can specify separate routers for outgoing and incoming connections. To disable MAC-based forwarding, use the configuration utility or the command line.

To enable or disable MAC-based forwarding by using the command line interface

At the command prompt, type the following commands to enable/disable MAC-based forwarding mode and verify that it has been enabled/disabled:

- **enable ns mode** <Mode>
- **disable ns mode** <Mode>
- **show ns mode**

  Example

```
> enable ns mode mbf
 Done
> show ns mode

     Mode                        Acronym          Status
     -------                     -------          ------
 1)  Fast Ramp                   FR               ON
 2)  Layer 2 mode                L2               OFF
 .
 .
 .
 6)  MAC-based forwarding        MBF              ON
 .
 .
 .
 Done
>

> disable ns mode mbf
 Done
> show ns mode

     Mode                        Acronym          Status
     -------                     -------          ------
 1)  Fast Ramp                   FR               ON
 2)  Layer 2 mode                L2               OFF
 .
 .
 .
 6)  MAC-based forwarding        MBF              OFF
 .
 .
 .
 Done
>
```

To enable or disable MAC-based forwarding by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.

2. In the details pane, under **Modes and Features** group, click **Configure modes**.
3. In the **Configure Modes** dialog box, to enable MAC-based forwarding mode, select the **MAC Based Forwarding** check box. To disable MAC-based forwarding mode, clear the check box.
4. Click **OK**.
   The **Enable/Disable Mode(s)?** message appears in the details pane.
5. Click **Yes**.

Configuring Network Interfaces

NetScaler interfaces are numbered in slot/port notation. In addition to modifying the characteristics of individual interfaces, you can configure virtual LANs to restrict traffic to specific groups of hosts. You can also aggregate links into high-speed channels.

Virtual LANs

The NetScaler supports (Layer 2) port and IEEE802.1Q tagged virtual LANs (VLANs). VLAN configurations are useful when you need to restrict traffic to certain groups of stations. You can configure a network interface to belong to multiple VLANs by using IEEE 802.1q tagging.

You can bind your configured VLANs to IP subnets. The NetScaler (if it is configured as the default router for the hosts on the subnets) then performs IP forwarding between these VLANs. A NetScaler supports the following types of VLANs.

Default VLAN
By default, the network interfaces on a NetScaler are included in a single, port-based VLAN as untagged network interfaces. This default VLAN has a VID of 1 and exists permanently. It cannot be deleted, and its VID cannot be changed.

Port-Based VLANs
A set of network interfaces that share a common, exclusive, Layer 2 broadcast domain define the membership of a port-based VLAN. You can configure multiple port-based VLANs. When you add an interface to a new VLAN as an untagged member, it is automatically removed from the default VLAN.

Tagged VLAN
A network interface can be a tagged or untagged member of a VLAN. Each network interface is an untagged member of only one VLAN (its native VLAN). The untagged network interface forwards the frames for the native VLAN as untagged frames. A tagged network interface can be a part of more than one VLAN. When you configure tagging, be sure that both ends of the link have matching VLAN settings. You can use the configuration utility to define a tagged VLAN (nsvlan) that can have any ports bound as tagged members of the VLAN. Configuring this VLAN requires a reboot of the NetScaler and therefore must be done during initial network configuration.

Link Aggregate Channels

Link aggregation combines incoming data from multiple ports into a single high speed link. Configuring the link aggregate channel increases the capacity and availability of the communication channel between a NetScaler and other connected devices. An aggregated link is also referred to as a channel.

When a network interface is bound to a channel, the channel parameters have precedence over the network interface parameters. A network interface can be bound to only one channel. Binding a network interface to a link aggregate channel changes the VLAN configuration. That is, binding network interfaces to a channel removes them from the VLANs that they originally belonged to and adds them to the default VLAN. However, you can bind the channel back to the old VLAN, or to a new one. For example, if you have bound network interfaces 1/2 and 1/3 to a VLAN with ID 2, and then you bind them to link aggregate channel LA/1, the network interfaces are moved to the default VLAN, but you can bind them to VLAN 2.

Note: You can also use Link Aggregation Control Protocol (LACP) to configure link aggregation. For more information, see "Configuring Link Aggregation by Using the Link Aggregation Control Protocol."

Configuring Clock Synchronization

You can configure your NetScaler appliance to synchronize its local clock with a Network Time Protocol (NTP) server. This ensures that its clock has the same date and time settings as the other servers on your network. NTP uses User Datagram Protocol (UDP) port 123 as its transport layer. You have to add NTP servers in the NTP configuration file so that the appliance periodically gets updates from these servers.

If you do not have a local NTP server, you can find a list of public, open access, NTP servers at the official NTP site at http://www.ntp.org.

To configure clock synchronization on your appliance

1. Log on to the command line and enter the `shell` command.
2. At the shell prompt, copy the `ntp.conf` file from the `/etc` directory to the `/nsconfig` directory. If the file already exists in the `/nsconfig` directory, make sure that you remove the following entries from the `ntp.conf` file:

   ```
   restrict localhost

   restrict 127.0.0.2
   ```

   These entries are required only if you want to run the device as a time server. However, this feature is not supported on the NetScaler.

3. Edit `/nsconfig/ntp.conf` by typing the IP address for the desired NTP server under the file's server and restrict entries.
4. Create a file named `rc.netscaler` in the `/nsconfig` directory, if the file does not already exist in the directory.
5. Edit `/nsconfig/rc.netscaler` by adding the following entry:

   ```
   /usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ntpd.log &
   ```

   This entry starts the ntpd service, checks the `ntp.conf` file, and logs messages in the `/var/log` directory.

   Note: If the time difference between the NetScaler and the time server is more than 1000 sec, the ntpd service terminates with a message to the NetScaler log. To avoid this, you need to start ntpd with the -g option, which forcibly syncs the time. Add the following entry in `/nsconfig/rc.netscaler`:

   ```
   /usr/sbin/ntpd -g -c /nsconfig/ntp.conf -l /var/log/ntpd.log
   &
   ```

   If you do not want to forcibly sync the time when there is a large difference, you can set the date manually and then start ntpd again. You can check the time difference between the appliance and the time server by running the following command in the shell:

   ```
   ntpdate -q <IP address or domain name of the NTP server>
   ```

6. Reboot the appliance to enable clock synchronization.

   Note: If you want to start time synchronization before you restart the appliance, enter the following command (which you added to the rc.netscaler file in step 5) at the shell prompt:

   ```
   /usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/
   ntpd.log &
   ```

Configuring DNS

You can configure a NetScaler appliance to function as an Authoritative Domain Name Server (ADNS), DNS proxy server, End Resolver, or Forwarder. You can add DNS resource records such as SRV Records, AAAA Records, A Records, MX Records, NS Records, CNAME Records, PTR Records, and SOA Records. Also, the appliance can balance the load on external DNS servers.

A common practice is to configure an appliance as a forwarder. For this configuration, you need to add external name servers. After you have added the external servers, you should verify that your configuration is correct.

You can add, remove, enable, and disable external name servers. You can create a name server by specifying its IP address, or you can configure an existing virtual server as the name server.

When adding name servers, you can specify IP addresses or virtual IP addresses (VIPs). If you use IP addresses, the appliance load balances requests to the configured name servers in a round robin manner. If you use VIPs, you can specify any load balancing method. For information about using a VIP, see "Load Balancing DNS Servers."

To add a name server by using the command line interface

At the command prompt, type the following commands to add a name server and verify the configuration:

- **add dns nameServer** `<IP>`
- **show dns nameServer** `<IP>`

Example

```
> add dns nameServer 10.102.29.10
 Done
> show dns nameServer 10.102.29.10
1)       10.102.29.10  -  State: DOWN
 Done
>
```

To add a name server by using the configuration utility

1. In the navigation pane, expand **DNS**, and then click **Name Servers**.
2. In the details pane, click **Add**.
3. In the **Create Name Server** dialog box, select **IP Address**.
4. In the **IP Address** text box, type the IP address of the name server (for example, `10.102.29.10`). If you are adding an external name server, clear the **Local** check box.
5. Click **Create**, and then click **Close**.
6. Verify that the name server you added appears in the **Name Servers** pane.

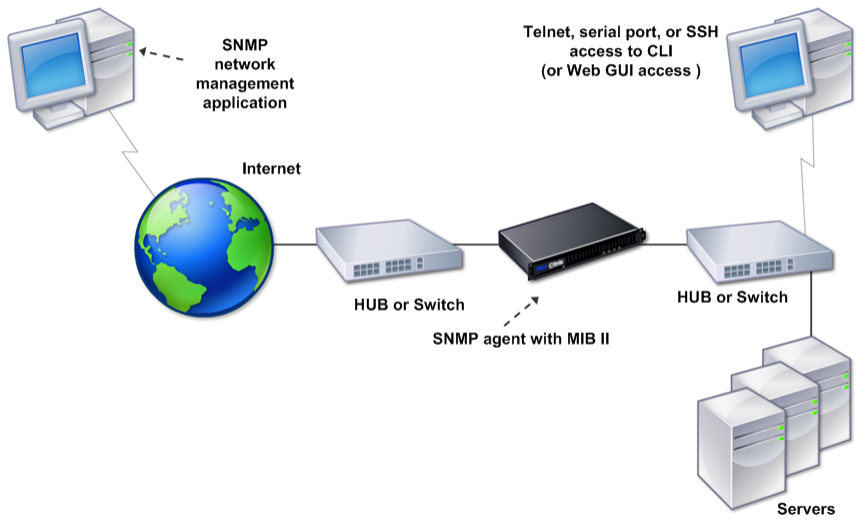
Configuring SNMP

The Simple Network Management Protocol (SNMP) network management application, running on an external computer, queries the SNMP agent on the NetScaler. The agent

searches the management information base (MIB) for data requested by the network management application and sends the data to the application.

SNMP monitoring uses traps messages and alarms. SNMP traps messages are asynchronous events that the agent generates to signal abnormal conditions, which are indicated by alarms. For example, if you want to be informed when CPU utilization is above 90 percent, you can set up an alarm for that condition. The following figure shows a network with a NetScaler that has SNMP enabled and configured.

Figure 3. SNMP on the NetScaler



The SNMP agent on a NetScaler supports SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2), and SNMP version 3 (SNMPv3). Because it operates in bilingual mode, the agent can handle SNMPv2 queries, such as Get-Bulk, and SNMPv1 queries. The SNMP agent also sends traps compliant with SNMPv2 and supports SNMPv2 data types, such as counter64. SNMPv1 managers (programs on other servers that request SNMP information from the NetScaler) use the NS-MIB-smiv1.mib file when processing SNMP queries. SNMPv2 managers use the NS-MIB-smiv2.mib file.

The NetScaler supports the following enterprise-specific MIBs:

A subset of standard MIB-2 groups
Provides MIB-2 groups SYSTEM, IF, ICMP, UDP, and SNMP.

A system enterprise MIB
Provides system-specific configuration and statistics.

To configure SNMP, you specify which managers can query the SNMP agent, add SNMP trap listeners that will receive the SNMP trap messages, and configure SNMP Alarms.

Adding SNMP Managers

You can configure a workstation running a management application that complies with SNMP version 1, 2, or 3 to access an appliance. Such a workstation is called an SNMP manager. If you do not specify an SNMP manager on the appliance, the appliance accepts and responds to SNMP queries from all IP addresses on the network. If you configure one or more SNMP managers, the appliance accepts and responds to SNMP queries from only those specific IP addresses. When specifying the IP address of an SNMP manager, you can use the netmask parameter to grant access from entire subnets. You can add a maximum of 100 SNMP managers or networks.

To add an SNMP manager by using the command line interface

At the command prompt, type the following commands to add an SNMP manager and verify the configuration:

- **add snmp manager** `<IPAddress> ... [-netmask <netmask>]`
- **show snmp manager** `<IPAddress>`

  Example

```
> add snmp manager 10.102.29.5 -netmask 255.255.255.255
 Done
> show snmp manager 10.102.29.5
1)      10.102.29.5         255.255.255.255
 Done
>
```

To add an SNMP manager by using the configuration utility

1. In the navigation pane, expand **System**, expand **SNMP**, and then click **Managers**.
2. In the details pane, click **Add**.
3. In the **Add SNMP Manager** dialog box, in the **IP Address** text box, type the IP address of the workstation running the management application (for example, `10.102.29.5`).
4. Click **Create**, and then click **Close**.
5. Verify that the SNMP manager you added appears in the **Details** section at the bottom of the pane.

Adding SNMP Traps Listeners

After configuring the alarms, you need to specify the trap listener to which the appliance will send the trap messages. Apart from specifying parameters like IP address

and the destination port of the trap listener, you can specify the type of trap (either generic or specific) and the SNMP version.

You can configure a maximum of 20 trap listeners for receiving either generic or specific traps.

To add an SNMP trap listener by using the command line interface

At the command prompt, type the following command to add an SNMP trap and verify that it has been added:

- **add snmp trap** `specific <IP>`
- **show snmp trap**

  Example

```
> add snmp trap specific 10.102.29.3
 Done
> show snmp trap
Type     DestinationIP   DestinationPort  Version
SourceIP      Min-Severity  Community
----     -------------   ---------------  -------
--------      ------------  ---------
generic  10.102.29.9     162              V2       NetScaler
IP  N/A           public
generic  10.102.29.5     162              V2       NetScaler
IP  N/A           public
generic  10.102.120.101  162              V2       NetScaler
IP  N/A           public
.
.
.
specific 10.102.29.3     162              V2       NetScaler
IP   -            public
 Done
>
```

To add an SNMP trap listener by using the configuration utility

1. In the navigation pane, expand **System**, expand **SNMP**, and then click **Traps**.
2. In the details pane, click **Add**.
3. In the **Create SNMP Trap Destination** dialog box, in the **Destination IP Address** text box, type the IP address (for example, `10.102.29.3`).
4. Click **Create** and then click **Close**.
5. Verify that the SNMP trap you added appears in the **Details** section at the bottom of the pane.

Configuring SNMP Alarms

You configure alarms so that the appliance generates a trap message when an event corresponding to one of the alarms occurs. Configuring an alarm consists of enabling the alarm and setting the severity level at which a trap is generated. There are five severity levels: Critical, Major, Minor, Warning, and Informational. A trap is sent only when the severity of the alarm matches the severity specified for the trap.

Some alarms are enabled by default. If you disable an SNMP alarm, the appliance will not generate trap messages when corresponding events occur. For example, if you disable the Login-Failure SNMP alarm, the appliance will not generate a trap message when a login failure occurs.

To enable or disable an alarm by using the command line interface

At the command prompt, type the following commands to enable or disable an alarm and verify that it has been enabled or disabled:

- **set snmp alarm** `<trapName> [-state ENABLED | DISABLED ]`
- **show snmp alarm** `<trapName>`

  Example

```
> set snmp alarm LOGIN-FAILURE -state ENABLED
 Done
> show snmp alarm LOGIN-FAILURE
   Alarm           Alarm Threshold  Normal Threshold  Time
State     Severity   Logging
   -----           ---------------  ----------------  ----
--------  ---------  --------
 1) LOGIN-FAILURE  N/A              N/A               N/A
ENABLED   -          ENABLED
 Done
>
```

To set the severity of the alarm by using the command line interface

At the command prompt, type the following commands to set the severity of the alarm and verify that the severity has been set correctly:

- **set snmp alarm** `<trapName> [-severity <severity>]`
- **show snmp alarm** `<trapName>`

  Example

```
> set snmp alarm LOGIN-FAILURE -severity Major
 Done
> show snmp alarm LOGIN-FAILURE
   Alarm           Alarm Threshold  Normal Threshold  Time
State     Severity   Logging
   -----           ---------------  ----------------  ----
--------  ---------  --------
```

```
 1) LOGIN-FAILURE  N/A              N/A               N/A
ENABLED   Major      ENABLED
 Done
>
```

To configure alarms by using the configuration utility

1. In the navigation pane, expand **System**, expand **SNMP**, and then click **Alarms**.
2. In the details pane, select an alarm (for example, **LOGIN-FAILURE**), and then click **Open**.
3. In the **Configure SNMP Alarm** dialog box, to enable the alarm, select the **Enable** check box. To disable the alarm, clear the **Enable** check box.
4. In the **Severity** drop-down list, select a severity option (for example, **Major**).
5. Click **OK**, and then click **Close**.
6. Verify that the parameters for the SNMP alarm you configured are correctly configured by viewing the **Details** section at the bottom of the pane.

Configuring Syslog

You can customize logging of NetScaler and Access Gateway Enterprise Edition access events for the needs of your site. You can direct these logs either to files on the NetScaler or to external log servers. The NetScaler uses the Audit Server Logging feature for logging the states and status information collected by different modules in the kernel and by user-level daemons.

Syslog is used to monitor a NetScaler and to log connections, statistics, and so on. You can customize the two logging functions for system events messaging and syslog. The NetScaler internal event message generator passes log entries to the syslog server. The syslog server accepts these log entries and logs them. For more information about the Audit Server Logging feature, see "Audit Logging."

Verifying the Configuration

After you finish configuring your system, complete the following checklists to verify your configuration.

Configuration Checklist

- The build running is:
- There are no incompatibility issues. (Incompatibility issues are documented in the build's release notes.)
- The port settings (speed, duplex, flow control, monitoring) are the same as the switch's port.
- Enough mapped IP addresses have been configured to support all server-side connections during peak times.

- The number of configured mapped IP addresses is: ____
- The expected number of simultaneous server connections is:

  [ ] 62,000 [ ] 124,000 [ ] Other____

Topology Configuration Checklist

- The routes have been used to resolve servers on other subnets.

  The routes entered are:

  _____

- If the NetScaler is in a public-private topology, reverse NAT has been configured.
- The failover (high availability) settings configured on the NetScaler resolve in a one arm or two-arm configuration. All unused network interfaces have been disabled:

  _____

- If the NetScaler is placed behind an external load balancer, then the load balancing policy on the external load balancer is not “least connection.”

  The load balancing policy configured on the external load balancer is:

  _____

- If the NetScaler is placed in front of a firewall, the session time-out on the firewall is set to a value greater than or equal to 300 seconds.

  Note: The TCP idle connection timeout on a NetScaler appliance is 360 seconds. If the timeout on the firewall is also set to 300 seconds or more, then the appliance can perform TCP connection multiplexing effectively because connections will not be closed earlier.

  The value configured for the session time-out is: _____

Server Configuration Checklist

- “Keep-alive” has been enabled on all the servers.

  The value configured for the keep-alive time-out is: _____

- The default gateway has been set to the correct value. (The default gateway should either be a NetScaler or upstream router.) The default gateway is:

  _____

- The server port settings (speed, duplex, flow control, monitoring) are the same as the switch port settings.

  _____

- If the Microsoft® Internet Information Server is used, buffering is enabled on the server.
- If an Apache Server is used, the MaxConn (maximum number of connections) parameter is configured on the server and on the NetScaler.

The MaxConn (maximum number of connections) value that has been set is:

_____

- If a Netscape® Enterprise Server™ is used, the maximum requests per connection parameter is set on the NetScaler. The maximum requests per connection value that has been set is:

  _____

Software Features Configuration Checklist

- Does the Layer 2 mode feature need to be disabled? (Disable if another Layer 2 device is working in parallel with a NetScaler.)

  Reason for enabling or disabling:

  _____

- Does the MAC-based forwarding feature need to be disabled? (If the MAC address used by return traffic is different, it should be disabled.)

  Reason for enabling or disabling:

  _____

- Does host-based reuse need to be disabled? (Is there virtual hosting on the servers?)

  Reason for enabling or disabling:

  _____

- Do the default settings of the surge protection feature need to be changed?

  Reason for changing or not changing:

  _____

Access Checklist

- The system IPs can be pinged from the client-side network.
- The system IPs can be pinged from the server-side network.
- The managed server(s) can be pinged through the NetScaler.
- Internet hosts can be pinged from the managed servers.
- The managed server(s) can be accessed through the browser.
- The Internet can be accessed from managed server(s) using the browser.
- The system can be accessed using SSH.
- Admin access to all managed server(s) is working.

Note: When you are using the ping utility, ensure that the pinged server has ICMP ECHO enabled, or your ping will not succeed.

Firewall Checklist

The following firewall requirements have been met:

- UDP 161 (SNMP)
- UDP 162 (SNMP trap)
- TCP/UDP 3010 (GUI)
- HTTP 80 (GUI)
- TCP 22 (SSH)

Load Balancing Traffic on a NetScaler Appliance

The load balancing feature distributes client requests across multiple servers to optimize resource utilization. In a real-world scenario with a limited number of servers providing service to a large number of clients, a server can become overloaded and degrade the performance of the server farm. A Citrix NetScaler appliance uses load balancing criteria to prevent bottlenecks by forwarding each client request to the server best suited to handle the request when it arrives.

To configure load balancing, you define a virtual server to proxy multiple servers in a server farm and balance the load among them.

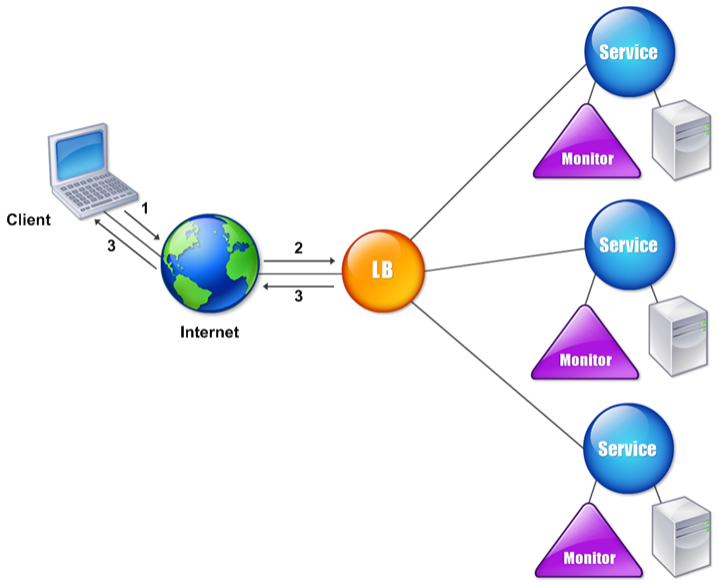
How Load Balancing Works

When a client initiates a connection to the server, a virtual server terminates the client connection and initiates a new connection with the selected server, or reuses an existing connection with the server, to perform load balancing. The load balancing feature provides traffic management from Layer 4 (TCP and UDP) through Layer 7 (FTP, HTTP, and HTTPS).

The NetScaler appliance uses a number of algorithms, called load balancing methods, to determine how to distribute the load among the servers. The default load balancing method is the Least Connections method.

A typical load balancing deployment consists of the entities described in the following figure.

Figure 1. Load Balancing Architecture



The entities function as follows:

- **Virtual server**. An entity that is represented by an IP address, a port, and a protocol. The virtual server IP address (VIP) is usually a public IP address. The client sends connection requests to this IP address. The virtual server represents a bank of servers.
- **Service**. A logical representation of a server or an application running on a server. Identifies the server's IP address, a port, and a protocol. The services are bound to the virtual servers.
- **Server object**. An entity that is represented by an IP address. The server object is created when you create a service. The IP address of the service is taken as the name of the server object. You can also create a server object and then create services by using the server object.
- **Monitor**. An entity that tracks the health of the services. The appliance periodically probes the servers using the monitor bound to each service. If a server does not respond within a specified response timeout, and the specified number of probes fails, the service is marked DOWN. The appliance then performs load balancing among the remaining services.

Configuring Load Balancing

To configure load balancing, you must first create services. Then, you create virtual servers and bind the services to the virtual servers. By default, the NetScaler appliance

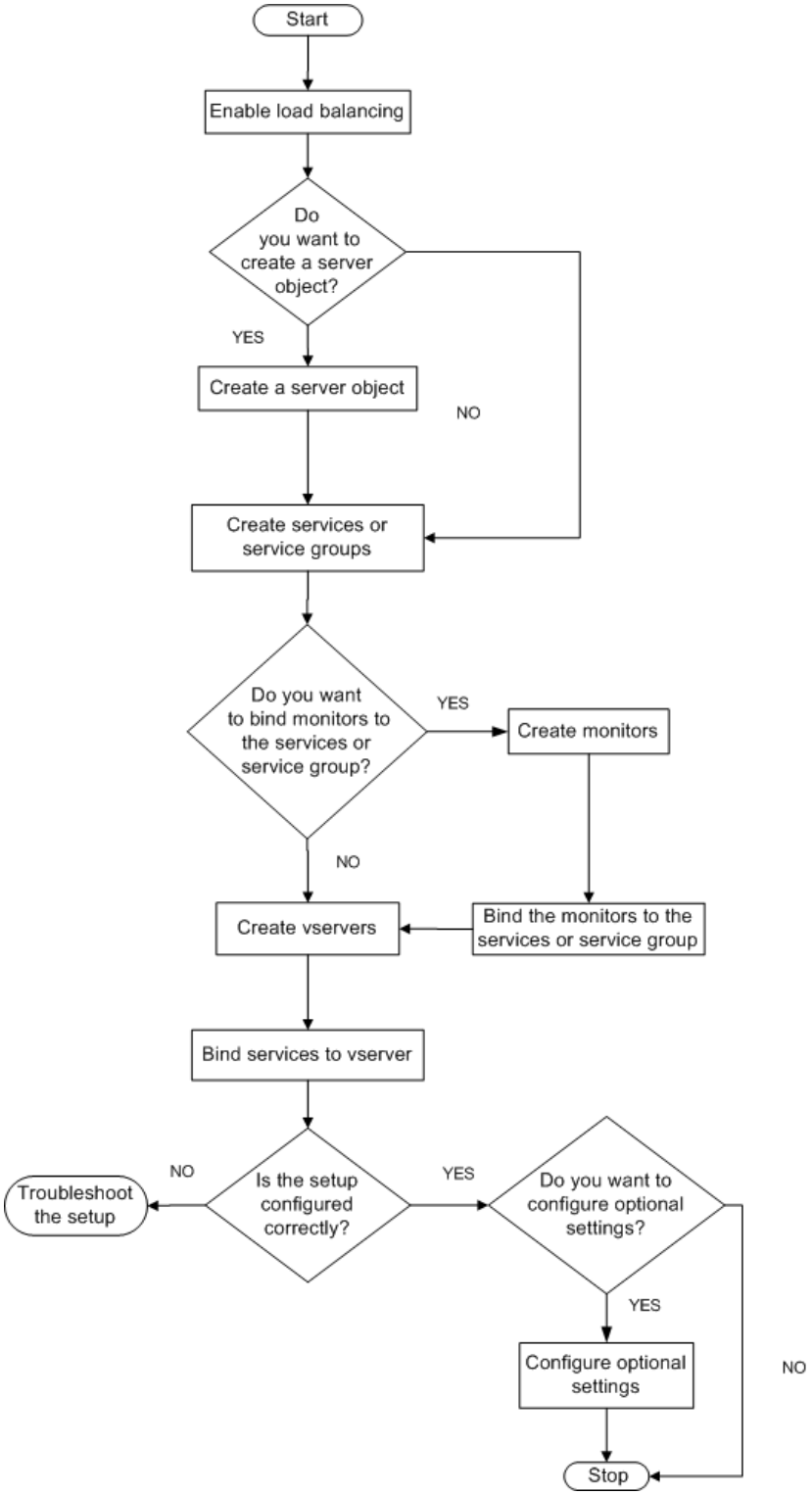
binds a monitor to each service. After binding the services, verify your configuration by making sure that all of the settings are correct.

Note: After you deploy the configuration, you can display statistics that show how the entities in the configuration are performing. Use the statistical utility or the **stat lb vserver** `<vserverName>` command.

Optionally, you can assign weights to a service. The load balancing method then uses the assigned weight to select a service. For getting started, however, you can limit optional tasks to configuring some basic persistence settings, for sessions that must maintain a connection to a particular server, and some basic configuration-protection settings.

The following flow chart illustrates the sequence of the configuration tasks.

Figure 2. Sequence of Tasks to Configure Load Balancing



Enabling Load Balancing

Before configuring load balancing, make sure that the load balancing feature is enabled.

To enable load balancing by using the command line interface

At the command prompt, type the following commands to enable load balancing and verify that it is enabled:

- **enable feature** `lb`
- **show feature**

  Example

```
> enable feature lb
 Done
> show feature

     Feature                  Acronym          Status
     -------                  -------          ------
 1)  Web Logging              WL               OFF
 2)  Surge Protection         SP               OFF
 3)  Load Balancing           LB               ON
 .
 .
 .
 9)  SSL Offloading           SSL              ON
 .
 .
 .
Done
```

To enable load balancing by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.
2. In the details pane, under **Modes and Features**, click **Change basic features**.
3. In the **Configure Basic Features** dialog box, select the **Load Balancing** check box, and then click **OK**.
4. In the **Enable/Disable Feature(s)?** message, click **Yes**.

Configuring Services and a Virtual Server

When you have identified the services you want to load balance, you can implement your initial load balancing configuration by creating the service objects, creating a load balancing virtual server, and binding the service objects to the virtual server.

To implement the initial load balancing configuration by using the command line interface

At the command prompt, type the following commands to implement and verify the initial configuration:

- **add service** <name> <IPaddress> <serviceType> <port>
- **add lb vserver** <vServerName> <serviceType> [<IPaddress> <port>]
- **bind lb vserver** <name> <serviceName>
- **show service bindings** <serviceName>

  Example

```
> add service service-HTTP-1 10.102.29.5 HTTP 80
 Done
> add lb vserver vserver-LB-1 HTTP 10.102.29.60 80
 Done
> bind lb vserver vserver-LB-1 service-HTTP-1
 Done
> show service bindings service-HTTP-1
   service-HTTP-1 (10.102.29.5:80) - State : DOWN

     1)      vserver-LB-1 (10.102.29.60:80) - State : DOWN
 Done
```

To implement the initial load balancing configuration by using the configuration utility

1. In the navigation pane, click **Load Balancing**.
2. In the details pane, under **Getting Started**, click **Load Balancing wizard**, and follow the instructions to create a basic load balancing setup.
3. Return to the navigation pane, expand **Load Balancing**, and then click **Virtual Servers**.
4. Select the virtual server that you configured and verify that the parameters displayed at the bottom of the page are correctly configured.
5. Click **Open**.
6. Verify that each service is bound to the virtual server by confirming that the **Active** check box is selected for each service on the **Services** tab.

Choosing and Configuring Persistence Settings

You must configure persistence on a virtual server if you want to maintain the states of connections on the servers represented by that virtual server (for example, connections used in e-commerce). The appliance then uses the configured load balancing method for the initial selection of a server, but forwards to that same server all subsequent requests from the same client.

If persistence is configured, it overrides the load balancing methods once the server has been selected. If the configured persistence applies to a service that is down, the appliance uses the load balancing methods to select a new service, and the new service becomes persistent for subsequent requests from the client. If the selected service is in an Out Of Service state, it continues to serve the outstanding requests but does not accept new requests or connections. After the shutdown period elapses, the existing connections are closed. The following table lists the types of persistence that you can configure.

Table 1. Limitations on Number of Simultaneous Persistent Connections

Persistence Type	Persistent Connections
Source IP, SSL Session ID, Rule, DESTIP, SRCIPDESTIP	250K
CookieInsert, URL passive, Custom Server ID	Memory limit. In case of CookieInsert, if time out is not 0, any number of connections is allowed until limited by memory.

If the configured persistence cannot be maintained because of a lack of resources on an appliance, the load balancing methods are used for server selection. Persistence is maintained for a configured period of time, depending on the persistence type. Some persistence types are specific to certain virtual servers. The following table shows the relationship.

Table 2. Persistence Types Available for Each Type of Virtual Server

Persistence TypeHeader 1	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge
Source IP	YES	YES	YES	YES	YES
CookieInsert	YES	YES	NO	NO	NO
SSL Session ID	NO	YES	NO	NO	YES
URL Passive	YES	YES	NO	NO	NO
Custom Server ID	YES	YES	NO	NO	NO
Rule	YES	YES	NO	NO	NO
SRCIPDESTIP	N/A	N/A	YES	YES	N/A
DESTIP	N/A	N/A	YES	YES	N/A

You can also specify persistence for a group of virtual servers. When you enable persistence on the group, the client requests are directed to the same selected server regardless of which virtual server in the group receives the client request. When the configured time for persistence elapses, any virtual server in the group can be selected for incoming client requests.

Two commonly used persistence types are persistence based on cookies and persistence based on server IDs in URLs. For more information about all persistence types, see "Persistence and Persistent Connections."

Configuring Persistence Based on Cookies

When you enable persistence based on cookies, the NetScaler adds an HTTP cookie into the Set-Cookie header field of the HTTP response. The cookie contains information about the service to which the HTTP requests must be sent. The client stores the cookie and includes it in all subsequent requests, and the NetScaler uses it to select the service for those requests. You can use this type of persistence on virtual servers of type HTTP or HTTPS.

The NetScaler inserts the cookie <NSC_XXXX>= <ServiceIP> <ServicePort>

where:

- <NSC_XXXX> is the virtual server ID that is derived from the virtual server name.
- <ServiceIP> is the hexadecimal value of the IP address of the service.
- <ServicePort> is the hexadecimal value of the port of the service.

The NetScaler encrypts ServiceIP and ServicePort when it inserts a cookie, and decrypts them when it receives a cookie.

Note: If the client is not allowed to store the HTTP cookie, the subsequent requests do not have the HTTP cookie, and persistence is not honored.

By default, the NetScaler sends HTTP cookie version 0, in compliance with the Netscape specification. It can also send version 1, in compliance with RFC 2109.

You can configure a timeout value for persistence that is based on HTTP cookies. Note the following:

- If HTTP cookie version 0 is used, the NetScaler inserts the absolute Coordinated Universal Time (GMT) of the cookie's expiration (the expires attribute of the HTTP cookie), calculated as the sum of the current GMT time on a NetScaler, and the timeout value.
- If an HTTP cookie version 1 is used, the NetScaler inserts a relative expiration time (Max-Age attribute of the HTTP cookie). In this case, the client software calculates the actual expiration time.

Note: Most client software currently installed (Microsoft Internet Explorer and Netscape browsers) understand HTTP cookie version 0; however, some HTTP proxies understand HTTP cookie version 1.

If you set the timeout value to 0, the NetScaler does not specify the expiration time, regardless of the HTTP cookie version used. The expiration time then depends on the

client software, and such cookies are not valid if that software is shut down. This persistence type does not consume any system resources. Therefore, it can accommodate an unlimited number of persistent clients.

An administrator can use the procedure in the following table to change the HTTP cookie version.

To change the HTTP cookie version by using the configuration utility

1. Navigate to **System** > **Settings**.
2. In the details pane, click **Change HTTP Parameters**.
3. In the **Configure HTTP Parameters** dialog box, under **Cookie**, select **Version 0** or **Version 1**.

Note: For information about the parameters, see "Configuring Persistence Based on Cookies."

To configure persistence based on cookies by using the command line interface

At the command prompt, type the following commands to configure persistence based on cookies and verify the configuration:

- **set lb vserver** <name> -persistenceType `COOKIEINSERT`
- **show lb vserver** <name>

  Example

```
> set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT
 Done
> show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    .
    .
    .
    Persistence: COOKIEINSERT (version 0)   Persistence
Timeout: 2 min
    .
    .
    .
 Done
>
```

To configure persistence based on cookies by using the configuration utility

1. In the navigation pane, expand **Load Balancing**, and then click **Virtual Servers**.
2. In the details pane, select the virtual server for which you want to configure persistence (for example, **vserver-LB-1**), and then click **Open**.

3. In the **Configure Virtual Server (Load Balancing)** dialog box, on the **Method and Persistence** tab, in the **Persistence** list, select **COOKIEINSERT**.
4. In the **Time-out (min)** text box, type the time-out value (for example, `2`).
5. Click **OK**.
6. Verify that the virtual server for which you configured persistence is correctly configured by selecting the virtual server and viewing the **Details** section at the bottom of the pane.

Configuring Persistence Based on Server IDs in URLs

The NetScaler can maintain persistence based on the server IDs in the URLs. In a technique called URL passive persistence, the NetScaler extracts the server ID from the server response and embeds it in the URL query of the client request. The server ID is an IP address and port specified as a hexadecimal number. The NetScaler extracts the server ID from subsequent client requests and uses it to select the server.

URL passive persistence requires configuring either a payload expression or a policy infrastructure expression specifying the location of the server ID in the client requests. For more information about expressions, see "Policy Configuration and Reference."

Note: If the server ID cannot be extracted from the client requests, server selection is based on the load balancing method.

Example: Payload Expression

The expression, URLQUERY contains sid= configures the system to extract the server ID from the URL query of a client request, after matching token sid=. Thus, a request with the URL http://www.citrix.com/index.asp?&sid;=c0a864100050 is directed to the server with the IP address10.102.29.10 and port 80.

The timeout value does not affect this type of persistence, which is maintained as long as the server ID can be extracted from the client requests. This persistence type does not consume any system resources, so it can accommodate an unlimited number of persistent clients.

Note: For information about the parameters, see "Load Balancing."

To configure persistence based on server IDs in URLs by using the command line interface

At the command prompt, type the following commands to configure persistence based on server IDs in URLs and verify the configuration:

- **set lb vserver** `<name> -persistenceType URLPASSIVE`
- **show lb vserver** `<name>`

  Example

```
> set lb vserver vserver-LB-1 -persistenceType URLPASSIVE
 Done
> show lb vserver vserver-LB-1
```

```
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    .
    .
    .
    Persistence: URLPASSIVE Persistence Timeout: 2 min
    .
    .
    .
 Done
>
```

To configure persistence based on server IDs in URLs by using the configuration utility

1. In the navigation pane, expand **Load Balancing**, and then click **Virtual Servers**.
2. In the details pane, select the virtual server for which you want to configure persistence (for example, **vserver-LB-1**), and then click **Open**.
3. In the **Configure Virtual Server (Load Balancing)** dialog box, on the **Method and Persistence** tab, in the **Persistence** list, select **URLPASSIVE**.
4. In the **Time-out (min)** text box, type the time-out value (for example, `2`).
5. In the **Rule** text box, enter a valid expression. Alternatively, click **Configure** next to the **Rule** text box and use the **Create Expression** dialog box to create an expression.
6. Click **OK**.
7. Verify that the virtual server for which you configured persistence is correctly configured by selecting the virtual server and viewing the **Details** section at the bottom of the pane.

Configuring Features to Protect the Load Balancing Configuration

You can configure URL redirection to provide notifications of virtual server malfunctions, and you can configure backup virtual servers to take over if a primary virtual server becomes unavailable.

Configuring URL Redirection

You can configure a redirect URL to communicate the status of the appliance in the event that a virtual server of type HTTP or HTTPS is down or disabled. This URL can be a local or remote link. The appliance uses HTTP 302 redirect.

Redirects can be absolute URLs or relative URLs. If the configured redirect URL contains an absolute URL, the HTTP redirect is sent to the configured location, regardless of the URL specified in the incoming HTTP request. If the configured redirect URL contains only the domain name (relative URL), the HTTP redirect is sent to a location after appending the incoming URL to the domain configured in the redirect URL.

Note: If a load balancing virtual server is configured with both a backup virtual server and a redirect URL, the backup virtual server takes precedence over the redirect URL. In this case, a redirect is used when both the primary and backup virtual servers are down.

To configure a virtual server to redirect client requests to a URL by using the command line interface

At the command prompt, type the following commands to configure a virtual server to redirect client requests to a URL and verify the configuration:

- **set lb vserver** <name> -redirectURL <URL>
- **show lb vserver** <name>

  Example

```
> set lb vserver vserver-LB-1 -redirectURL http://
www.newdomain.com/mysite/maintenance
 Done
> show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    State: DOWN
    Last state change was at Wed Jun 17 08:56:34 2009 (+666
ms)
    .
    .
    .
    Redirect URL: http://www.newdomain.com/mysite/maintenance
    .
    .
    .
 Done
>
```

To configure a virtual server to redirect client requests to a URL by using the configuration utility

1. In the navigation pane, expand **Load Balancing**, and then click **Virtual Servers**.
2. In the details pane, select the virtual server for which you want to configure URL redirection (for example, **vserver-LB-1**), and then click **Open**.
3. In the **Configure Virtual Server (Load Balancing)** dialog box, on the **Advanced** tab, in the **Redirect URL** text box, type the URL (for example, `http://www.newdomain.com/mysite/maintenance`), and then click **OK**.
4. Verify that the redirect URL you configured for the server appears in the **Details** section at the bottom of the pane.

Configuring Backup Virtual Servers

If the primary virtual server is down or disabled, the appliance can direct the connections or client requests to a backup virtual server that forwards the client traffic

to the services. The appliance can also send a notification message to the client regarding the site outage or maintenance. The backup virtual server is a proxy and is transparent to the client.

You can configure a backup virtual server when you create a virtual server or when you change the optional parameters of an existing virtual server. You can also configure a backup virtual server for an existing backup virtual server, thus creating a cascaded backup virtual server. The maximum depth of cascading backup virtual servers is 10. The appliance searches for a backup virtual server that is up and accesses that virtual server to deliver the content.

You can configure URL redirection on the primary for use when the primary and the backup virtual servers are down or have reached their thresholds for handling requests.

Note: If no backup virtual server exists, an error message appears, unless the virtual server is configured with a redirect URL. If both a backup virtual server and a redirect URL are configured, the backup virtual server takes precedence.

To configure a backup virtual server by using the command line interface

At the command prompt, type the following commands to configure a backup server and verify the configuration:

- **set lb vserver** <name> [-backupVserver <string>]
- **show lb vserver** <name>

  Example

```
> set lb vserver vserver-LB-1 -backupVserver vserver-LB-2
 Done
> show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    State: DOWN
    Last state change was at Wed Jun 17 08:56:34 2009 (+661
ms)
    .
    .
    .
    Backup: vserver-LB-2
    .
    .
    .
 Done
>
```

To set up a backup virtual server by using the configuration utility

1. In the navigation pane, expand **Load Balancing**, and then click **Virtual Servers**.
2. In the details pane, select the virtual server for which you want to configure the backup virtual server (for example, **vserver-LB-1**), and then click **Open**.

3. In the **Configure Virtual Server (Load Balancing)** dialog box, on the **Advanced** tab, in the **Backup Virtual Server** list, select the backup virtual server (for example, **vserver-LB-2**, and then click **OK**.
4. Verify that the backup virtual server you configured appears in the **Details** section at the bottom of the pane.

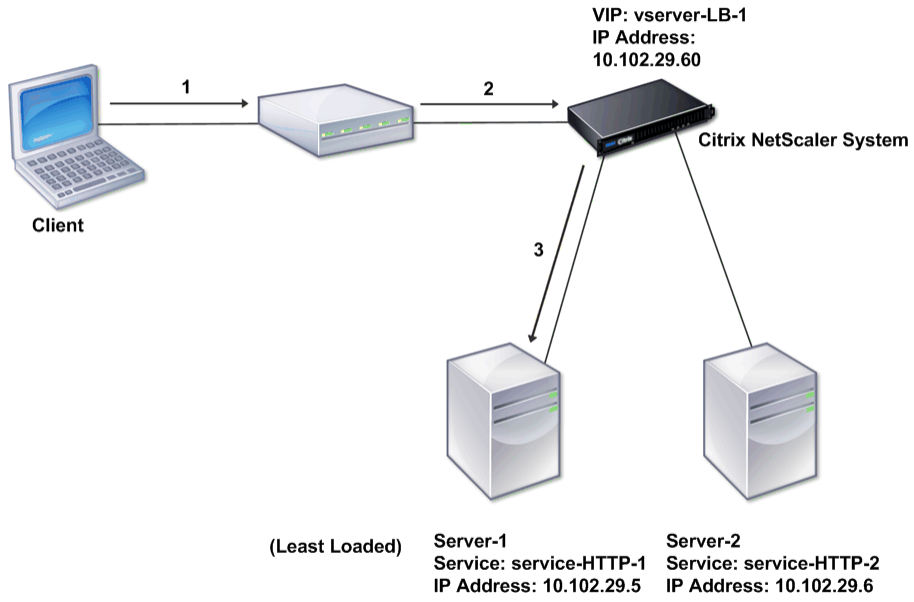
Note: If the primary server goes down and then comes back up, and you want the backup virtual server to function as the primary server until you explicitly reestablish the primary virtual server, select the **Disable Primary When Down** check box.

A Typical Load Balancing Scenario

In a load balancing setup, the NetScaler appliances are logically located between the client and the server farm, and they manage traffic flow to the servers.

The following figure shows the topology of a basic load balancing configuration.

Figure 3. Basic Load Balancing Topology



The virtual server selects the service and assigns it to serve client requests. Consider the scenario in the preceding figure, where the services service-HTTP-1 and service-HTTP-2 are created and bound to the virtual server named virtual server-LB-1. Virtual server-LB-1 forwards the client request to either service-HTTP-1 or service-HTTP-2. The system selects the service for each request by using the Least Connections load

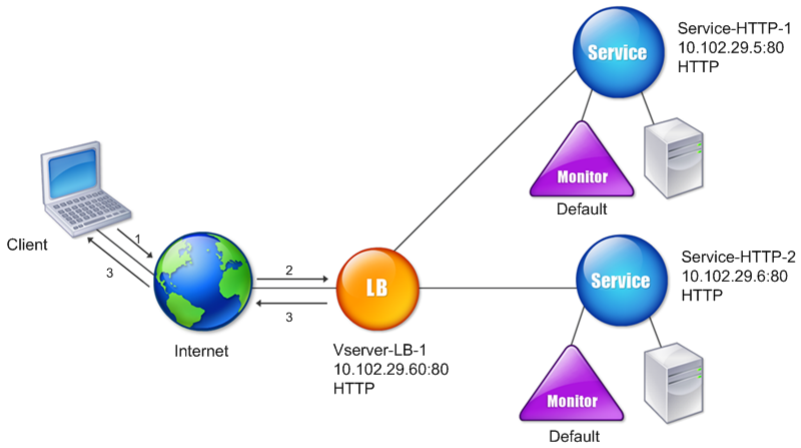
balancing method. The following table lists the names and values of the basic entities that must be configured on the system.

Table 3. LB Configuration Parameter Values

Entity Type	Required parameters and sample values			
	Name	IP Address	Port	Protocol
Virtual Server	vserver-LB-1	10.102.29.60	80	HTTP
Services	service-HTTP-1	10.102.29.5	8083	HTTP
	service-HTTP-2	10.102.29.6	80	HTTP
Monitors	Default	None	None	None

The following figure shows the load balancing sample values and required parameters that are described in the preceding table.

Figure 4. Load Balancing Entity Model



The following tables list the commands used to configure this load balancing setup by using the command line interface.

Table 4. Initial Configuration Tasks

Task	Command
To enable load balancing	enable feature lb
To create a service named service-HTTP-1	add service service-HTTP-1 10.102.29.5 HTTP 80
To create a service named service-HTTP-2	add service service-HTTP-2 10.102.29.6 HTTP 80
To create a virtual server named vserver-LB-1	add lb vserver vserver-LB-1 HTTP 10.102.29.60 80
To bind a service named service-HTTP-1 to a virtual server named vserver-LB-1	bind lb vserver vserver-LB-1 service-HTTP-1
To bind a service named service-HTTP-2 to a virtual server named vserver-LB-1	bind lb vserver vserver-LB-1 service-HTTP-2

For more information about the initial configuration tasks, see "Enabling Load Balancing" and "Configuring Services and a Vserver."

Table 5. Verification Tasks

Task	Command
To view the properties of a virtual server named vserver-LB-1	show lb vserver vserver-LB-1
To view the statistics of a virtual server named vserver-LB-1	stat lb vserver vserver-LB-1
To view the properties of a service named service-HTTP-1	show service service-HTTP-1
To view the statistics of a service named service-HTTP-1	stat service service-HTTP-1
To view the bindings of a service named service-HTTP-1	show service bindings service-HTTP-1

Table 6. Customization Tasks

Task	Command
To configure persistence on a virtual server named vserver-LB-1	set lb vserver vserver-LB-1 -persistenceType SOURCEIP -persistenceMask 255.255.255.255 -timeout 2
To configure COOKIEINSERT persistence on a virtual server named vserver-LB-1	set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT
To configure URLPassive persistence on a virtual server named vserver-LB-1	set lb vserver vserver-LB-1 -persistenceType URLPASSIVE
To configure a virtual server to redirect the client request to a URL on a virtual server named vserver-LB-1	set lb vserver vserver-LB-1 -redirectURL http://www.newdomain.com/mysite/maintenance
To set a backup virtual server on a virtual server named vserver-LB-1	set lb vserver vserver-LB-1 -backupVserver vserver-LB-2

For more information about configuring persistence, see "Choosing and Configuring Persistence Settings." For information about configuring a virtual server to redirect a client request to a URL and setting up a backup virtual server, see "Configuring Features to Protect the Load Balancing Configuration."

Accelerating Load Balanced Traffic by Using Compression

Compression is a popular means of optimizing bandwidth usage, and most web browsers support compressed data. If you enable the compression feature, the NetScaler appliance intercepts requests from clients and determines whether the client can accept compressed content. After receiving the HTTP response from the server, the appliance examines the content to determine whether it is compressible. If the content is compressible, the appliance compresses it, modifies the response header to indicate the type of compression performed, and forwards the compressed content to the client.

NetScaler compression is a policy-based feature. A policy filters requests and responses to identify responses to be compressed, and specifies the type of compression to apply to each response. The appliance provides several built-in policies to compress common MIME types such as text/html, text/plain, text/xml, text/css, text/rtf, application/msword, application/vnd.ms-excel, and application/vnd.ms-powerpoint. You can also create custom policies. The appliance does not compress compressed MIME types such as application/octet-stream, binary, bytes, and compressed image formats such as GIF and JPEG.

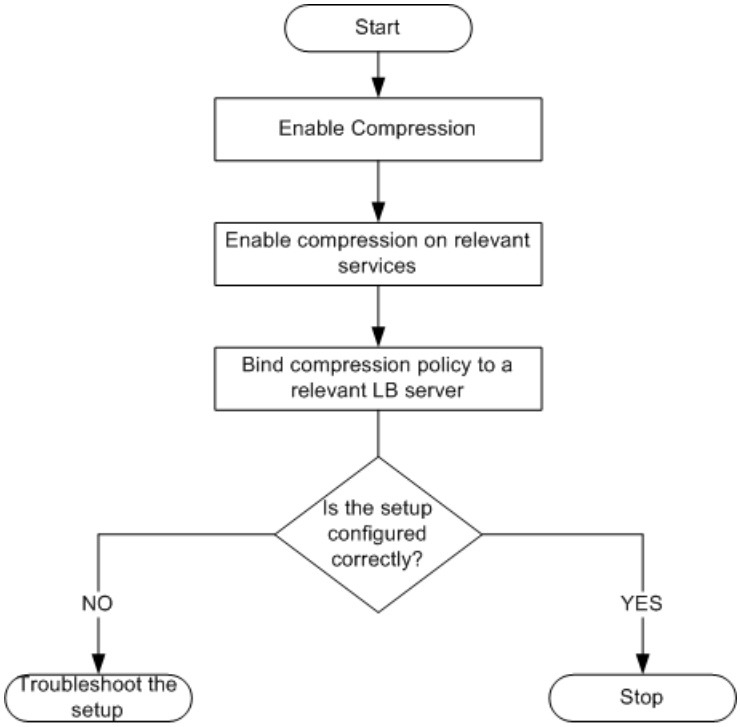
To configure compression, you must enable it globally and on each service that will provide responses that you want compressed. If you have configured virtual servers for load balancing or content switching, you should bind the polices to the virtual servers. Otherwise, the policies apply to all traffic that passes through the appliance.

Note: For more information about compression, see "Compression."

Compression Configuration Task Sequence

The following flow chart shows the sequence of tasks for configuring basic compression in a load balancing setup.

Figure 1. Sequence of Tasks to Configure Compression



Note: The steps in the above figure assume that load balancing has already been configured. For information about configuring load balancing, or for more information about services, see "Load Balancing."

If you want to configure something other than a basic compression setup, (for example, if you need to configure optional parameters in addition to the required parameters) see "Compression."

Enabling Compression

By default, compression is not enabled. You must enable the compression feature to allow compression of HTTP responses that are sent to the client.

To enable compression by using the command line interface

At the command prompt, type the following commands to enable compression and verify the configuration:

- **enable ns feature** `CMP`
- **show ns feature**

Example

```
> enable ns feature CMP
Done
> show ns feature

        Feature                         Acronym
Status
        -------                         -------
------
1)      Web Logging                     WL                      ON
2)      Surge Protection                SP
OFF
.
7)      Compression Control             CMP                     ON
8)      Priority Queuing                PQ
OFF
.
Done
```

To enable compression by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.
2. In the details pane, under **Modes and Features**, click **Change basic features**.
3. In the **Configure Basic Features** dialog box, select the **Compression** check box, and then click **OK**.
4. In the **Enable/Disable Feature(s)?** dialog box, click **Yes**.

Configuring Services to Compress Data

In addition to enabling compression globally, you must enable it on each service that will deliver files to be compressed. To create a service, see "Configuring Services."

To enable compression on a service by using the command line

At the command prompt, type the following commands to enable compression on a service and verify the configuration:

- **set service** <name> -CMP YES
- **show service** <name>

  Example

```
> show service SVC_HTTP1
```

```
SVC_HTTP1 (10.102.29.18:80) - HTTP
State: UP
Last state change was at Tue Jun 16 06:19:14 2009 (+737 ms)
Time since last state change: 0 days, 03:03:37.200
Server Name: 10.102.29.18
Server ID : 0   Monitor Threshold : 0
Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
Use Source IP: NO
Client Keepalive(CKA): NO
Access Down Service: NO
TCP Buffering(TCPB): NO
HTTP Compression(CMP): YES
Idle timeout: Client: 180 sec   Server: 360 sec
Client IP: DISABLED
Cacheable: NO
SC: OFF
SP: OFF
Down state flush: ENABLED

1)      Monitor Name: tcp-default
State: DOWN     Weight: 1
Probes: 1095    Failed [Total: 1095 Current: 1095]
Last response: Failure - TCP syn sent, reset received.
Response Time: N/A
Done
```

To enable compression on a service by using the configuration utility

1. In the navigation pane, expand **Load Balancing**, and then click **Services**.
2. In the details pane, select the service for which you want to configure compression (for example, **service-HTTP-1**), and then click **Open**.
3. On the **Advanced** tab, under **Settings**, select the **Compression** check box, and then click **OK.**
4. Verify that, when the service is selected, `HTTP Compression(CMP): ON` appears in the **Details** section at the bottom of the pane.

Binding a Compression Policy to a Virtual Server

If you bind a policy to a virtual server, the policy is evaluated only by the services associated with that virtual server. You can bind compression policies to a virtual server either from the **Configure Virtual Server (Load Balancing)** dialog box or from the **Compression Policy Manager** dialog box. This topic includes instructions to bind compression policies to a load balancing virtual server by using the **Configure Virtual Server (Load Balancing)** dialog box. For information about how you can bind a

compression policy to a load balancing virtual server by using the **Compression Policy Manager** dialog box, see "Configuring and Binding Policies with the Policy Manager."

To bind or unbind a compression policy to a virtual server by using the command line

At the command prompt, type the following commands to bind or unbind a compression policy to a load balancing virtual server and verify the configuration:

- **(bind|unbind) lb vserver** `<name> -policyName <string>`
- **show lb vserver** `<name>`

  Example

```
> bind lb vserver lbvip -policyName ns_cmp_msapp
Done
> show lb vserver lbvip
lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
State: UP
Last state change was at Thu May 28 05:37:21 2009 (+685 ms)
Time since last state change: 19 days, 04:26:50.470
Effective State: UP
Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
Port Rewrite : DISABLED
No. of Bound Services :  1 (Total)       1 (Active)
Configured Method: LEASTCONNECTION
Current Method: Round Robin, Reason: Bound service's state
changed to UP
Mode: IP
Persistence: NONE
Vserver IP and Port insertion: OFF
Push: DISABLED  Push VServer:
Push Multi Clients: NO
Push Label Rule:

Bound Service Groups:
1)      Group Name: Service-Group-1

1) Service-Group-1 (10.102.29.252: 80) - HTTP State: UP
Weight:                                                  1

1)      Policy : ns_cmp_msapp Priority:0
Done
```

To bind or unbind a compression policy to a load balancing virtual server by using the configuration utility

1. In the navigation pane, expand **Load Balancing**, and then click **Virtual Servers**.
2. In the details pane, select the virtual server to which you want to bind or unbind a compression policy (for example, **Vserver-LB-1**), and then click **Open**.
3. In the **Configure Virtual Server (Load Balancing)** dialog box, on the **Policies** tab, click **Compression**.
4. Do one of the following:
   - To bind a compression policy, click **Insert Policy**, and then select the policy you want to bind to the virtual server.
   - To unbind a compression policy, click the name of the policy you want to unbind from the virtual server, and then click **Unbind Policy**.
5. Click **OK.**

Securing Load Balanced Traffic by Using SSL

The Citrix NetScaler SSL offload feature transparently improves the performance of web sites that conduct SSL transactions. By offloading CPU-intensive SSL encryption and decryption tasks from the local web server to the appliance, SSL offloading ensures secure delivery of web applications without the performance penalty incurred when the server processes the SSL data. Once the SSL traffic is decrypted, it can be processed by all standard services. The SSL protocol works seamlessly with various types of HTTP and TCP data and provides a secure channel for transactions using such data.

To configure SSL, you must first enable it. Then, you configure HTTP or TCP services and an SSL virtual server on the appliance, and bind the services to the virtual server. You must also add a certificate-key pair and bind it to the SSL virtual server. If you use Outlook Web Access servers, you must create an action to enable SSL support and a policy to apply the action. An SSL virtual server intercepts incoming encrypted traffic and decrypts it by using a negotiated algorithm. The SSL virtual server then forwards the decrypted data to the other entities on the appliance for appropriate processing.

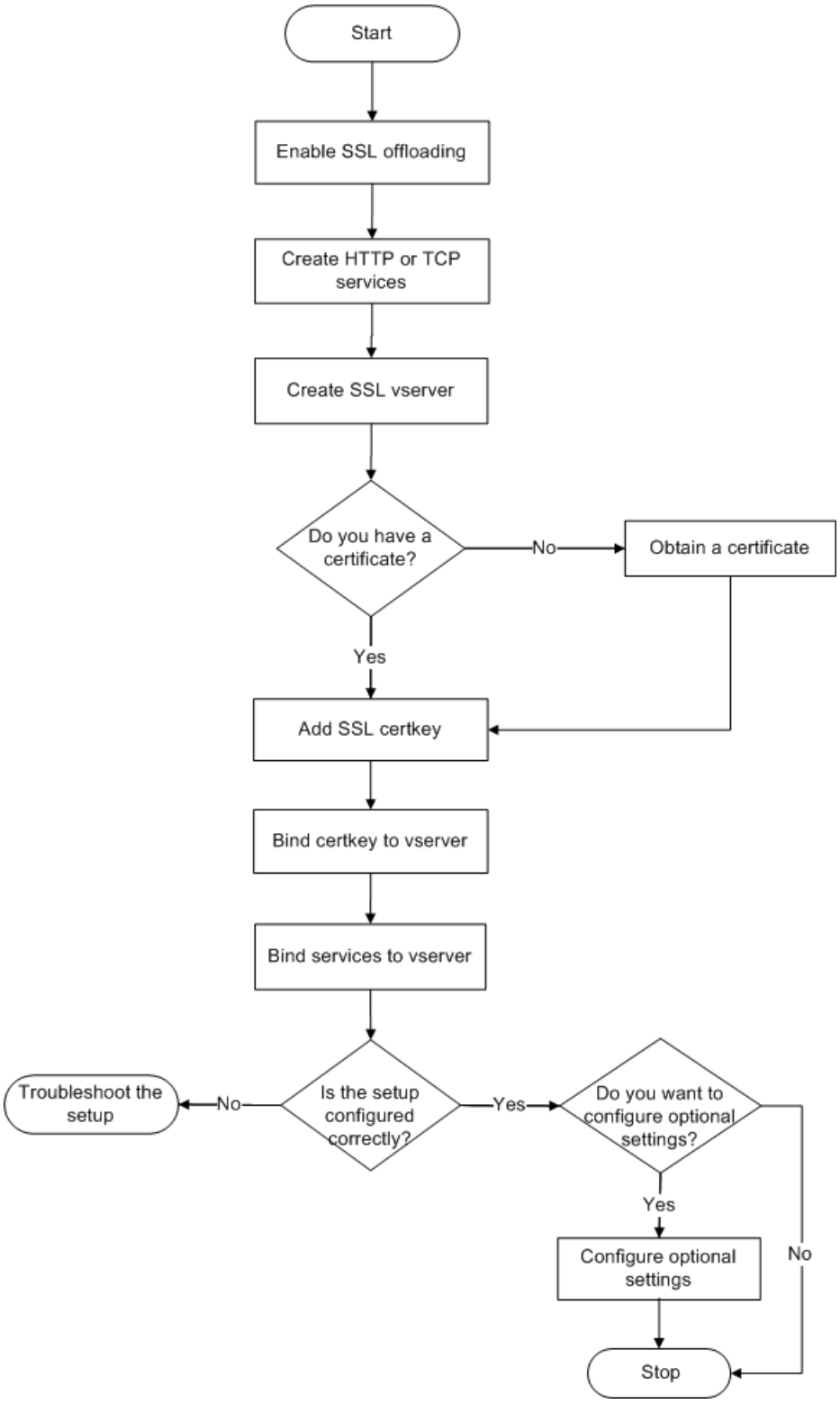
SSL Configuration Task Sequence

To configure SSL, you must first enable it. Then, you must create an SSL virtual server and HTTP or TCP services on the NetScaler. Finally, you must bind a valid SSL certificate and the configured services to the SSL virtual server.

An SSL virtual server intercepts incoming encrypted traffic and decrypts it using a negotiated algorithm. The SSL virtual server then forwards the decrypted data to the other entities on the NetScaler for appropriate processing.

The following flow chart shows the sequence of tasks for configuring a basic SSL offload setup.

Figure 1. Sequence of Tasks to Configure SSL Offloading



Enabling SSL Offload

You should enable the SSL feature before configuring SSL offload. You can configure SSL-based entities on the appliance without enabling the SSL feature, but they will not work until you enable SSL.

To enable SSL by using the command line interface

At the command prompt, type the following commands to enable SSL Offload and verify the configuration:

- **enable ns feature** `SSL`
- **show ns feature**

  Example

```
> enable ns feature ssl
Done
> show ns feature
Feature Acronym Status
------- ------- ------
1) Web Logging WL ON
2) SurgeProtection SP OFF
3) Load Balancing LB ON . . .
 9) SSL Offloading SSL ON
10) Global Server Load Balancing GSLB ON . .
Done >
```

To enable SSL by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.
2. In the details pane, under **Modes and Features**, click **Change basic features**.
3. Select the **SSL Offloading** check box, and then click **OK**.
4. In the **Enable/Disable Feature(s)?** message box, click **Yes**.

Creating HTTP Services

A service on the appliance represents an application on a server. Once configured, services are in the disabled state until the appliance can reach the server on the network and monitor its status. This topic covers the steps to create an HTTP service.

Note: For TCP traffic, perform the procedures in this and the following topics, but create TCP services instead of HTTP services.

To add an HTTP service by using the command line interface

At the command prompt, type the following commands to add a HTTP service and verify the configuration:

- **add service** `<name> (<IP> | <serverName>) <serviceType> <port>`
- **show service** `<name>`

```
> add service SVC_HTTP1 10.102.29.18 HTTP 80
 Done
> show service SVC_HTTP1
        SVC_HTTP1 (10.102.29.18:80) - HTTP
        State: UP
        Last state change was at Wed Jul 15 06:13:05 2009
        Time since last state change: 0 days, 00:00:15.350
        Server Name: 10.102.29.18
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0
kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): YES
        Idle timeout: Client: 180 sec   Server: 360 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: tcp-default
                State: UP       Weight: 1
                Probes: 4       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack
received.
                Response Time: N/A
 Done
```

To add an HTTP service by using the configuration utility

1. In the navigation pane, expand **SSL Offload**, and then click **Services**.
2. In details pane, click **Add**.

3. In the **Create Service** dialog box, in the **Service Name**, **Server**, and **Port** text boxes, type the name of the service, IP address, and port (for example, `SVC_HTTP1`, `10.102.29.18`, and `80`).
4. In the **Protocol** list, select the type of the service (for example, `HTTP`).
5. Click **Create**, and then click **Close**.
   The HTTP service you configured appears in the **Services** page.
6. Verify that the parameters you configured are correctly configured by selecting the service and viewing the **Details** section at the bottom of the pane.

For more information about services, see "Configuring Services."

Adding an SSL-Based Virtual Server

In a basic SSL offloading setup, the SSL virtual server intercepts encrypted traffic, decrypts it, and sends the clear text messages to the services that are bound to the virtual server. Offloading CPU-intensive SSL processing to the appliance allows the back-end servers to process a greater number of requests.

To add an SSL-based virtual server by using the command line interface

At the command prompt, type the following commands to create an SSL-based virtual server and verify the configuration:

- **add lb vserver** `<name> <serviceType> [<IPAddress> <port>]`
- **show lb vserver** `<name>`

  Example

```
  > add lb vserver vserver-SSL-1 SSL 10.102.29.50 443
  Done
  > show lb vserver vserver-SSL-1
  vserver-SSL-1 (10.102.29.50:443) - SSL Type: ADDRESS
  State: DOWN[Certkey not bound] Last state change was at
Tue Jun 16 06:33:08 2009 (+176 ms)
  Time since last state change: 0 days, 00:03:44.120
  Effective State: DOWN Client Idle Timeout: 180 sec
  Down state flush: ENABLED
  Disable Primary Vserver On Down : DISABLED
  No. of Bound Services : 0 (Total) 0 (Active)
  Configured Method: LEASTCONNECTION Mode: IP
  Persistence: NONE
  Vserver IP and Port insertion: OFF
  Push: DISABLED Push VServer: Push Multi Clients: NO Push
Label Rule: Done
```

⚠ **Caution:** To ensure secure connections, you must bind a valid SSL certificate to the SSL-based virtual server before you enable it.

To add an SSL-based virtual server by using the configuration utility

1. In the navigation pane, expand **SSL Offload**, and then click **Virtual Servers**.
2. In the details pane, click **Add**.
3. In the **Create Virtual Server (SSL Offload)** dialog box, in the **Name**, **IP Address**, and **Port** text boxes, type the name of the virtual server, IP address, and port (for example, `Vserver-SSL-1`, `10.102.29.50`, and `443`).
4. In the **Protocol** list, select the type of the virtual server, for example, **SSL.**
5. Click **Create**, and then click **Close**.
6. Verify that the parameters you configured are correctly configured by selecting the virtual server and viewing the **Details** section at the bottom of the pane. The virtual server is marked as DOWN because a certificate-key pair and services have not been bound to it.

⚠ **Caution:** To ensure secure connections, you must bind a valid SSL certificate to the SSL-based virtual server before you enable it.

Binding Services to the SSL Virtual Server

After decrypting the incoming data, the SSL virtual server forwards the data to the services that you have bound to the virtual server.

Data transfer between the appliance and the servers can be encrypted or in clear text. If the data transfer between the appliance and the servers is encrypted, the entire transaction is secure from end to end. For more information about configuring the system for end-to-end security, see "SSL Offload and Acceleration."

To bind a service to a virtual server by using the command line interface

At the command prompt, type the following commands to bind service to the SSL virtual server and verify the configuration:

- **bind lb vserver** `<name> <serviceName>`
- **show lb vserver** `<name>`

Example

```
  > bind lb vserver vserver-SSL-1 SVC_HTTP1
  Done
  > show lb vserver vserver-SSL-1 vserver-SSL-1
(10.102.29.50:443) - SSL Type:
  ADDRESS State: DOWN[Certkey not bound]
  Last state change was at Tue Jun 16 06:33:08 2009 (+174
ms)
  Time since last state change: 0 days, 00:31:53.70
  Effective State: DOWN Client Idle
  Timeout: 180 sec
  Down state flush: ENABLED Disable Primary Vserver On Down :
  DISABLED No. of Bound Services : 1 (Total) 0 (Active)
  Configured Method: LEASTCONNECTION Mode: IP Persistence:
NONE Vserver IP and
  Port insertion: OFF Push: DISABLED Push VServer: Push
Multi Clients: NO Push Label Rule:

  1) SVC_HTTP1 (10.102.29.18: 80) - HTTP
  State: DOWN Weight: 1
  Done
```

To bind a service to a virtual server by using the configuration utility

1. In the navigation pane, expand **SSL Offload**, and then click **Virtual Servers**.
2. In the details pane, select a virtual server, and then click **Open**.
3. On the **Services** tab, in the **Active** column, select the check boxes next to the services that you want to bind to the selected virtual server.
4. Click **OK.**
5. Verify that the **Number of Bound Services** counter in the **Details** section at the bottom of the pane is incremented by the number of services that you bound to the virtual server.

Adding a Certificate Key Pair

An SSL certificate is an integral element of the SSL Key-Exchange and encryption/decryption process. The certificate is used during SSL handshake to establish the identity of the SSL server. You can use a valid, existing SSL certificate that you have on the NetScaler appliance, or you can create your own SSL certificate. The appliance supports RSA/DSA certificates of up to 4096 bits.

Note: Citrix recommends that you use a valid SSL certificate that has been issued by a trusted certificate authority. Invalid certificates and self-created certificates are not compatible with all SSL clients.

Before a certificate can be used for SSL processing, you must pair it with its corresponding key. The certificate key pair is then bound to the virtual server and used for SSL processing.

To add a certificate key pair by using the command line interface

At the command prompt, type the following commands to create a certificate key pair and verify the configuration:

- **add ssl certKey** <certkeyName> -cert <string> [-key <string>]
- **show sslcertkey** <name>

  Example

```
> add ssl certKey CertKey-SSL-1 -cert ns-root.cert -key ns-
root.key
 Done
> show sslcertkey CertKey-SSL-1
   Name: CertKey-SSL-1 Status: Valid,
   Days to expiration:4811 Version: 3
   Serial Number: 00 Signature Algorithm:
md5WithRSAEncryption Issuer: C=US,ST=California,L=San
   Jose,O=Citrix ANG,OU=NS Internal,CN=de fault
   Validity Not Before: Oct 6 06:52:07 2006 GMT Not After :
Aug 17 21:26:47 2022 GMT
   Subject: C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS
Internal,CN=d efault Public Key
   Algorithm: rsaEncryption Public Key
   size: 1024
 Done
```

To add a certificate key pair by using the configuration utility

1. In the navigation pane, expand **SSL**, and then click **Certificates**.
2. In the details pane, click **Add**.
3. In the **Install Certificate** dialog box, in the **Certificate-Key Pair Name** text box, type a name for the certificate key pair you want to add, for example, `Certkey-SSL-1`.

4. Under **Details**, in **Certificate File Name**, click **Browse (Appliance)** to locate the certificate.

   Both the certificate and the key are stored in the /nsconfig/ssl/ folder on the appliance. To use a certificate present on the local system, select **Local**.

5. Select the certificate you want to use, and then click **Select**.
6. In **Private Key File Name**, click **Browse (Appliance)** to locate the private key file.

   To use a private key present on the local system, select **Local**.

7. Select the key you want to use and click **Select.**

   To encrypt the key used in the certificate key pair, type the password to be used for encryption in the **Password** text box.

8. Click **Install**.
9. Double-click the certificate key pair and, in the **Certificate Details** window, verify that the parameters have been configured correctly and saved.

Binding an SSL Certificate Key Pair to the Virtual Server

After you have paired an SSL certificate with its corresponding key, you must bind the certificate key pair to the SSL virtual server so that it can be used for SSL processing. Secure sessions require establishing a connection between the client computer and an SSL-based virtual server on the appliance. SSL processing is then carried out on the incoming traffic at the virtual server. Therefore, before enabling the SSL virtual server on the appliance, you need to bind a valid SSL certificate to the SSL virtual server.

To bind an SSL certificate key pair to a virtual server by using the command line interface

At the command prompt, type the following commands to bind an SSL certificate key pair to a virtual server and verify the configuration:

- **bind ssl vserver** <vServerName> -certkeyName <string>
- **show ssl vserver** <name>

  Example

```
 > bind ssl vserver Vserver-SSL-1 -certkeyName CertKey-SSL-1
Done
> show ssl vserver Vserver-SSL-1

     Advanced SSL configuration for VServer Vserver-SSL-1:
     DH: DISABLED
     Ephemeral RSA: ENABLED Refresh Count: 0
     Session Reuse: ENABLED Timeout: 120 seconds
     Cipher Redirect: ENABLED
     SSLv2 Redirect: ENABLED
```

```
     ClearText Port: 0
     Client Auth: DISABLED
     SSL Redirect: DISABLED
     Non FIPS Ciphers: DISABLED
     SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED

1) CertKey Name: CertKey-SSL-1 Server Certificate
1) Cipher Name: DEFAULT
   Description: Predefined Cipher Alias
Done
```

To bind an SSL certificate key pair to a virtual server by using the configuration utility

1. In the navigation pane, expand **SSL Offload**, and then click **Virtual Servers**.
2. Select the virtual server to which you want to bind the certificate key pair, for example, **Vserver-SSL-1**, and click **Open**.
3. In the **Configure Virtual Server (SSL Offload)** dialog box, on the **SSL Settings** tab, under **Available**, select the certificate key pair that you want to bind to the virtual server (for example, **Certkey-SSL-1**), and then click **Add**.
4. Click **OK.**
5. Verify that the certificate key pair that you selected appears in the **Configured** area.

Configuring Support for Outlook Web Access

If you use Outlook Web Access (OWA) servers on your NetScaler appliance, you must configure the appliance to insert a special header field, FRONT-END-HTTPS: ON, in HTTP requests directed to the OWA servers, so that the servers generate URL links as https:// instead of http://.

Note: You can enable OWA support for HTTP-based SSL virtual servers and services only. You cannot apply it for TCP-based SSL virtual servers and services.

To configure OWA support, do the following:

- Create an SSL action to enable OWA support.
- Create an SSL policy.
- Bind the policy to the SSL virtual server.

Creating an SSL Action to Enable OWA Support

Before you can enable Outlook Web Access (OWA) support, you must create an SSL action. SSL actions are bound to SSL policies and triggered when incoming data matches the rule specified by the policy.

To create an SSL action to enable OWA support by using the command line interface

At the command prompt, type the following commands to create an SSL action to enable OWA support and verify the configuration:

- **add ssl action** <name> -OWASupport ENABLED
- **show SSL action** <name>

```
 > add ssl action Action-SSL-OWA -OWASupport enabled
Done
> show SSL action Action-SSL-OWA
   Name: Action-SSL-OWA
   Data Insertion Action: OWA
   Support: ENABLED
Done
```

To create an SSL action to enable OWA support by using the configuration utility

1. In the navigation pane, expand **SSL**, and then click **Policies**.
2. In the details pane, on the **Actions** tab, click **Add**.
3. In the **Create SSL Action** dialog box, in the **Name** text box, type `Action-SSL-OWA`.
4. Under **Outlook Web Access**, select **Enabled**.
5. Click **Create**, and then click **Close**.
6. Verify that **Action-SSL-OWA** appears in the **SSL Actions** page.

Creating SSL Policies

SSL policies are created by using the policy infrastructure. Each SSL policy has an SSL action bound to it, and the action is carried out when incoming traffic matches the rule that has been configured in the policy.

To create an SSL policy by using the command line interface

At the command prompt, type the following commands to configure an SSL policy and verify the configuration:

- **add ssl policy** <name> -rule <expression> -reqAction <string>

- **show ssl policy** <name>

  Example

```
   > add ssl policy Policy-SSL-1 -rule ns_true -reqaction
Action-SSL-OWA
   Done
   > show ssl policy Policy-SSL-1
   Name: Policy-SSL-1      Rule: ns_true
   Action: Action-SSL-OWA  Hits: 0
   Policy is bound to following entities
   1)      PRIORITY : 0
   Done
```

To create an SSL policy by using the configuration utility

1. In the navigation pane, expand **SSL**, and then click **Policies**.
2. In the details pane, click **Add**.
3. In the **Create SSL Policy** dialog box, in the **Name** text box, type the name of the SSL Policy (for example, `Policy-SSL-1`).
4. In **Request Action**, select the configured SSL action that you want to associate with this policy (for example, **Action-SSL-OWA**).

   The `ns_true` general expression applies the policy to all successful SSL handshake traffic. However, if you need to filter specific responses, you can create policies with a higher level of detail. For more information about configuring granular policy expressions, see "Understanding Policies and Expressions."
5. In **Named Expressions**, choose the built-in general expression `ns_true` and click **Add Expression**. The expression `ns_true` now appears in the Expression text box.
6. Click **Create**, and then click **Close**.
7. Verify that the policy is correctly configured by selecting the policy and viewing the **Details** section at the bottom of the pane.

Binding the SSL Policy to an SSL Virtual Server

After you configure an SSL policy for Outlook Web Access, bind the policy to a virtual server that will intercept incoming Outlook traffic. If the incoming data matches any of the rules configured in the SSL policy, the policy is triggered and the action associated with it is carried out.

To bind an SSL policy to an SSL virtual server by using the command line interface

At the command prompt, type the following commands to bind an SSL policy to an SSL virtual server and verify the configuration:

- **bind ssl vserver** <vServerName> -policyName <string>

- **show ssl vserver** <name>

  Example

```
> bind ssl vserver Vserver-SSL-1 -policyName Policy-SSL-1
 Done
> show ssl vserver Vserver-SSL-1
        Advanced SSL configuration for VServer Vserver-
SSL-1:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 0
        Session Reuse: ENABLED          Timeout: 120 seconds
        Cipher Redirect: ENABLED
        SSLv2 Redirect: ENABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED

1)      CertKey Name: CertKey-SSL-1 Server Certificate

1)      Policy Name: Policy-SSL-1
                        Priority: 0
1)      Cipher Name: DEFAULT
        Description: Predefined Cipher Alias
 Done
>
```

To bind an SSL policy to an SSL virtual server by using the configuration utility

1. In the navigation pane, expand **SSL Offload**, and then click **Virtual Servers**.
2. In the details pane, select the virtual server (for example, **Vserver-SSL-1**), and then click **Open**.
3. In the **Configure Virtual Server (SSL Offload)** dialog box, click **Insert Policy**, and then select the policy that you want to bind to the SSL virtual server. Optionally, you can double-click the **Priority** field and type a new priority level.
4. Click **OK.**

Features at a Glance

Citrix NetScaler features can be configured independently or in combinations to address specific needs. Although some features fit more than one category, the numerous NetScaler features can generally be categorized as application switching and traffic management features, application acceleration features, and application security and firewall features, and an application visibility feature.

To understand the order in which the features perform their processing, see "Processing Order of Features."

Application Switching and Traffic Management Features

SSL Offloading

Transparently offloads SSL encryption and decryption from web servers, freeing server resources to service content requests. SSL places a heavy burden on an application's performance and can render many optimization measures ineffective. SSL offload and acceleration allow all the benefits of Citrix Request Switching technology to be applied to SSL traffic, ensuring secure delivery of web applications without degrading end-user performance.

For more information, see "SSL Offload and Acceleration."

Access Control Lists

Compares incoming packets to Access Control Lists (ACLs). If a packet matches an ACL rule, the action specified in the rule is applied to the packet. Otherwise, the default action (ALLOW) is applied and the packet is processed normally. For the appliance to compare incoming packets to the ACLs, you have to apply the ACLs. All ACLs are enabled by default, but you have to apply them in order for the NetScaler to compare incoming packets against them. If an ACL is not required to be a part of the lookup table, but still needs to be retained in the configuration, it should be disabled before the ACLs are applied. A NetScaler does not compare incoming packets to disabled ACLs.

For more information, see "Access Control Lists."

Load Balancing

Load balancing decisions are based on a variety of algorithms, including round robin, least connections, weighted least bandwidth, weighted least packets, minimum response time, and hashing based on URL, domain source IP, or destination IP. Both the TCP and UDP protocols are supported, so the NetScaler can load balance all traffic that uses those protocols as the underlying carrier (for example, HTTP, HTTPS, UDP, DNS, NNTP, and general firewall traffic). In addition, the NetScaler can maintain

session persistence based on source IP, cookie, server, group, or SSL session. It allows users to apply custom Extended Content Verification (ECV) to servers, caches, firewalls and other infrastructure devices to ensure that these systems are functioning properly and are providing the right content to users. It can also perform health checks using ping, TCP, or HTTP URL, and the user can create monitors based on Perl scripts. To provide high-scale WAN optimization, the CloudBridge appliances deployed at data centers can be load balanced through NetScaler appliances. The bandwidth and number of concurrent sessions can be improved significantly.

For more information, see "Load Balancing."

Content Switching

Determines the server to which to send the request on the basis of configured content switching policies. Policy rules can be based on the IP address, URL, and HTTP headers. This allows switching decisions to be based on user and device characteristics such as who the user is, what type of agent is being used, and what content the user requested.

For more information, see "Content Switching."

Global Server Load Balancing (GSLB)

Extends the traffic management capabilities of a NetScaler to include distributed Internet sites and global enterprises. Whether installations are spread across multiple network locations or multiple clusters in a single location, the NetScaler maintains availability and distributes traffic across them. It makes intelligent DNS decisions to prevent users from being sent to a site that is down or overloaded. When the proximity-based GSLB method is enabled, the NetScaler can make load balancing decisions based on the proximity of the client's local DNS server (LDNS) in relation to different sites. The main benefit of the proximity-based GSLB method is faster response time resulting from the selection of the closest available site.

For more information, see "Global Server Load Balancing."

Dynamic Routing

Enables routers to obtain topology information, routes, and IP addresses from neighboring routers automatically. When dynamic routing is enabled, the corresponding routing process listens to route updates and advertises routes. The routing processes can also be placed in passive mode. Routing protocols enable an upstream router to load balance traffic to identical virtual servers hosted on two standalone NetScaler units using the Equal Cost Multipath technique.

For more information, see "Configuring Dynamic Routes."

Link Load Balancing

Load balances multiple WAN links and provides link failover, further optimizing network performance and ensuring business continuity. Ensures that network connections remain highly available, by applying intelligent traffic control and health checks to distribute traffic efficiently across upstream routers. Identifies the best WAN link to route both incoming and outbound traffic based on policies and network conditions, and protects applications against WAN or Internet link failure by providing rapid fault detection and failover.

For more information, see " Link Load Balancing."

TCP Optimization

You can use TCP profiles to optimize TCP traffic. TCP profiles define the way that NetScaler virtual servers process TCP traffic. Administrators can use the built-in TCP profiles or configure custom profiles. After defining a TCP profile, you can bind it to a single virtual server or to multiple virtual servers.

Web Interface on NetScaler

Provides access to XenApp and XenDesktop resources, which include applications, content, and desktops. Users access resources through a standard Web browser or by using the Citrix XenApp plug-in. The Web Interface runs as a service on port 8080 on the NetScaler appliance. To create Web Interface sites, Java is executed on Apache Tomcat Web server version 6.0.26 on the NetScaler appliance.

Note: Web Interface is supported only on NetScaler nCore releases.

For more information, see "Web Interface."

CloudBridge

The Citrix NetScaler CloudBridge feature, a fundamental part of the Citrix OpenCloud framework, is a tool used to build a cloud-extended data center. The OpenCloud Bridge enables you to connect one or more NetScaler appliances or NetScaler virtual appliances on the cloud-to your network without reconfiguring your network. Cloud hosted applications appear as though they are running on one contiguous enterprise network. The primary purpose of the OpenCloud Bridge is to enable companies to move their applications to the cloud while reducing costs and the risk of application failure. In addition, the OpenCloud Bridge increases network security in cloud environments. An OpenCloud Bridge is a Layer-2 network bridge that connects a NetScaler appliance or NetScaler virtual appliance on a cloud instance to a NetScaler appliance or NetScaler virtual appliance on your LAN. The connection is made through a tunnel that uses the Generic Routing Encapsulation (GRE) protocol. The GRE protocol provides a mechanism for encapsulating packets from a wide variety of network protocols to be forwarded over another protocol. Then Internet Protocol security (IPsec) protocol suite is used to secure the communication between the peers in the OpenCloud Bridge.

For more information, see "CloudBridge."

DataStream

The NetScaler DataStream feature provides an intelligent mechanism for request switching at the database layer by distributing requests on the basis of the SQL query being sent.

When deployed in front of database servers, a NetScaler ensures optimal distribution of traffic from the application servers and Web servers. Administrators can segment traffic according to information in the SQL query and on the basis of database names, user names, character sets, and packet size.

You can configure load balancing to switch requests according to load balancing algorithms, or you can elaborate the switching criteria by configuring content

switching to make a decision based on SQL query parameters, such as user name, database names, and command parameters. You can further configure monitors to track the states of database servers.

The advanced policy infrastructure on the NetScaler appliance includes expressions that you can use to evaluate and process the requests. The advanced expressions evaluate traffic associated with MySQL database servers. You can use request-based expressions (expressions that begin with `MYSQL.CLIENT` and `MYSQL.REQ`) in advanced policies to make request switching decisions at the content switching virtual server bind point and response-based expressions (expressions that begin with `MYSQL.RES`) to evaluate server responses to user-configured health monitors.

Note: DataStream is supported for MySQL and MS SQL databases.

For more information, see "DataStream."

Application Acceleration Features

AppCompress

Uses the gzip compression protocol to provide transparent compression for HTML and text files. The typical 4:1 compression ratio yields up to 50% reduction in bandwidth requirements out of the data center. It also results in significantly improved end-user response time, because it reduces the amount of data that must be delivered to the user's browser.

For more information, see "Compression."

Cache Redirection

Manages the flow of traffic to a reverse proxy, transparent proxy, or forward proxy cache farm. Inspects all requests, and identifies non-cacheable requests and sends them directly to the origin servers over persistent connections. By intelligently redirecting non-cacheable requests back to the origin web servers, the NetScaler appliance frees cache resources and increases cache hit rates while reducing overall bandwidth consumption and response delays for these requests.

For more information, see "Cache Redirection."

AppCache

Helps optimize web content and application data delivery by providing a fast in-memory HTTP/1.1 and HTTP/1.0 compliant web caching for both static and dynamic content. This on-board cache stores the results of incoming application requests even when an incoming request is secured or the data compressed, and then reuses the data to fulfill subsequent requests for the same information. By serving data directly from the on-board cache, the appliance can reduce page regeneration times by eliminating the need to funnel static and dynamic content requests to the server.

For more information, see "Integrated Caching."

TCP Buffering

Buffers the server's response and delivers it to the client at the client's speed, thus offloading the server faster and thereby improving the performance of web sites.

For more information, see "TCP Buffering."

Application Security and Firewall Features

Denial of Service Attack (DoS) Defense

Detects and stops malicious distributed denial-of-service (DDoS) attacks and other types of malicious attacks before they reach your servers, preventing them from affecting network and application performance. The NetScaler appliance identifies legitimate clients and elevates their priority, leaving suspect clients unable to consume a disproportionate percentage of resources and cripple your site. The appliance provides application-level protection from the following types of malicious attacks:

- SYN flood attacks
- Pipeline attacks
- Teardrop attacks
- Land attacks
- Fraggle attacks
- Zombie connection attacks

The appliance aggressively defends against these types of attacks by preventing the allocation of server resources for these connections. This insulates servers from the overwhelming flood of packets associated with these events.

The appliance also protects network resources from ICMP based attacks by using ICMP rate limiting and aggressive ICMP packet inspection. It performs strong IP reassembly, drops a variety of suspicious and malformed packets, and applies Access Control Lists (ACLs) to site traffic for further protection.

For more information, see "HTTP Denial-of-Service Protection."

Content Filtering

Provides protection from malicious attacks for web sites at the Layer 7 level. The appliance inspects each incoming request according to user-configured rules based on HTTP headers, and performs the action the user configured. Actions can include resetting the connection, dropping the request, or sending an error message to the user's browser. This allows the appliance to screen unwanted requests and reduces your servers' exposure to attacks.

This feature can also analyze HTTP GET and POST requests and filter out known bad signatures, allowing it to defend your servers against HTTP-based attacks.

For more information, see "Content Filtering."

Responder

Functions like an advanced filter and can be used to generate responses from the appliance to the client. Some common uses of this feature are generation of redirect responses, user defined responses, and resets.

For more information, see "Responder."

Rewrite

Modifies HTTP headers and body text. You can use the rewrite feature to add HTTP headers to an HTTP request or response, make modifications to individual HTTP headers, or delete HTTP headers. It also enables you to modify the HTTP body in requests and responses.

When the appliance receives a request or sends a response, it checks for rewrite rules, and if applicable rules exist, it applies them to the request or response before passing it on to the web server or client computer.

For more information, see "Rewrite."

Priority Queuing

Prioritizes user requests to ensure that the most important traffic is serviced first during surges in request volume. You can establish priority based on request URLs, cookies, or a variety of other factors. The appliance places requests in a three-tier queue based on their configured priority, enabling business-critical transactions to flow smoothly even during surges or site attacks.

For more information, see "Priority Queuing."

Surge Protection

Regulates the flow of user requests to servers and controls the number of users that can simultaneously access the resources on the servers, queuing any additional requests once your servers have reached their capacity. By controlling the rate at which connections can be established, the appliance blocks surges in requests from being passed on to your servers, thus preventing site overload.

For more information, see "Surge Protection."

Access Gateway

Access Gateway is a secure application access solution that provides administrators granular application-level policy and action controls to secure access to applications and data while allowing users to work from anywhere. It gives IT administrators a single point of control and tools to help ensure compliance with regulations and the highest levels of information security across and outside the enterprise. At the same time, it empowers users with a single point of access—optimized for roles, devices, and networks—to the enterprise applications and data they need. This unique combination of capabilities helps maximize the productivity of today's mobile workforce.

For more information, see "Access Gateway."

Application Firewall

Protects applications from misuse by hackers and malware, such as cross site scripting attacks, buffer overflow attacks, SQL injection attacks, and forceful browsing, by filtering traffic between each protected web server and users that connect to any web site on that web server. The application firewall examines all traffic for evidence of attacks on web server security or misuse of web server resources, and takes the appropriate action to prevent these attacks from succeeding.

For more information, see "Application Firewall."

Application Visibility Feature

NetScaler Insight Center

NetScaler Insight Center is a high performance collector that provides end-to-end user experience visibility across Web and HDX (ICA) traffic. It collects HTTP and ICA AppFlow records generated by NetScaler ADC appliances and populates analytical reports covering Layer 3 to Layer 7 statistics. NetScaler Insight Center provides in-depth analysis for the last five minutes of real-time data, and for historical data collected for the last one hour, one day, one week, and one month.

HDX (ICA) analytic dashboard enables you to drill down from HDX Users, Applications, Desktops, and even from gateway-level information. Similarly, HTTP analytics provide a bird's eye view of Web Applications, URLs Accessed, Client IP Addresses and Server IP Addresses, and other dashboards. The administrator can drill down and identify the pain points from any of these dashboards, as appropriate for the use case.

EdgeSight for NetScaler

Support for application performance monitoring based on end user experience. This solution leverages the HTML injection feature to obtain various time values, which are used by EdgeSight server for analysis and report generation. EdgeSight for NetScaler provides a way to monitor the performance benefits of a NetScaler and determine potential bottlenecks in a network.

For more information, see "EdgeSight Monitoring for NetScaler."

Enhanced Application Visibility Using AppFlow

The Citrix NetScaler appliance is a central point of control for all application traffic in the data center. It collects flow and user-session level information valuable for application performance monitoring, analytics, and business intelligence applications. AppFlow transmits this information by using the Internet Protocol Flow Information eXport (IPFIX) format, which is an open Internet Engineering Task Force (IETF) standard defined in RFC 5101. IPFIX (the standardized version of Cisco's NetFlow) is widely used to monitor network flow information. AppFlow defines new Information Elements to represent application-level information.

Using UDP as the transport protocol, AppFlow transmits the collected data, called *flow records*, to one or more IPv4 collectors. The collectors aggregate the flow records and generate real-time or historical reports.

AppFlow provides visibility at the transaction level for HTTP, SSL, TCP, and SSL_TCP flows. You can sample and filter the flow types that you want to monitor.

To limit the types of flows to monitor, by sampling and filtering the application traffic, you can enable AppFlow for a virtual server. AppFlow can also provide statistics for the virtual server.

You can also enable AppFlow for a specific service, representing an application server, and monitor the traffic to that application server.

For more information, see "AppFlow."

Stream Analytics

The performance of your web site or application depends on how well you optimize the delivery of the most frequently requested content. Techniques such as caching and compression help accelerate the delivery of services to clients, but you need to be able to identify the resources that are requested most frequently, and then cache or compress those resources. You can identify the most frequently used resources by aggregating real-time statistics about website or application traffic. Statistics such as how frequently a resource is accessed relative to other resources and how much bandwidth is consumed by those resources help you determine whether those resources need to be cached or compressed to improve server performance and network utilization. Statistics such as response times and the number of concurrent connections to the application help you determine whether you must enhance server-side resources.

If the web site or application does not change frequently, you can use products that collect statistical data, and then manually analyze the statistics and optimize the delivery of content. However, if you do not want to perform manual optimizations, or if your web site or application is dynamic in nature, you need infrastructure that can not only collect statistical data but can also automatically optimize the delivery of resources on the basis of the statistics. On the NetScaler appliance, this functionality is provided by the Stream Analytics feature. The feature operates on a single NetScaler appliance and collects run-time statistics on the basis of criteria that you define. When used with NetScaler policies, the feature also provides you with the infrastructure that you need for automatic, real-time traffic optimization.

For more information, see "Stream Analytics."

Licensing, Upgrading, and Downgrading

2015-05-18 16:52:06 UTC

Contents

Licensing, Upgrading, and Downgrading

The following topics describe the migration instructions for setting up a new version of a NetScaler with a list of all new and deprecated commands, parameters, and SNMP OIDs.

New and Deprecated Commands, Parameters, and SNMP OIDs	Lists the foundational changes that affect the base system and its configuration, including new and deprecated commands, parameters, and SNMP OIDs.
Upgrading or Downgrading the System Software	Describes the licensing framework and the procedure for upgrading or downgrading the system software across releases and within a release.

New and Deprecated Commands, Parameters, and SNMP OIDs

Welcome to the NetScaler 10 system software release. There are new commands, parameters, and SNMP OIDs in this release. Some commands, parameters, and SNMP OIDs will be deprecated in this release. For complete descriptions of the new commands and parameters, see "Command Reference". For complete descriptions of the SNMP OIDs, see the *Citrix NetScaler SNMP OID Reference Guide* at "http://support.citrix.com/article/CTX132381".

New and Deprecated Commands, Parameters, and SNMP OIDs

Welcome to the NetScaler 10 system software release. There are new commands, parameters, and SNMP OIDs in this release. Some commands, parameters, and SNMP OIDs will be deprecated in this release. For complete descriptions of the new commands and parameters, see "Command Reference". For complete descriptions of the SNMP OIDs, see the *Citrix NetScaler SNMP OID Reference Guide* at "http://support.citrix.com/article/CTX132381".

ns-migration-new-cmds-10-ref

Due to technical difficulties, we are unable to display this topic. Citrix is currently fixing this problem. In the meantime, you can view this topic online:

http://support.citrix.com/proddocs/index.jsp?lang=en&topic=/netscaler-migration-10/ns-migration-new-cmds-10-ref.html

Deprecated Commands

The following commands are deprecated in release 10.

- rm vserver
- set vserver
- unset vserver
- enable vserver
- disable vserver
- add lb wlm
- rm lb wlm
- set lb wlm
- show lb wlm
- bind lb wlm
- unbind lb wlm
- add ns limitSelector
- rm ns limitSelector
- set ns limitSelector
- show ns limitSelector
- add ns appflowCollector
- rm ns appflowCollector
- show ns appflowCollector
- set ns appflowParam
- show ns appflowParam

ns-migration-new-params-10-ref

Due to technical difficulties, we are unable to display this topic. Citrix is currently fixing this problem. In the meantime, you can view this topic online:

http://support.citrix.com/proddocs/index.jsp?lang=en&topic=/netscaler-migration-10/ns-migration-new-params-10-ref.html

Deprecated Parameters

The following parameters are deprecated in release 10.

- add service -serverID
- set service -serverID
- unset service -serverID
- bind serviceGroup -serverID
- add dns policy -viewName -preferredLocation -drop -cacheBypass
- set dns policy -viewName -preferredLocation -drop -cacheBypass
- show dns aaaaRec [<IPv6Address>]
- show dns addRec [<IPAddress>]
- show dns mxRec [-mx <string>]
- show dns nsRec [<nameServer>]
- show dns ptrRec [<domain>]
- add lb monitor -destIP *
- set lb monitor -destIP *
- add gslb vserver -backupSessionTimeout
- set gslb vserver -backupSessionTimeout
- set ns config -httpPort -maxConn -maxReq -cip -cookieversion -secureCookie -pmtuMin -pmtuTimeout -ftpPortRange -crPortRange -timezone -grantQuotaMaxClient -exclusiveQuotaMaxClient -grantQuotaSpillOver -exclusiveQuotaSpillOver
- unset ns config -ftpPortRange -crPortRange -timezone
- set ns -tcpParam -KAprobeUpdateLastactivity
- add ssl policy -reqAction

New SNMP OIDs

The following table lists the new SNMP OIDs in release 10.

OID	Description
Application firewall	
1.3.6.1.4.1.5951.4.1.1.64.1.34	AppFirewall SNMP traps dropped due to time limit.
Cluster	
1.3.6.1.4.1.5951.4.1.1.72	The cluster table. This is indexed on the clID.
1.3.6.1.4.1.5951.4.1.1.72.1	
1.3.6.1.4.1.5951.4.1.1.72.1.1	This represents the unique id of the cluster node
1.3.6.1.4.1.5951.4.1.1.72.1.2	This represents the IP address of the cluster node
Load Balancing	
1.3.6.1.4.1.5951.4.1.2.7.1.36	The name of the server of the servicegroup member
1.3.6.1.4.1.5951.4.1.3.1.1.67	Number invalid requests/responses on this vserver
1.3.6.1.4.1.5951.4.1.3.1.1.68	Number invalid requests/responses dropped on this vserver
Networking	
1.3.6.1.4.1.5951.4.1.1.20.62	This represents whether ISIS feature is enabled or disabled on NetScaler
1.3.6.1.4.1.5951.4.1.1.22.7	This provides statistical information about the configured PBR6s, in the rs9000 product family of NetScaler products.
1.3.6.1.4.1.5951.4.1.1.22.7.20	This table contains all the PBRs configured. This is indexed on the acPbrName.
1.3.6.1.4.1.5951.4.1.1.22.7.20.1	
1.3.6.1.4.1.5951.4.1.1.22.7.20.1.1	The name of the PBR6
1.3.6.1.4.1.5951.4.1.1.22.7.20.1.2	The full name of the PBR6
1.3.6.1.4.1.5951.4.1.1.22.7.20.1.3	The priority of the PBR6
1.3.6.1.4.1.5951.4.1.1.22.7.20.1.4	Number of times the pbr6 was hit
1.3.6.1.4.1.5951.4.1.1.22.7.21	Total packets that matched the PBR6 with action ALLOW
1.3.6.1.4.1.5951.4.1.1.22.7.22	Total packets that matched PBR6 with action DENY
1.3.6.1.4.1.5951.4.1.1.22.7.23	Total packets that matched one of the configured PBR6

1.3.6.1.4.1.5951.4.1.1.22.7.24	Total packets that did not match any PBR6
1.3.6.1.4.1.5951.4.1.1.71	This provides statistical information about the total number of megabits received/transmitted on the Network Interfaces configured in the Netscaler product.
1.3.6.1.4.1.5951.4.1.1.71.1	Number of megabits received by the NetScaler appliance.
1.3.6.1.4.1.5951.4.1.1.71.2	Number of megabits transmitted by the NetScaler appliance.
1.3.6.1.4.1.5951.4.1.10.2.32	the state of HA License check
SSL	
1.3.6.1.4.1.5951.4.1.10.2.33	This represents the interpretation details of sslCardStatus.
System	
1.3.6.1.4.1.5951.4.1.1.16	The model ID is populated if the system is such that it is license controlled. If the system does not support license based models, then the model id will be zero.
1.3.6.1.4.1.5951.4.1.1.46.90	Current threshold for TCP rate control. By default, there is no rate control for TCP.
1.3.6.1.4.1.5951.4.1.10.2.34	This represents the status of CallHome Upload Event.

Upgrading or Downgrading the System Software

NetScaler 10 offers new and updated features with increased functionality. A comprehensive list of enhancements is listed in the release notes accompanying the release announcement. Take a moment to read this document before you upgrade your software.

It is important to understand the licensing framework and types of licenses before you upgrade your software. A software edition upgrade may require new licenses, such as upgrading from the standard edition to the enterprise edition, the standard edition to the platinum edition, or the enterprise edition to the platinum edition.

Note: For upgrading or downgrading the nodes in a cluster setup, see "Upgrading or Downgrading the Cluster Software".

Changes to the Licensing Framework

The licensing framework has changed since release 8.1, build 65.5. For more information, see "http://support.citrix.com/article/ctx121062".

Citrix NetScaler Application Accelerator users have been upgraded to the Access Gateway Enterprise Edition without any change in functionality.

NetScaler Licenses

A NetScaler must be properly licensed before it can be deployed to distribute, optimize, or secure network traffic for Web applications. After you have obtained the licenses, you must install the licenses on your appliance, and then verify that the features corresponding to these licenses are enabled.

Obtaining NetScaler Licenses

The procedure to obtain NetScaler licenses has changed. For more information, see "http://support.citrix.com/article/ctx121062".

Installing NetScaler Licenses

Install each license to use the feature controlled by that license.

To install the licenses by using the command line interface

1. Open an SSH connection to the NetScaler by using an SSH client, such as PuTTY.
2. Log on to the NetScaler by using the administrator credentials.
3. Switch to the shell prompt, create a license subdirectory in the nsconfig directory, if it does not exist, and copy the new license file(s) to this directory.

   Example

   ```
   login: nsroot
   Password: nsroot
   Last login: Mon Aug  4 03:37:27 2008 from 10.102.29.9
   Done
   > shell
   Last login: Mon Aug  4 03:51:42 from 10.103.25.64
   root@ns# mkdir /nsconfig/license
   root@ns# cd /nsconfig/license
   ```

   Copy the new license file(s) to this directory.

   Note: The NetScaler appliance does not prompt for a reboot option when you use the command line interface to install the licenses. Run the `reboot -w` command to warm reboot the system, or run the `reboot` command to reboot the system normally.

To install the licenses by using the configuration utility

1. In a Web browser, type the IP address of the NetScaler, such as `http://192.168.100.1`.
2. In User Name and Password, type the administrator credentials.
3. In Start in, select Configuration, and then click Login, as shown in the following figure.

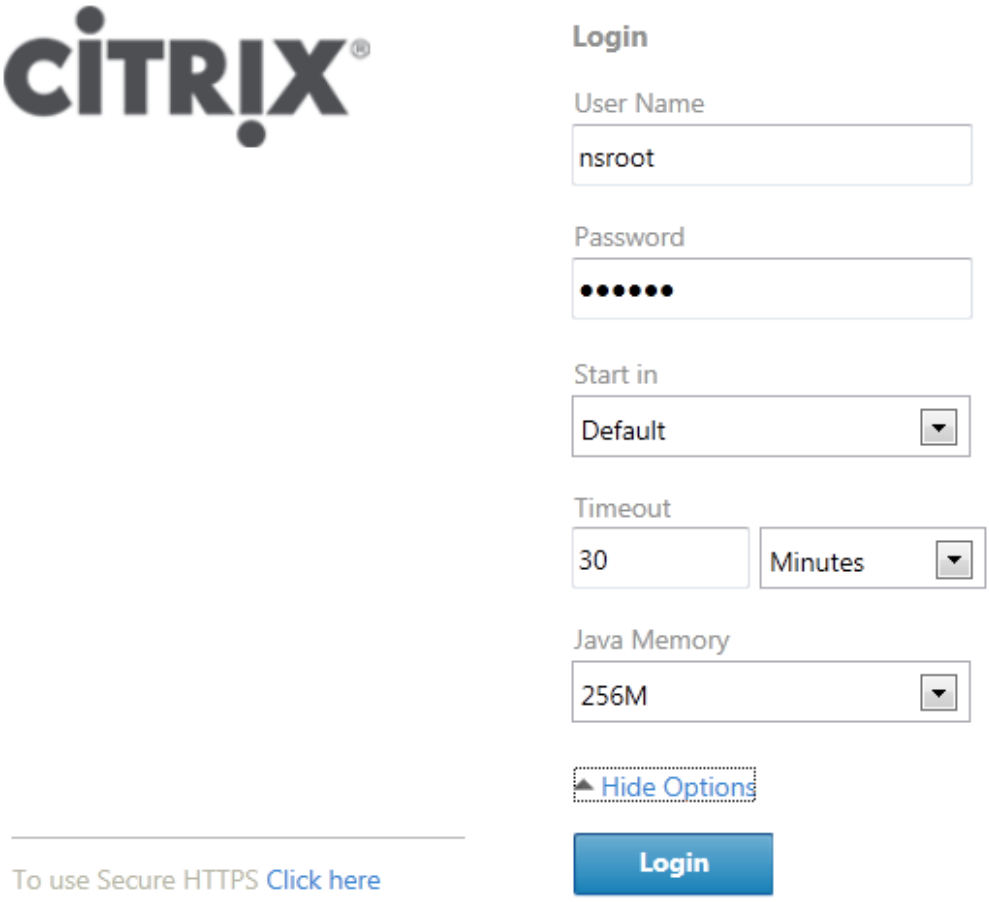


Figure 1. Login Screen

4. In the navigation pane, expand System, and then click Licenses.
5. In the Licenses pane, click Manage Licenses. If the /nsconfig/license directory does not exist, you are prompted to create it.
6. In the Manage Licenses dialog box, click Add.
7. In the Select License Files dialog box, navigate to the location of the license files and select the file you want to upload (for example, Citrix NetScaler IPv6 - Option.lic).
8. Click Select.

9. After your file is uploaded to the license directory, click OK.
10. When prompted to restart the NetScaler, do one of the following:
    - If you plan to upgrade your software, click No.
    - If you don’t plan to upgrade your software, click Yes to restart the NetScaler.

Verifying the Licensed Features

Before using a feature, make sure that your license supports the feature.

To verify the licensed features by using the command line interface

1. Open an SSH connection to the NetScaler by using an SSH client, such as PuTTY.
2. Log on to the NetScaler by using the administrator credentials.
3. At the command prompt, enter the sh ns license command to display the features supported by the license.

   Example

```
sh ns license
        License status:
                        Web Logging: YES
                    Surge Protection: YES
                      .......

                      HTML Injection: YES
 Done
```

To verify the licensed features by using the configuration utility

1. In a Web browser, type the IP address of the NetScaler, such as `http://192.168.100.1`.
2. In User Name and Password, type the administrator credentials.
3. In Start in, select Configuration, and then click Login, as shown in the following figure.

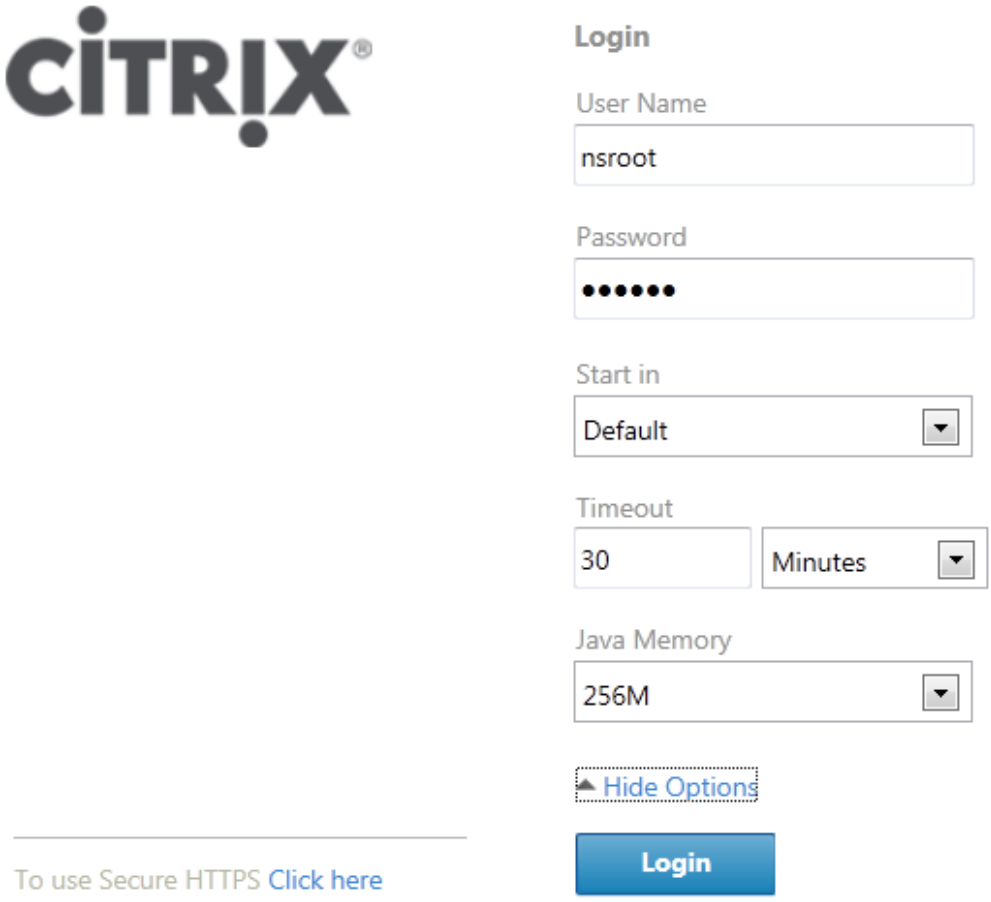


Figure 1. Login Screen

4. In the navigation pane, expand System, and then click Licenses. You will see a green check mark next to the licensed features.

Enabling or Disabling a Feature

When you use the NetScaler for the first time, you need to enable a feature before you can use its functionality. If you configure a feature before it is enabled, a warning message appears. The configuration is saved but it will apply only after the feature is enabled.

To enable a feature by using the command line interface

At the NetScaler command prompt, type the following commands to enable a feature and verify the configuration:

- `enable feature <FeatureName>`
- `show feature`

Example

```
enable feature lb cs
done
 >show feature

      Feature                Acronym          Status
      -------                -------          ------
1)    Web Logging              WL               OFF
2)    Surge Protection         SP               ON
3)    Load Balancing           LB               ON
4)    Content Switching        CS               ON
5)    Cache Redirection        CR               ON
.
.
.
24)   NetScaler Push           push             OFF
Done
```

The example shows how to enable load balancing (lb) and content switching (cs).
If the license key is not available for a particular feature, the following error message appears for that feature:

```
ERROR: feature(s) not licensed
```

Note: To enable an optional feature, you need a feature-specific license. For example, if you have purchased and installed the Citrix NetScaler Enterprise Edition license and need to enable the Integrated Caching feature, you first need to purchase and install the AppCache license.

To disable a feature by using the command line interface

At the NetScaler command prompt, type the following commands to disable a feature and verify the configuration:

- `disable feature <FeatureName>`
- `show feature`

Example

```
> disable feature lb
 Done
> show feature

      Feature                 Acronym          Status
      -------                 -------          ------
 1)   Web Logging               WL               OFF
 2)   Surge Protection          SP               ON
 3)   Load Balancing            LB               OFF
 4)   Content Switching          CS               ON
 .
 .
 .
 24)  NetScaler Push            push             OFF
Done
>
```

The example shows how to disable load balancing (lb).

Access Gateway Universal License

The Access Gateway universal license limits the number of concurrent user sessions to the number of licenses purchased. If you purchase 100 licenses, you can have 100 concurrent sessions at any time. When a user ends a session, that license is released for the next user. A user who logs on to the Access Gateway from more than one computer occupies a license for each session.

If all licenses are occupied, no additional connections can be opened until a user ends a session or the administrator terminates the session using the configuration utility. When a connection is closed, the license is released and can be used for a new user.

Obtaining the Universal License

You need the following information before going to the Citrix Web site for the universal license.

The license code

You can find the code on the Access Gateway CD, in an email you receive from Citrix, or from the Subscription Advantage Management-Renewal-Information (SAMRI) system.

Your user ID and password for My Citrix

Register at My Citrix (www.mycitrix.com) to receive your user ID and password.

Note: If you cannot locate either the license code or your user ID and password, contact Citrix Customer Service.

The host name of the Access Gateway

The entry field for this name on My Citrix is case-sensitive, so make sure that you copy the host name exactly as it is configured on the NetScaler.

The number of licenses you want to include in the license file

You do not have to download all of the licenses you are entitled to at once. For example, if your company purchased 100 licenses, you can choose to download 50. You can allocate the rest in another license file at a later time. Multiple license files can be installed on the Access Gateway.

Note: Before obtaining your licenses, make sure you configure the host name of the NetScaler using the Setup Wizard and then restart the NetScaler.

To obtain your universal license

1. In a Web browser, go to http://www.citrix.com/ and click My Citrix.
2. Enter your user name and password. If this is the first time you are logging on to the site, you are asked for additional background information.
3. Under My Tools, point to Choose a toolbox, and click Activation System/Manage Assets.
4. In the Current Tool drop-down menu, select Activate/Allocate and follow the directions to obtain your license file.

Installing the Universal License

To install the license, see "Installing NetScaler Licenses". After installation, verify that the license was installed correctly.

Verifying Installation of the Universal License

Before proceeding, verify that your universal license is installed correctly.

To verify installation of the universal license by using the command line interface

1. Open an SSH connection to the NetScaler by using an SSH client, such as PuTTY.
2. Log on to the NetScaler by using the administrator credentials.
3. Use the show license command to verify that “SSL VPN = YES” and that Maximum Users has increased from 5 to the expected number of concurrent users.

To verify installation of the universal license by using the configuration utility

1. In a Web browser, type the IP address of the NetScaler, such as `http://192.168.100.1`.
2. In User Name and Password, type the administrator credentials.
3. In the navigation pane, expand System, and then click Licenses.
4. In the Licenses pane, you will see a green check mark next to Access Gateway. The field Maximum Access Gateway Users Allowed displays the number of concurrent user sessions licensed on the NetScaler.

Upgrading to Release 10

You can upgrade to release 10 on a standalone NetScaler or a high availability (HA) pair by using the configuration utility or the command line interface.

Important:

If an IPv6 address is configured as the NetScaler IP (NSIP) address, upgrading from release 8.1 to release 10 changes the NSIP address to the subnet IP (SNIP) address. To add the NSIP address after the upgrade, at the command line interface, type:

```
rm ns ip6
```

```
add ns ip6 <ipv6 address> -type NSIP.
```

There is no change if the NSIP address is an IPv4 address.

Upgrading a Standalone NetScaler

Before upgrading the system software, make sure that you have the required licenses. For more information, see "NetScaler Licenses". Software upgrades from 8.x to 9.x, 8.x and 9.x to 10, and 8.x, 9.x, and 10.x to 10.1 do not require a new license.

Note: When upgrading from release 8.0, 8.1, 9.0, 9.1, 9.2, or 9.3 you have the option to use the configuration utility. All upgrades can be performed by using the command line interface, which is the recommended option. When using the upgrade wizard in the configuration utility to upgrade from release 8.0, do not use the Device option to upload your software.

To upgrade a standalone NetScaler running release 8.1, 9.0, 9.1, 9.2, 9.3 by using the command line interface

In the following procedure, <release> and <releasenumber> represent the release version you are upgrading to, and <targetbuildnumber> represents the build number that you are upgrading to. Refer to the table below for specific values.

Table 1. Release Version Values

Release Version	<release>	<releasenumber>
9.3	9.3	9.3
9.2	9.2	9.2
9.1	9.1	9.1
9.0	9.0	9.0
8.1	rhodes	8.1
8.0	andes	8.0

1. Open an SSH connection to the NetScaler by using an SSH client, such as PuTTY.

2. Log on to the NetScaler by using the administrator credentials. Save the running configuration. At the prompt, type:`save config`

3. Create a copy of the ns.conf file. At the shell prompt, type:

   a. cd /nsconfig

   b. cp ns.conf ns.conf.NS<releasenumber><currentbuildnumber>
   You should backup a copy of the configuration file on another computer.

4. Create a <releasenumber>nsinstall subdirectory in the /var/nsinstall directory.

5. Change directory to /var/nsinstall/<releasenumber>nsinstall, create a directory named build_<targetbuildnumber>, and change to this directory.

6. Download or copy the installation package (build-<release>-<build number>_nc.tgz) and the documentation bundle (ns-<releasenumber>-<build number>-doc.tgz) to this directory and extract the contents of the installation package. To download the installation package from the Citrix Web site, follow the steps below:

   a. Go to MyCitrix.com, log on using your credentials, and click Downloads.

   b. In the Select a Product, select NetScaler ADC.

   c. Under Firmware, click the release and build number to download.

   d. Click Get Firmware.

   e. Click Show Documentation and then click Get Documentation.
7. Run the installns script to install the new version of the system software.

   Note:

   To install a FIPS appliance, run the installns script with the -F option. To automatically clean up the flash, run the installns script with the -c option.

   If the configuration file for the build that you are upgrading to exists on the appliance, you are prompted to load that configuration, as shown in the following figure.

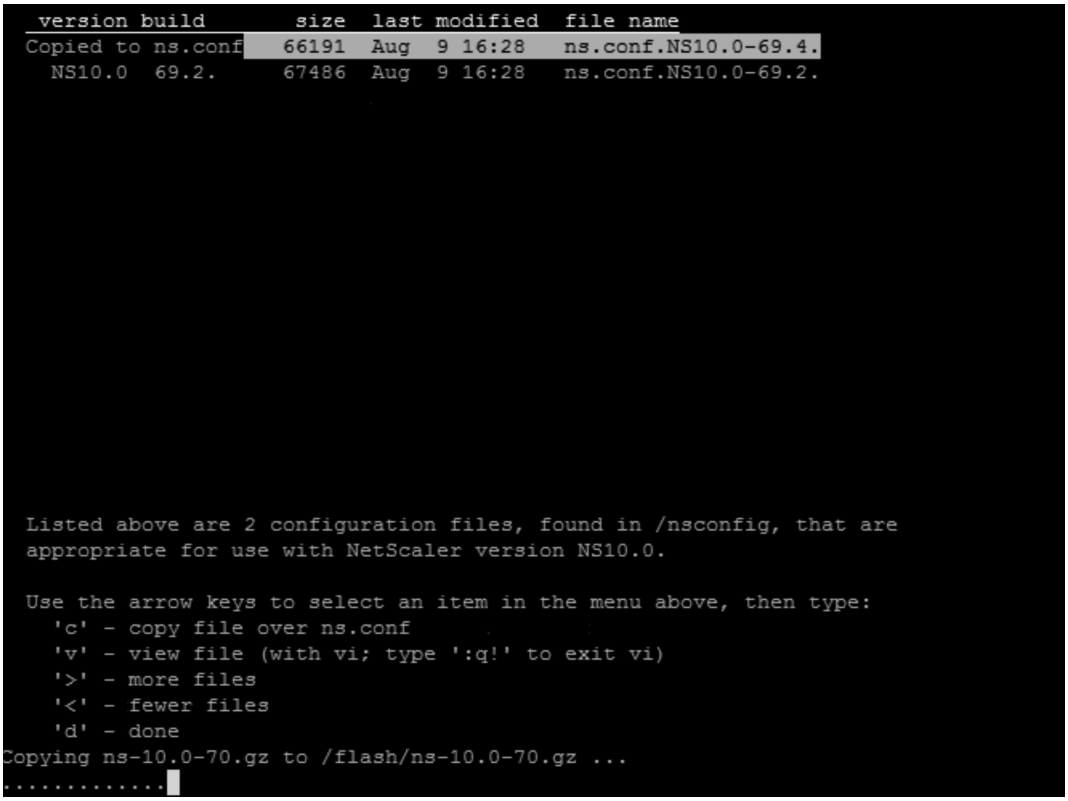


Figure 1. Upgrade menu if configuration file exists

Warning: When upgrading to the NetScaler 10 nCore build, the installation script prompts you to delete the /var directory if the swap partition is smaller than 32 gigabytes (GB). If you receive this prompt, type N, save any important files located in /var to a backup location, and then re-run the installation script.

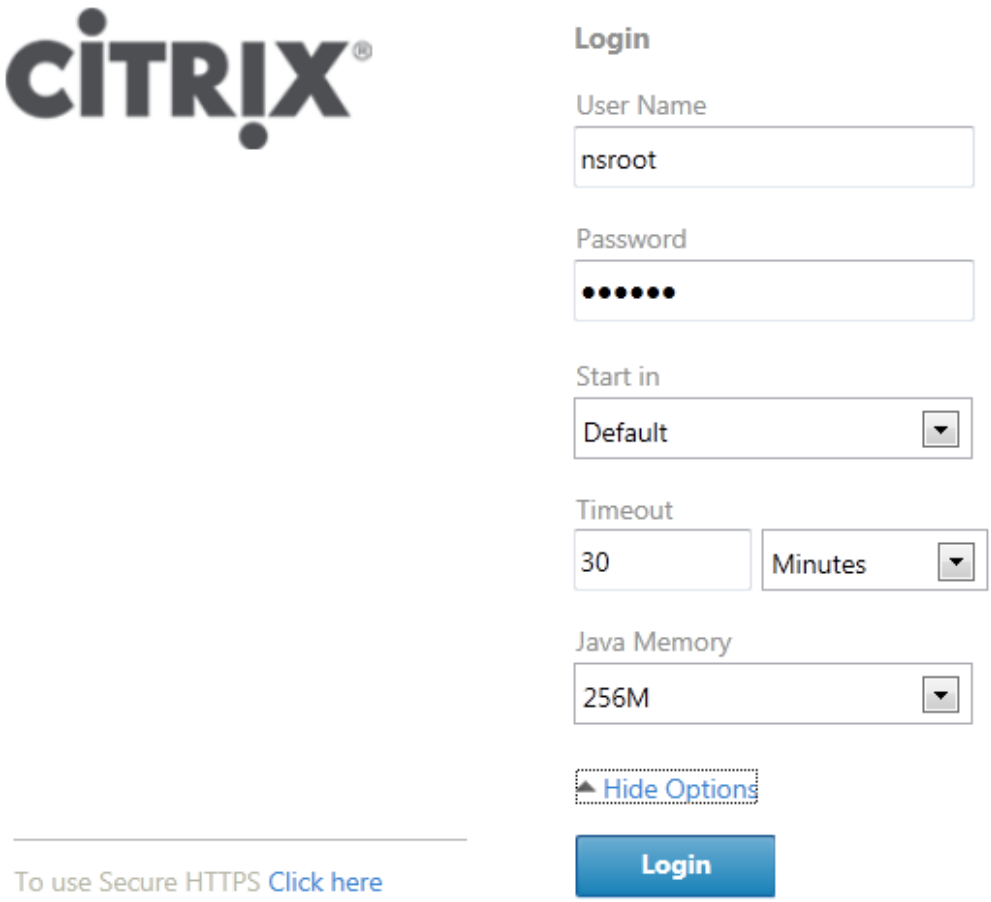
If the free space available on the flash drive is insufficient to install the new build, the NetScaler prompts you to initiate a cleanup of the flash drive. For more information, see "Auto Cleanup".

8. When prompted, restart the NetScaler.

Example

```
login: nsroot
Password: nsroot
Last login: Mon Mar  26 03:37:27 2008 from 10.102.29.9
Done
> save config
> shell
Last login: Mon Mar  26 03:51:42 from 10.103.25.64
root@NSnnn# cd /var/nsinstall
root@NSnnn# cd 10nsinstall
root@NSnnn# mkdir build_53
root@NSnnn# cd build_53
root@NSnnn# ftp ... get build-10.0-53.5_nc.tgz
root@NSnnn# get ns-10.0-53.5-doc.tgz
root@NSnnn# tar xzvf build-10.0-53.5_nc.tgz
root@NSnnn# ./installns
installns version (10.0-53.5) kernel (ns-10.0-53.5_nc.gz)
...
...
...
Copying ns-10.0-53.5_nc.gz to /flash/ns-10.0-53.5_nc.gz ...

Installing documentation...
...
...
...
Installation has completed.

Reboot NOW? [Y/N] Y
```

To upgrade a standalone NetScaler running release 8.1, 9.0, 9.1, 9.2, 9.3 by using the configuration utility

1. In a Web browser, type the IP address of the NetScaler, such as `http://10.102.29.50`.
2. In User Name and Password, type the administrator credentials.
3. 

   In Start in, select Configuration, and then click Login, as shown in the following figure.
4. In the configuration utility, in the navigation pane, click System.
5. In the System Overview page, click Upgrade Wizard.
6. Follow the instructions to upgrade the software.
7. When prompted, select Reboot.

   Note: After the upgrade, close all browser instances and clear your computer's cache before accessing the appliance.

Upgrading a High Availability Pair

To upgrade the system software on NetScaler units in a high availability pair, you need to upgrade the software first on the secondary node and then on the primary node.

To upgrade NetScaler units in a high availability pair running release 8.1, 9.0, 9.1, 9.2, 9.3 by using the command line interface

Machine A is the primary node and machine B is the secondary node before the upgrade.

On machine B (original secondary node)

1. Follow the procedure for upgrading a standalone node as described in "Upgrading a Standalone NetScaler".

2. After the NetScaler restarts, log on using the administrator credentials and enter the show ha node command to verify that the NetScaler is a secondary node and synchronization and propagation are disabled.

   Example

```
login: nsroot
Password: nsroot
Last login: Mon Mar  26 08:37:26 2008 from 10.102.29.9
Done
show ha node
      2 nodes:
1)     Node ID:      0
      IP:       10.0.4.2
      Node State: UP
      Master State: Secondary
      ...
      Sync State: AUTO DISABLED
      Propagation: AUTO DISABLED
      ...
Done
```

   Note: Before upgrading the primary node (machine A), you have the option to test the new release by entering the force failover command on the secondary node (machine B). When you do so, machine B becomes the primary node. If machine B does not function as expected, enter the force failover command on the new primary node (machine B) forcing it to again become the secondary node, and contact Citrix Customer Service before proceeding. If machine B properly assumes the role of primary node, proceed with upgrading the former primary node (machine A).

On machine A (original primary node)

3. Follow the procedure for upgrading a standalone node as described in "Upgrading a Standalone NetScaler".

4. After the NetScaler restarts, log on using the administrator credentials and enter the show ha node command to verify that the NetScaler is a secondary node and synchronization is disabled.

On machine B (new primary node)

5. Enter the show ha node command to verify whether machine B is the primary node.

On machine A (new secondary node)

6. Enter the show ns runningconfig command to verify whether the configuration of machine A has been synchronized with that of machine B

On machine B (new primary node)

7. Enter the save ns config command to save the configuration.

Machine B (original secondary node) is now the primary node and machine A (original primary node) is now the secondary node.

To upgrade NetScaler units in a high availability pair running release 8.1, 9.0, 9.1, 9.2, 9.3 by using the configuration utility

1. Log on to the secondary node and perform the upgrade as described in "To upgrade a standalone NetScaler running release 8.0, 8.1, 9.0, 9.1, 9.2, or 9.3 by using the configuration utility:.

   Note: Before upgrading the primary node (machine A), you have the option to test the new release by entering the force failover command at the command line interface on the secondary node (machine B). When you do so, machine B becomes the primary node. If machine B does not function as expected, enter the force failover command at the command line interface on the new primary node (machine B) forcing it to again become the secondary node, and contact Citrix Customer Service before proceeding. If machine B properly assumes the role of primary node, proceed with upgrading the former primary node (machine A).

2. Log on to the primary node and perform the upgrade as described in "To upgrade a standalone NetScaler running release 8.0, 8.1, 9.0, 9.1, 9.2, or 9.3 by using the configuration utility".

Upgrading to a Later Build within Release 10

You can upgrade from an earlier 10 build to a later 10 build on a standalone NetScaler or a high availability pair. This procedure can be performed by using the configuration utility or the command line interface.

Upgrading a Standalone NetScaler to a Later Build

In the following procedure, <targetbuildnumber> is the build number that you are upgrading to within the 10 release.

To upgrade a standalone NetScaler running release 10 to a later build by using the command line interface

1. Open an SSH connection to the NetScaler by using an SSH client, such as PuTTY.

2. Log on to the NetScaler by using the administrator credentials. Save the running configuration. At the prompt, type:

   save ns config

3. Create a copy of the ns.conf file. At the shell prompt, type:

   a. cd /nsconfig

   b. cp ns.conf ns.conf.NS<releasenumber><currentbuildnumber>

   You should backup a copy of the configuration file on another computer.

4. Download or copy the installation package (build-10-<targetbuildnumber>_nc.tgz) and the documentation bundle (ns-10-<targetbuildnumber>-doc.tgz) to this directory and extract the contents of the installation package.

5. Run the installns script to install the new version of the system software.

   Note:

   To install a FIPS appliance, run the installns script with the -F option. To automatically clean up the flash, run the installns script with the -c option.

   If the configuration file for the build that you are upgrading to exists on the appliance, you are prompted to load that configuration, as shown in the following figure.

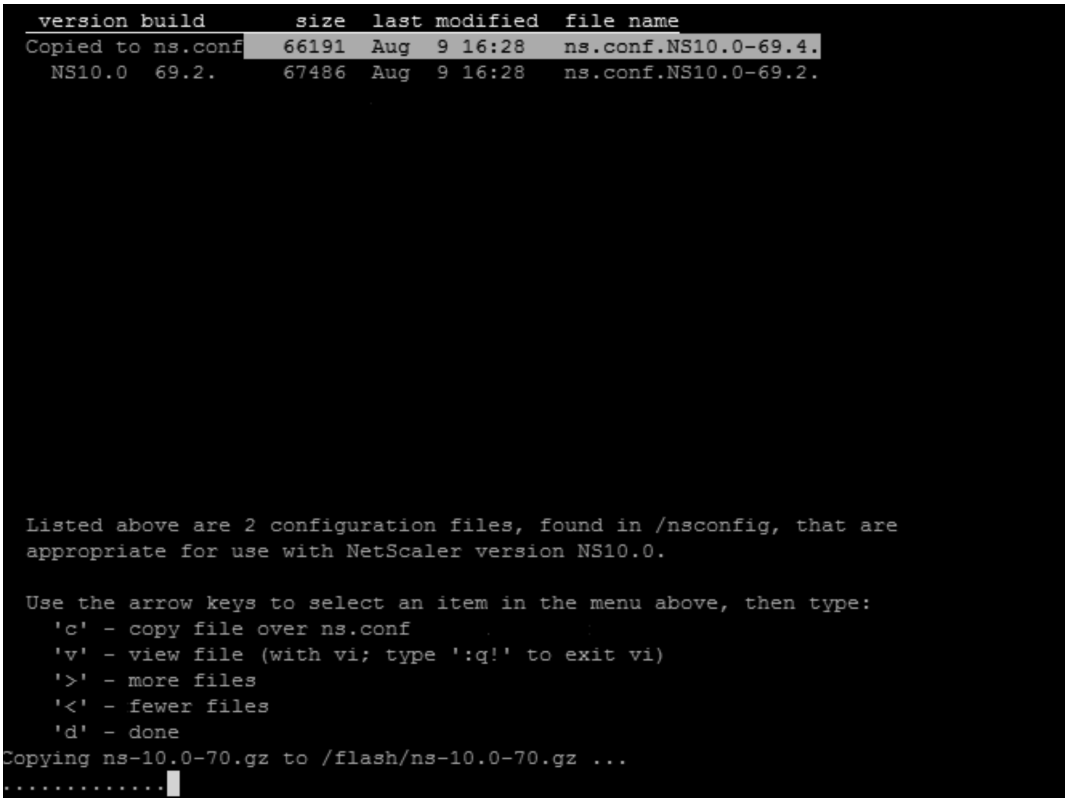


Figure 1. Upgrade menu if configuration file exists

If the free space available on the flash drive is insufficient to install the new build, the NetScaler prompts you to initiate a cleanup of the flash drive. For more information, see "Auto Cleanup".

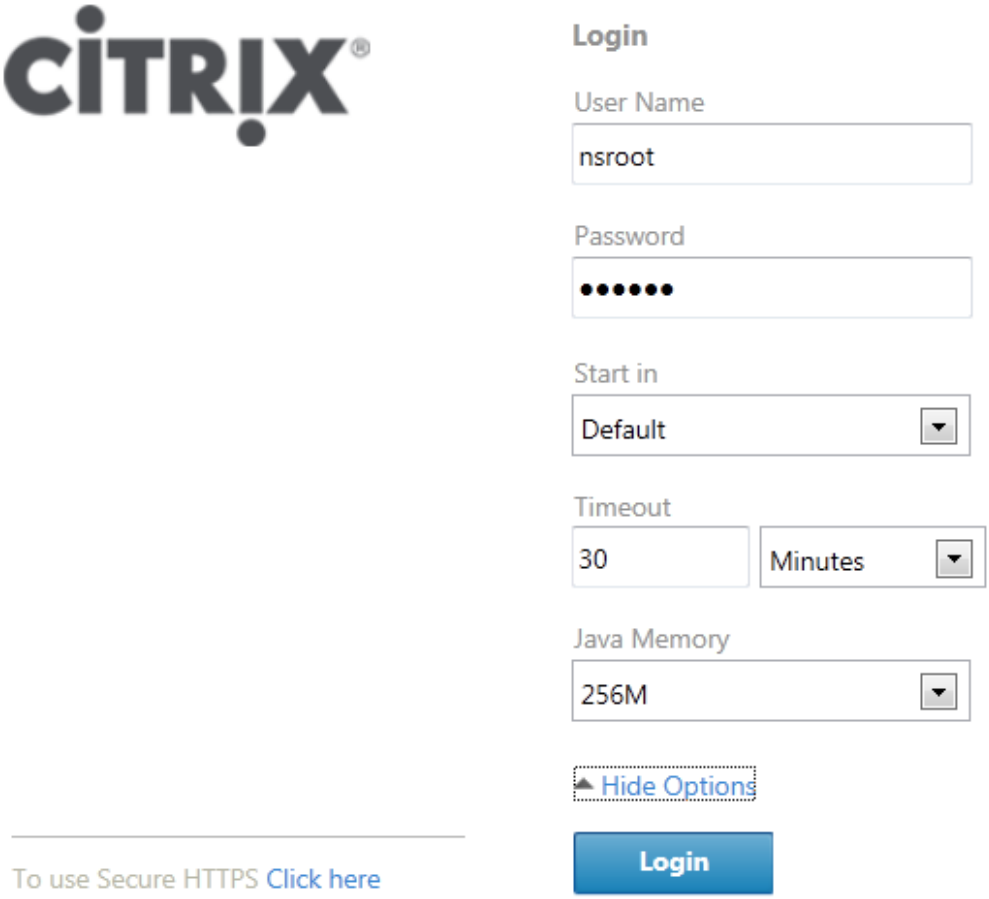
6. When prompted, restart the NetScaler.

Example

```
login: nsroot
Password:
Last login: Thu Aug  9 12:12:54 2012 from 10.144.7.22
Done
> save config
> shell
Last login: Mon Aug  9 03:51:42 from 10.103.25.64
root@NSnnn# cd /var/nsinstall
root@NSnnn# cd 10.0nsinstall
root@NSnnn# mkdir build_70
root@NSnnn# cd build_70
root@NSnnn# ftp ... get build-10.0-70_nc.tgz
root@NSnnn# get ns-10.0-70-doc.tgz
root@NSnnn# tar  build-10.0-70_nc.tgz
root@NSnnn# ./installns
installns version (10.0-70) kernel (ns-10.0-70_nc.gz)
The Netscaler version 10.0-70 checksum file is located on
http://www.mycitrix.com under Support > Downloads > Citrix NetScaler.
Select the Release 10.0-70 link and expand the "Show Documentation" link
to view the MD5 checksum file for build 10.0-70.
```

```
There may be a pause of up to 3 minutes while data is written to the flash.
Do not interrupt the installation process once it has begun....
...
...
Copying ns-10.0-70_nc.gz to /flash/ns-10.0-70_nc.gz ...
...
Installing documentation...
...
Installation has completed.

Reboot NOW? [Y/N] Y
```

To upgrade a standalone NetScaler running release 10 to a later build by using the configuration utility

1. In a Web browser, type the IP address of the NetScaler, such as `http://10.102.29.50`.
2. In User Name and Password, type the administrator credentials.
3. 

   In Start in, select Configuration, and then click Login, as shown in the following figure.
4. In the configuration utility, in the navigation pane, click System.
5. In the System Overview page, click Upgrade Wizard.
6. Follow the instructions to upgrade the software.
7. When prompted, select Reboot.

   Note: After the upgrade, close all browser instances and clear your computer's cache before accessing the appliance.

Upgrading a NetScaler High Availability Pair to a Later Build

To upgrade the system software on NetScaler units in a high availability pair, you need to upgrade the software first on the secondary node and then on the primary node.

Warning: In certain rare cases, synchronization and propagation are disabled if you upgrade only one of the nodes in an HA pair to a later build.

To determine whether synchronization and propagation are disabled, at the command line interface, type:

show ha node

Note: In an HA setup, both nodes must run NetScaler nCore or NetScaler classic. If the nodes are running NetScaler classic and you want to migrate to NetScaler nCore of the same NetScaler release, propagation and synchronization are not supported during the migration process. Once migration is complete, you have to manually enable propagation and synchronization. The same applies if you migrate from NetScaler nCore to NetScaler classic.

If synchronization and propagation are disabled, a new command added on the new primary node will not be propagated to the new secondary node. Also, if you restart the new secondary node, it will not synchronize and fetch the running configuration from the new primary node, but it will use the configuration that was last saved before the node was restarted.

To resolve this situation, upgrade both of the nodes to the same build as soon as possible and make sure that no new command is added on the new primary node when a different build is running on the new secondary node.

In the following procedure, machine A is the original primary and machine B is the original secondary node, and <targetbuildnumber> is the build number that you are upgrading to within the 10 release.

To upgrade a NetScaler high availability pair to a later build by using the command line interface

On machine B (original secondary node)

1. Open an SSH connection to the NetScaler by using an SSH client, such as PuTTY.
2. Log on to the NetScaler by using the administrator credentials. Save the running configuration. At the prompt, type:

   save config

3. Create a copy of the ns.conf file. At the shell prompt, type:

   a. cd **/nsconfig**

   b. cp **ns.conf ns.conf.NS10.0-**<currentbuildnumber>
4. Disable synchronization and propagation manually by entering the following commands in the order shown at the command line interface:

   a. set HA node -haSync DISABLED

   b. set HA node -haProp DISABLED

   c. save config

   On machine A (original primary node)

5. Open an SSH connection to the NetScaler by using an SSH client, such as PuTTY.

6. Log on to the NetScaler by using the administrator credentials.

7. Disable synchronization and propagation manually by entering the following commands in the order shown at the command line interafce:

   a. set HA node -haSync DISABLED

   b. set HA node -haProp DISABLED

   c. save config

   On machine B (original secondary node)

8. Change directory to /var/nsinstall/10nsinstall, create a directory named build_<targetbuildnumber>, and change to this directory.

9. Download or copy the installation package (build-10-<targetbuildnumber>_nc.tgz) and the documentation bundle (ns-10-<targetbuildnumber>_nc.tgz) to this directory, by using a Secure File Transfer Protocol (SFTP), and extract the contents of the installation package.

10. Run the `installns` script to install the new version of the system software.

    Note: To install a FIPS appliance, run the installns script with the -F option. To automatically clean up the flash, run the installns script with the -c option.

    If the free space available on the flash drive is insufficient to install the new build, the NetScaler prompts you to initiate a cleanup of the flash drive. For more information, see Auto Cleanup.

11. When prompted, restart the NetScaler.

12. After the NetScaler restarts, log on using the administrator credentials and enter the show ha node command to verify that the NetScaler is a secondary node.

Note: Before upgrading the primary node (machine A), you have the option to test the new build by entering the force failover command on the secondary node (machine B). When you do so, machine B becomes the primary node. If machine B does not function as expected, enter the force failover command on the new primary node (machine B) forcing it to again become the secondary node, and contact Citrix Customer Service before proceeding. If machine B properly assumes the role of primary node, proceed with upgrading the former primary node (machine A) by following steps 13 through 19.

On machine A (original primary node)

13. Follow the procedure for upgrading a standalone node.
14. After the NetScaler restarts, log on using the administrator credentials and enter the show ha node command to verify that the NetScaler is a secondary node.
15. Enable synchronization and propagation manually by entering the following commands in the order shown at the command line interface:
    a. set HA node -haSync ENABLED
    b. set HA node -haProp ENABLED
    c. save config

On machine B (new primary node)

16. Enter the show ha node command to verify that machine B is the primary node.
17. Enable synchronization and propagation by entering the following command in the order shown at the command line interface:
    a. set HA node -haSync ENABLED
    b. set HA node -haProp ENABLED
    c. save config

On machine A (new secondary node)

18. Enter the show ns runningconfig command to verify that the configuration of machine A has been synchronized with that of machine B.

On machine B (new primary node)

19. Enter the save ns config command to save the current configuration.

Machine B (original secondary node) is now the primary node and machine A (original primary node) is now the secondary node.

Downgrading from Release 10

You can downgrade to any release on a standalone NetScaler or a high availability pair by using the command line interface.

Caution: Loss in configuration may occur when downgrading. You should compare the configurations before and after the downgrade, and then manually read any missing entries.

This procedure provides steps to downgrade from release 10 to an earlier release. For downgrading to an earlier build within release 10, see "Downgrading to an Earlier Build within Release 10".

Note: Downgrading using the configuration utility is not supported.

Downgrading a Standalone NetScaler

In the following procedure, <release> and <releasenumber> represent the release version you are downgrading to, and <targetbuildnumber> represents the build number that you are downgrading to. Refer to the table below for specific values.

Table 1. Release Version Values

Release Version	<release>	<releasenumber>
9.3	9.3	9.3
9.2	9.2	9.2
9.1	9.1	9.1
8.1	rhodes	8.1
8.0	andes	8.0
7.0	sierra	7.0

To downgrade a standalone NetScaler

1. Open an SSH connection to the NetScaler by using an SSH client, such as PuTTY.

2. Log on to the NetScaler by using the administrator credentials. Save the running configuration. At the prompt, type:

   save config

3. Create a copy of the ns.conf file. At the shell prompt, type:

   a. cd /nsconfig

   b. cp ns.conf ns.conf.NS10<currentbuildnumber>

   You should backup a copy of the configuration file on another computer.

4. Copy the <releasenumber> configuration file (ns.conf.NS<releasenumber>) to ns.conf. At the shell prompt, type:

   cp **ns.conf.NS**<releasenumber> **ns.conf**

   Note: ns.conf.NS<releasenumber> is the backup configuration file that is automatically created when the system software is upgraded from release version <releasenumber> to the current release version. There may be some loss in configuration when downgrading. After the appliance restarts, compare the configuration saved in step 3 with the running configuration, and make any adjustments for features and entities configured before the downgrade. Save the running configuration after making the changes.

   Important: If routing is enabled, perform step 5. Otherwise, skip to step 6.

5. If routing is enabled, the ZebOS.conf file will contain the configuration. At the shell prompt, type:

   a. cd **/nsconfig**

   b. cp **ZebOS.conf ZebOS.conf.NS**10

   c. cp ZebOS.conf.NS<targetreleasenumber> ZebOS.conf

6. Change directory to /var/nsinstall/<releasenumber>nsinstall, or create one if it does not exist.

7. Change directory to build_<targetbuildnumber>, or create one if it does not exist.

8. Download or copy the installation package (build-<release>-<targetbuildnumber>.tgz) and the documentation bundle (ns-<releasenumber>-<targetbuildnumber>-doc.tgz) to this directory and extract the contents of the installation package.

9. Run the `installns` script to install the new version of the system software.

   If the configuration file for the build that you are downgrading to exists on the appliance, you are prompted to load that configuration, as shown in the following figure.

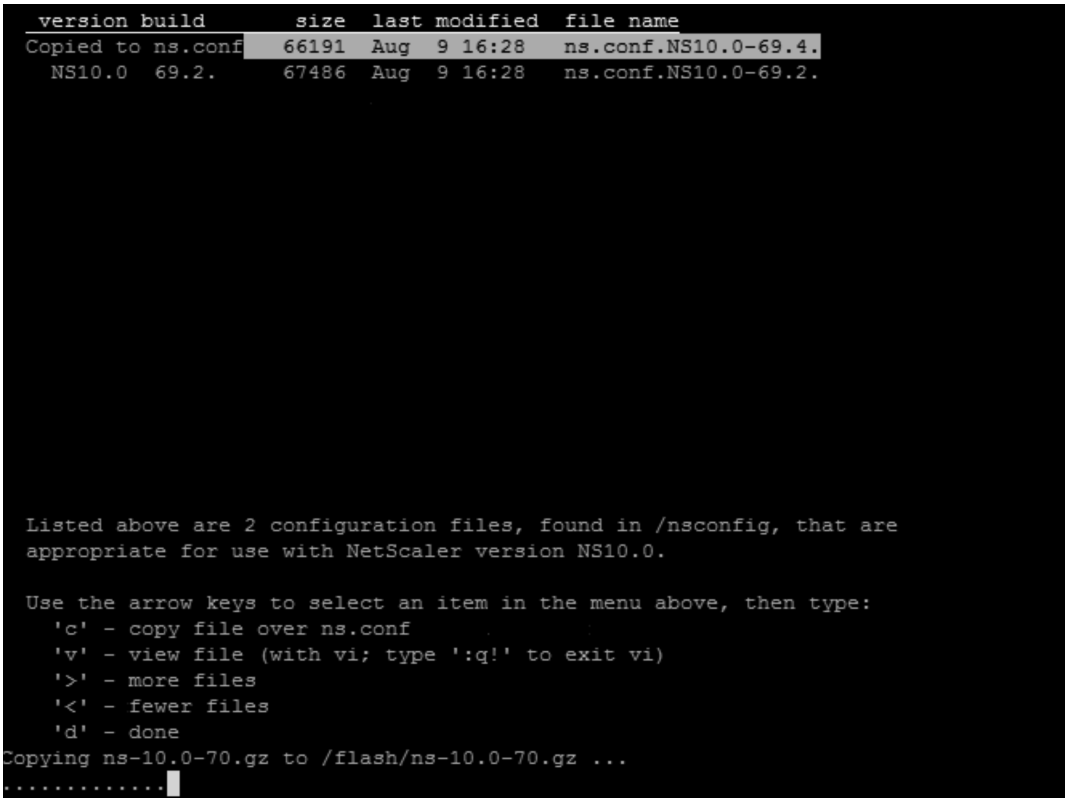


Figure 1. Downgrade menu if configuration file exists

If the free space available on the flash drive is insufficient to install the new build, the NetScaler prompts you to initiate a cleanup of the flash drive. For more information, see "Auto Cleanup".

10. When prompted, restart the NetScaler.

Example

login: nsroot
Password: nsroot
Last login: Tue Mar 27 01:38:25 2008 from 10.102.29.9
Done
> save config
> shell
Last login: Tue Mar 27 02:07:06 from 10.103.25.64
root@NSnnn# cp ns.conf.NS9.3 ns.conf
root@NSnnn# cd /var/nsinstall
root@NSnnn# mkdir 9.3nsinstall
root@NSnnn# cd 9.3nsinstall
root@NSnnn# mkdir build_55
root@NSnnn# cd build_55
root@NSnnn# ftp ... get build_93_55_nc.tgz
root@NSnnn# get ns-9.3-55-doc.tgz
root@NSnnn# tar xzvf build_93_55_nc.tgz
root@NSnnn# ./installns
installns version (9.3-55) kernel (ns-9.3-55.gz)
...
...

```
...
Copying ns-9.3-55.gz to /flash/ns-9.3-55_nc.gz ...
Changing /flash/boot/loader.conf for ns-9.3-55 ...
Installing documentation...

Installation has completed.

Reboot NOW? [Y/N] Y
```

Downgrading a High Availability Pair

To downgrade the system software on NetScaler units in a high availability pair, you need to downgrade the software first on the secondary node and then on the primary node. For instructions on downgrading each node separately, see "Downgrading a Standalone NetScaler".

Downgrading to an Earlier Build within Release 10

You can downgrade from a later 10 build to an earlier 10 build on a standalone NetScaler or a high availability pair. This procedure must be performed by using the command line interface.

Note: Loss in configuration may occur when downgrading. You should compare the configurations before and after the downgrade, and then manually read any missing entries.

Downgrading a Standalone NetScaler to an Earlier Build

In the procedure below, <targetbuildnumber> is the build number that you are downgrading to within the same release.

To downgrade a standalone NetScaler to an earlier build

1. Open an SSH connection to the NetScaler by using an SSH client, such as PuTTY.
2. Log on to the NetScaler by using the administrator credentials. Save the running configuration. At the prompt, type:

   save ns config

   Caution: If ns.conf.NS10-<targetbuildnumber> does not exist, loss in configuration may occur when downgrading to an earlier build. The errors and warnings appear only on the console. Please watch the console closely for these errors and warnings. After the appliance restarts, compare the configuration saved in step 3 with the running configuration, and make any adjustments for features and entities configured before the downgrade. Save the running configuration after making the changes.
3. Change directory to /var/nsinstall/10nsinstall.
4. Change directory to build_<targetbuildnumber>, or create one if it does not exist.
5. Run the installns script to install the old version of the system software.

   If the configuration file for the build that you are downgrading to exists on the appliance, you are prompted to load that configuration, as shown in the following figure.

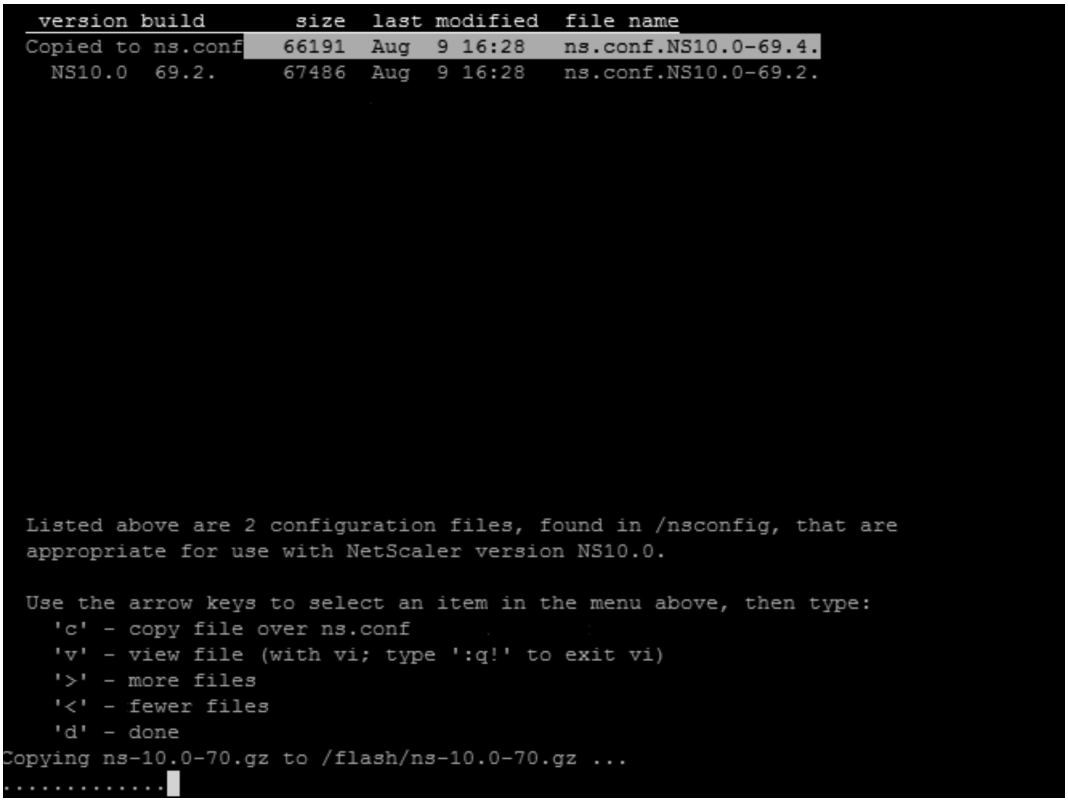


Figure 1. Downgrade menu if configuration file exists

If the free space available on the flash drive is insufficient to install the new build, the NetScaler prompts you to initiate a cleanup of the flash drive. For more information, see "Auto Cleanup".

6. When prompted, restart the NetScaler.

Example

```
login: nsroot
Password: nsroot
Last login: Sun Aug  5 08:38:25 2008 from 10.102.29.4
Done
> save ns config
> shell
Last login: Sun Aug  5 09:07:06 from 10.103.25.64
root@NSnnn# cp ns.conf.NS10.0-69.4 ns.conf
root@NSnnn# cd /var/nsinstall
root@NSnnn# cd 10nsinstall
root@NSnnn# cd build_69_4
root@NSnnn# ftp ... get build-10-69.4_nc.tgz
root@NSnnn# get ns-10.0-69.4-doc.tgz
root@NSnnn# tar xzvf build-10.0-69.4_nc.tgz
root@NSnnn# ./installns
installns version (10.0-69.4) kernel (ns-10.0-69.4.gz)
...
...
...
Copying ns-10.0-69.4_nc.gz to /flash/ns-10.0-69.4_nc.gz ...
Changing /flash/boot/loader.conf for ns-10.0-69.4 ...
Installing documentation...

Installation has completed.

Reboot NOW? [Y/N] Y
```

Downgrading a NetScaler High Availability Pair to an Earlier Build

To downgrade the system software on NetScaler units in a high availability pair, you need to downgrade the software first on the secondary node and then on the primary node. For instructions on downgrading each node separately, see "Downgrading a Standalone NetScaler to an Earlier Build".

Note: Note: In an HA setup, both nodes must run NetScaler nCore or NetScaler classic. If the nodes are running NetScaler classic and you want to migrate to NetScaler nCore of the same NetScaler release, propagation and synchronization are not supported during the migration process. Once migration is complete, you have to manually enable propagation and synchronization. The same applies if you migrate from NetScaler nCore to NetScaler classic.

Auto Cleanup

The cleanup procedure has been simplified in the later versions of release 7.0 (build 48 and later) and in releases 8.0, 8.1, 9.0, 9.1, 9.2, 9.3, and 10. You no longer have to manually delete build files from the flash drive. During the installation process, if the free space on the flash drive is found to be insufficient, the NetScaler prompts you to initiate the cleanup process.

Note: To automatically clean up the flash, run the installns script with the -c option.

When downgrading to release 7.0, the prompt looks like this:

```
Installation path for kernel will be /flash
Size of kernel ns-7.0-21.7.gz is 58003.323 kilobytes
Available space on /flash/ filesystem is 25075 kilobytes
Available space on /flash/ filesystem is insufficient to install ns-7.0-21.7.gz
Do you want Auto Cleanup [Y/N] ?
```

When upgrading to release 8.1, the prompt looks like this:

```
Installation path for kernel is /flash
Size of kernel ns-8.1-32.2.gz is 61062.235 kilobytes
Available space on /flash/ filesystem is 59108 kilobytes
Available space on /flash/ filesystem is insufficient to install ns-8.1-32.2.gz
Do you want installns to free space by archiving older releases? [Y/ N]
```

To initiate the cleanup process, press Y. Messages similar to the following appear:

```
Archiving older releases ...
  Creating the archive directory /var/nsbackup/ns_2007_2_16_1_6_26 ...
  Move //flash//ns-6.1-97.4.m.gz /var/nsbackup/ ns_2007_2_16_1_6_26ns-6.1-97.4.m.gz ...
  Move //flash//ns-8.1-32.2.gz /var/nsbackup/ns_2007_2_16_1_6_26ns-8.1-32.2.gz ...
Archive operation completed, free space is 156452, required space is 61062.235
```

The installation process automatically continues after successful completion of the cleanup.

API

2015-05-18 16:58:20 UTC

Contents

API

The following topics provides information on the API support provided for the NetScaler appliance. Intended for application developers who want to configure and monitor a NetScaler appliance programmatically.

NITRO API	Describes the use of the NITRO APIs for the REST, Java, and .NET platforms.
XML API	Describes the properties and use of the XML API.

NITRO API

The NetScaler NITRO protocol allows you to configure and monitor the NetScaler appliance programmatically.

NITRO exposes its functionality through Representational State Transfer (REST) interfaces. Therefore, NITRO applications can be developed in any programming language. Additionally, for applications that must be developed in Java or .NET, NITRO APIs are exposed through relevant libraries that are packaged as separate Software Development Kits (SDKs).

Note: You must have a basic understanding of the NetScaler appliance before using NITRO.

To use the NITRO protocol, the client application needs only the following:

- Access to a NetScaler appliance, version 9.2 or later.
- To use REST interfaces, you must have a system to generate HTTP or HTTPS requests (payload in JSON format) to the NetScaler appliance. You can use any programming language or tool.
- For Java clients, you must have a system where Java Development Kit (JDK) 1.5 or later is available. The JDK can be downloaded from http://www.oracle.com/technetwork/java/javase/downloads/index.html.
- For .NET clients, you must have a system with .NET framework 3.5 or later installed. The .NET framework can be downloaded from http://www.microsoft.com/downloads/en/default.aspx.

Note: You can also use XML APIs to configure the NetScaler appliance programmatically. For more information, see "XML API".

NITRO API

The NetScaler NITRO protocol allows you to configure and monitor the NetScaler appliance programmatically.

NITRO exposes its functionality through Representational State Transfer (REST) interfaces. Therefore, NITRO applications can be developed in any programming language. Additionally, for applications that must be developed in Java or .NET, NITRO APIs are exposed through relevant libraries that are packaged as separate Software Development Kits (SDKs).

Note: You must have a basic understanding of the NetScaler appliance before using NITRO.

To use the NITRO protocol, the client application needs only the following:

- Access to a NetScaler appliance, version 9.2 or later.
- To use REST interfaces, you must have a system to generate HTTP or HTTPS requests (payload in JSON format) to the NetScaler appliance. You can use any programming language or tool.
- For Java clients, you must have a system where Java Development Kit (JDK) 1.5 or later is available. The JDK can be downloaded from http://www.oracle.com/technetwork/java/javase/downloads/index.html.
- For .NET clients, you must have a system with .NET framework 3.5 or later installed. The .NET framework can be downloaded from http://www.microsoft.com/downloads/en/default.aspx.

Note: You can also use XML APIs to configure the NetScaler appliance programmatically. For more information, see "XML API".

Obtaining the NITRO Package

The NITRO package is available as a tar file on the Downloads page of the NetScaler appliance's configuration utility. You must download and un-tar the file to a folder on your local system. This folder is referred to as <NITRO_SDK_HOME> in this documentation.

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

Note:

- The REST package contains only documentation for using the REST interfaces.

How NITRO Works

The NITRO infrastructure consists of a client application and the NITRO Web service running on a NetScaler appliance. The communication between the client application and the NITRO web service is based on REST architecture using HTTP or HTTPS.

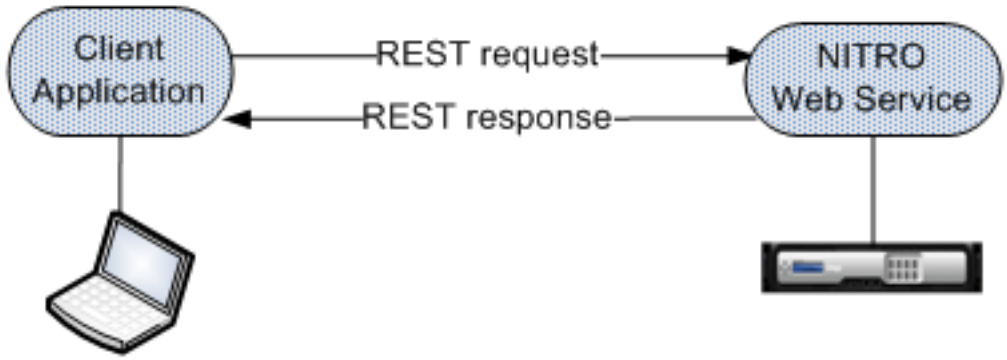


Figure 1. NITRO execution flow

As shown in the above figure, a NITRO request is executed as follows:

1. The client application sends REST request message to the NITRO web service. When using the SDKs, an API call is translated into the appropriate REST request message.

2. The web service processes the REST request message.

3. The NITRO web service returns the corresponding REST response message to the client application. When using the SDKs, the REST response message is translated into the appropriate response for the API call.

To minimize traffic on the NetScaler network, you retrieve the whole state of a resource from the server, make modifications to the state of the resource locally, and then upload it back to the server in one network transaction. For example, to update a load balancing virtual server, you must retrieve the object, update the properties, and then upload the changed object in a single transaction.

Note: Local operations on a resource (changing its properties) do not affect its state on the server until the state of the object is explicitly uploaded.

NITRO APIs are synchronous in nature. This means that the client application waits for a response from the NITRO web service before executing another NITRO API.

Java API

NetScaler NITRO APIs are categorized depending on the scope and purpose of the APIs into system APIs, feature configuration APIs, and feature statistics APIs. Additionally, you can import and export AppExpert applications. You can also troubleshoot NITRO operations.

Tutorials

These tutorials demonstrate the end-to-end usage of NITRO to achieve the following:

- Create Your First NITRO Application
- Create a NetScaler Cluster

Create Your First NITRO Application

After completing this tutorial, you will understand and be able to perform the following tasks:

- Integrate NITRO with the IDE
- Log in to the appliance
- Create a load balancing virtual server (lbvserver)
- Retrieve details of an lbvserver
- Delete an lbvserver
- Save the configurations on the appliance
- Log out of the appliance
- Debug the NITRO application

Before you begin, make sure that you have the latest NITRO SDK and that the client application satisfies the prerequisites for using the NITRO SDK.

Sample Code

For the executable code, see the <NITRO_SDK_HOME>/sample/MyFirstNitroApplication.java sample file.

To create your first NITRO application:

1. Copy the libraries from <NITRO_SDK_HOME>/lib folder to the project classpath.

2. Create a new class and name it **MyFirstNitroApplication**.

3. Create an instance of `com.citrix.netscaler.nitro.service.nitro_service` class. This instance is used to perform all operations on the appliance:

   ```
   nitro_service ns_session = new nitro_service("10.102.29.170","HTTP");
   ```

   This code establishes a connection with an appliance that has IP address 10.102.29.170 and uses the HTTP protocol. Replace 10.102.29.170 with the IP address of the NetScaler appliance that you have access to.
4. Use the `nitro_service` instance to log in to the appliance using your credentials:

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

   This code logs into the appliance, with user name as `admin` and password as `verysecret`. Replace the credentials with your login credentials.
5. Enable the load balancing feature:

   ```
   String[] features_to_be_enabled = {"lb"};
   ns_session.enable_features(features_to_be_enabled);
   ```

   This code first sets the features to be enabled in an array and then enables the LB feature.
6. Create an instance of the `com.citrix.netscaler.nitro.resource.config.lb.lbvserver` class. You will use this instance to perform operations on the lbvserver.

   ```
   lbvserver new_lbvserver_obj = new lbvserver();
   ```

7. Use the `lbvserver` instance to create a new lbvserver:

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

   This code first sets the attributes (name, IP address, service type, port, and load balancing method) of the lbvserver locally and then adds it to the appliance by using the corresponding `add()` method.
8. Retrieve the details of the lbvserver you have created:

   ```
   new_lbvserver_obj = lbvserver.get(ns_session,new_lbvserver_obj.get_name());
   System.out.println("Name : " +new_lbvserver_obj.get_name() +"\n" +"Protocol : " +new_lbvserver_obj.ge
   ```

   This code first retrieves the details of the lbvserver as an object from the NetScaler, extracts the required attributes (name and service type) from the object, and displays the results.
9. Delete the lbvserver you created in the above steps:

```
lbvserver.delete(ns_session, new_lbvserver_obj.get_name());
```

10. Save the configurations:

```
ns_session.save_config();
```

11. Log out of the appliance:

```
ns_session.logout();
```

Debug the NITRO application

All NITRO exceptions are captured by the `com.citrix.netscaler.nitro.exception.nitro_exception` class. For a more detailed description, see Exception Handling.

Create a NetScaler Cluster

After completing this tutorial you will be able to create a two-node NetScaler cluster. To add more appliances to the cluster you must repeat the procedure that adds and joins the node to the cluster.

Sample Code

For the executable code, see the <NITRO_SDK_HOME>/sample/CreateCluster.java sample file.

To create a cluster

1. Copy the libraries from <NITRO_SDK_HOME>/lib folder to the project classpath.

2. Create a new class and name it CreateCluster.

3. Log on to one of the appliances that you want to add to the cluster and create a cluster:

   ```
   //Connect to the first appliance that you want to add to the cluster
   nitro_service nonClipSession0 = new nitro_service(nsipAddress0,protocol);
   nonClipSession0.login(uName,password);

   //Create a cluster instance
   clusterinstance newClusterInstance = new clusterinstance();
   newClusterInstance.set_clid(1);
   clusterinstance.add(nonClipSession0,newClusterInstance);

   //Add the appliance to the cluster
   clusternode ClusterNode0 = new clusternode();
   ClusterNode0.set_nodeid(0);
   ClusterNode0.set_ipaddress(nsipAddress0);
   ClusterNode0.set_state("ACTIVE");
   ClusterNode0.set_backplane("0/1/1");
   clusternode.add(nonClipSession0,ClusterNode0);

   //Add the cluster IP address
   nsip newNSIPAddress = new nsip();
   newNSIPAddress.set_ipaddress(clipAddress);
   newNSIPAddress.set_netmask("255.255.255.255");
   newNSIPAddress.set_type("CLIP");
   nsip.add(nonClipSession0,newNSIPAddress);

   //Enable the cluster instance
   clusterinstance.enable(nonClipSession0, newClusterInstance);

   //Save the configurations
   nonClipSession0.save_config();

   //Warm reboot the appliance
   nonClipSession0.reboot(true);
   ```

   The cluster is created and the first node is added to the cluster. This node becomes the initial configuration coordinator of the cluster.

4. Log on to the cluster IP address to add other appliances to the cluster:

   ```
   //Connect to the cluster IP address
   nitro_service clipSession = new nitro_service(clipAddress,protocol);
   clipSession.login(uName,password);

   //Add the node to the cluster
   clusternode ClusterNode1 = new clusternode();
   ClusterNode1.set_nodeid(1);
   ClusterNode1.set_ipaddress(nsipAddress1);
   ```

```
ClusterNode1.set_state("ACTIVE");
ClusterNode1.set_backplane("1/1/1");
clusternode.add(clipSession,ClusterNode1);

//Save the configurations
clipSession.save_config();
```

5. Log on to the appliance that you added in the previous step and join it to the cluster:

```
//Connect to the node that you have just added to the cluster
nitro_service nonClipSession1 = new nitro_service(nsipAddress1,protocol);
nonClipSession1.login(uName,password);

//Join the node to the cluster
cluster newCluster = new cluster();
newCluster.set_clip(clipAddress);
newCluster.set_password(password);
cluster.join(nonClipSession1,newCluster);

//Save the configurations
nonClipSession1.save_config();

//Warm reboot the appliance
nonClipSession1.reboot(true);
```

   The second node is now a part of the cluster.

6. Verify the details of the cluster by logging on to the cluster IP address

```
//Retrieving the cluster node details
Long id = new Long(1);
clusternode node= clusternode.get(clipSession, id);
System.out.println("Node ID: "+ node.get_nodeid() + " | Admin state: " + node.get_state() + " | Backplane

//Retrieving the cluster instance details
Long id1 = new Long(1);
clusterinstance instance= clusterinstance.get(clipSession, id1);
System.out.println("Cluster instance ID: "+ instance.get_clid() + " | Operational state: " +instance.get_op
```

System APIs

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

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

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

The following sample code establishes a session with a NetScaler appliance with IP address 10.102.29.60 by using the HTTPS protocol:

```
//Specify the NetScaler appliance IP address and protocol
nitro_service ns_session = new nitro_service("10.102.29.60","https");

//Specify the login credentials
ns_session.login("admin","verysecret");
```

Note: When using HTTPS, you must make sure that the root CA is added to the truststore. By default, NITRO validates the SSL certificate and verifies the hostname. To disable this validation, use the following:

```
ns_session.set_certvalidation(false);
ns_session.set_hostnameverification(false);
```

Note: By default, the connection to the appliance expires after 30 minutes of inactivity. You can modify the timeout period by specifying a new timeout period (in seconds) in the `login` method. For example, to modify the timeout period to 60 minutes:

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

You must use the `nitro_service` object in all further NITRO operations on the appliance. For example to save the configurations on the appliance, you must use the `nitro_service` object as follows:

```
ns_session.save_config();
```

The `nitro_service` class also provides APIs to perform other system-level operations such as enabling and disabling NetScaler features and modes, saving and clearing NetScaler configurations, setting the session timeout, setting the severity of the exceptions to be handled, setting the behavior of bulk operations, and disconnecting from the appliance.

Feature Configuration APIs

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

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

Each NetScaler resource is represented by a class. For example, the class that represents a load balancing virtual server is called `lbvserver` (in `com.citrix.netscaler.nitro.resource.config.lb`). The state of a resource is represented by properties of a class. You can set the value for these properties by using the `set_<propertyname>()` methods provided by the resource class. For example to set the IP address of a load balancing virtual server, the lbvserver class provides the `set_ipv46()` method. Similarly, you can get the value of these properties by using the `get_<propertyname>()` methods of the resource class.

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

A resource class provides APIs to perform the following operations:

Create | Retrieve | Update | Delete | Enable/Disable | Unset | Bind/Unbind | Global bind | Bulk operations

Create

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

The following sample code creates a load balancing virtual server:

```
//Create an instance of the lbvserver class
lbvserver new_lbvserver_obj = new lbvserver();

//Set the properties of the resource locally
new_lbvserver_obj.set_name("MyFirstLbVServer");
new_lbvserver_obj.set_ipv46("10.102.29.88");
new_lbvserver_obj.set_port(88);
new_lbvserver_obj.set_servicetype("HTTP");
new_lbvserver_obj.set_lbmethod("ROUNDROBIN");

//Upload the resource to NetScaler
lbvserver.add(ns_session,new_lbvserver_obj);
```

Retrieve

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

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

```
//Retrieve the resource object from the NetScaler
new_lbvserver_obj = lbvserver.get(ns_session,"MyFirstLbVServer");

//Extract the properties of the resource from the object locally
System.out.println(new_lbvserver_obj.get_name());
System.out.println(new_lbvserver_obj.get_servicetype());
```

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

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

```
filtervalue[] filter = new filtervalue[2];
filter[0] = new filtervalue("port","80");
filter[1] = new filtervalue("servicetype","HTTP");
lbvserver[] result = lbvserver.get_filtered(ns_session,filter);
```

You can also retrieve all NetScaler resources of a certain type, such as all services in the NetScaler appliance, by calling the static `get()` method on the service class, without providing a second parameter, as follows:

```
service[] resources = service.get(ns_session);
```

Update

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

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

```
//Create an instance of the lbvserver class
lbvserver update_lb = new lbvserver();

//Specify the name of the lbvserver to be updated
update_lb.set_name("MyFirstLbVServer");

//Specify the updated service type and lb method
update_lb.set_servicetype("https");
update_lb.set_lbmethod("LEASTRESPONSETIME");

//Upload the resource to NetScaler
lbvserver.update(ns_session,update_lb);
```

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

Delete

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

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

```
lbvserver remove_lb = new lbvserver();
remove_lb.set_name("MyFirstLbVServer");
lbvserver.delete(ns_session, remove_lb);
```

Enable/Disable

To enable a resource, invoke the `enable()` method.

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

```
lbvserver obj = new lbvserver();
obj.set_name = "lb_vip";
lbvserver.enable(ns_session, obj);
```

Note: To disable a resource, invoke the `disable()` method.

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

Unset

To unset the value that is set to a parameter, invoke the `unset()` method on the resource class, by passing the name of the resource and the parameters to be unset. If the parameter has a default value, the value is reset to that value.

The following sample code unsets the load balancing method and the comments of a load balancing virtual server named "lb_123":

```
lbvserver lb1 = new lbvserver();
lb1.set_name("lb_123");
String args[] = {"comment", "lbmethod"};
lbvserver.unset(ns_session, lb1, args);
```

Bind/Unbind

NetScaler resources form relationships with each other through the process of binding. This is how services are associated with a load balancing virtual server (by binding them to it), or how various policies are bound to a load balancing virtual server. Each binding relationship is represented in NITRO by its own class.

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

Binding classes have a property representing the name of each resource in the binding relationship. They can also have other properties related to that relationship (for example, the weight of the binding between a load balancing virtual server and a service).

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

```
lbvserver_service_binding bindObj = new lbvserver_service_binding();
bindObj.set_name("MyFirstLbVServer");
bindObj.set_servicename("svc_prod");
bindObj.set_weight(20);
lbvserver_service_binding.add(ns_session,bindObj);
```

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

The following code sample unbinds a service from a server:

```
lbvserver_service_binding bindObj = new lbvserver_service_binding();
bindObj.set_name("MyFirstLbVServer");
bindObj.set_servicename("svc_prod");
lbvserver_service_binding.delete(ns_session,bindObj);
```

Global bind

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

Some NITRO classes can be used to bind resources globally. These classes have names that follow the following pattern: `<featurename>global_<resourcetype>_binding`.

For example, the class `aaaglobal_preauthenticationpolicy_binding` is used to bind preauthentication policies globally.

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

```
aaapreauthenticationaction preauth_act1;
aaapreauthenticationpolicy preauth_pol1;
aaaglobal_aaapreauthenticationpolicy_binding glob_binding;
preauth_act1 = new aaapreauthenticationaction();
preauth_act1.set_name("preauth_act1");
preauth_act1.set_preauthenticationaction("ALLOW");
aaapreauthenticationaction.add(ns_session,preauth_act1);
```

```
preauth_pol1 = new aaapreauthenticationpolicy();
preauth_pol1.set_name("preauth_pol1");
preauth_pol1.set_rule("CLIENT.APPLICATION.PROCESS(antivirus.exe) EXISTS");
preauth_pol1.set_reqaction("preauth_act1");
aaapreauthenticationpolicy.add(ns_session,preauth_pol1);

glob_binding = new aaaglobal_aaapreauthenticationpolicy_binding();
glob_binding.set_policy("preauth_pol1");
glob_binding.set_priority(200);
aaaglobal_aaapreauthenticationpolicy_binding.add(ns_session,glob_binding);
```

Bulk operations

You can create, retrieve, update, and delete multiple resources simultaneously and thus minimize network traffic. For example, you can add multiple load balancing virtual servers in the same operation. To perform a bulk operation, you instantiate an array of the resource class, configure the properties of all the instances locally, and then upload all the instances to the NetScaler with one command.

To account for the failure of some operations within the bulk operation, NITRO allows you to configure one of the following behaviors:

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

Note: You must configure the required behavior while establishing a connection with the appliance.

```
nitro_service ns_session = new nitro_service("10.102.29.60","http");
ns_session.set_onerror(OnerrorEnum.CONTINUE);
ns_session.login("admin","verysecret");
```

The following sample code creates two load balancing virtual servers:

```
//Create an array of lbvserver instances
lbvserver[] lbs = new lbvserver[2];

//Specify properties of the first lbvserver
lbs[0] = new lbvserver();
lbs[0].set_name("lbvserv1");
lbs[0].set_servicetype("http");
lbs[0].set_ipv46("10.70.136.5");
lbs[0].set_port(80);

//Specify properties of the second lbvserver
lbs[1] = new lbvserver();
lbs[1].set_name("lbvserv2");
```

```
lbs[1].set_servicetype("https");
lbs[1].set_ipv46("10.70.136.5");
lbs[1].set_port(443);

//Upload the properties of the two lbvservers to the NetScaler
lbvserver.add(ns_session,lbs);
```

Cluster APIs

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

Cluster Instance Operations

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

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

```
clusterinstance new_cl_inst_obj = new clusterinstance();
//Set the properties of the cluster instance locally
new_cl_inst_obj.set_clid(1);
new_cl_inst_obj.set_preemption("ENABLED");

//Upload the cluster instance
clusterinstance.add(ns_session,new_cl_inst_obj);
```

Cluster Node Operations

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

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

```
clusternode new_cl_node_obj = new clusternode();
//Set the properties of the cluster node locally
new_cl_node_obj.set_nodeid(0);
new_cl_node_obj.set_ipaddress("10.102.29.60");
new_cl_node_obj.set_state("ACTIVE");
new_cl_node_obj.set_backplane("0/1/1");

//Upload the cluster node
clusternode.add(ns_session,new_cl_node_obj);
```

Add a Cluster IP Address

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

The following sample code configures a cluster IP address on NetScaler appliance with IP address 10.102.29.60:

```
nsip new_nsip_obj = new nsip();
//Set the properties locally
new_nsip_obj.set_ipaddress("10.102.29.61");
new_nsip_obj.set_netmask("255.255.255.255");
new_nsip_obj.set_type("CLIP");

//Upload the cluster node
nsip.add(ns_session,new_nsip_obj);
```

Add a Spotted IP Address

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

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

```
nsip new_nsip_obj = new nsip();
//Set the properties locally
new_nsip_obj.set_ipaddress("10.102.29.77");
new_nsip_obj.set_netmask("255.255.255.0");
new_nsip_obj.set_type("SNIP");
new_nsip_obj.set_ownernode(1);

//Upload the cluster node
nsip.add(ns_session,new_nsip_obj);
```

Join NetScaler Appliance to Cluster

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

The following sample joins a NetScaler appliance to a cluster:

```
cluster new_cl_obj = new cluster();
//Set the properties of the cluster  locally
new_cl_obj.set_clip("10.102.29.61");
new_cl_obj.set_password("verysecret");

//Upload the cluster
cluster.add(ns_session,new_cl_obj);
```

Linkset Operations

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

To configure a linkset, do the following:

1. Add a linkset by invoking the `add()` method of the `linkset` class.

2. Bind the interfaces to the linkset using the `add()` method of the `linkset_interface_binding` class.

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

```
//Create the linkset
linkset new_linkset_obj = new linkset();
new_linkset_obj.set_id("LS/1");
linkset.add(ns_session,new_linkset_obj);

//Bind the interfaces to the linkset
linkset_interface_binding new_linkif_obj = new linkset_interface_binding();
new_linkif_obj.set_id("LS/1");
new_linkif_obj.set_ifnum("1/1/2 2/1/2");
linkset_interface_binding.add(ns_session,new_linkif_obj);
```

Feature Statistics APIs

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

The APIs to retrieve statistics of NetScaler features are available in packages that have the following pattern: `com.citrix.netscaler.nitro.resource.stat.<feature>`.

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

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

```
lbvserver_stats stats = lbvserver_stats.get(ns_session,"MyFirstLbVServer");
System.out.println(stats.get_curclntconnections());
System.out.println(stats.get_deferredreqrate());
```

Note: Not all NetScaler features and resources have statistic objects associated with them.

AppExpert Application APIs

To export an AppExpert application, you must instantiate the `com.citrix.netscaler.nitro.resource.config.app.application` class, configure the properties of the AppExpert locally, and then export the AppExpert application.

The following sample code exports an AppExpert application named "MyApp1":

```
application myapp = new application();
myapp.set_appname("MyApp1");
myapp.set_apptemplatefilename("myapp_template");
application.export(ns_session,myapp);
```

You can also import an AppExpert application. You must instantiate the `com.citrix.netscaler.nitro.resource.config.app.application` class, configure the properties of the AppExpert locally, and then import the AppExpert application.

The following sample code imports an AppExpert application named "MyApp1":

```
application myapp = new application();
myapp.set_appname("MyApp1");
myapp.set_apptemplatefilename("myapp_template");
application.Import(ns_session,myapp);
```

Exception Handling

The status of a NITRO request is captured in the `com.citrix.netscaler.nitro.exception.nitro_exception` class. This class provides the following details of the exception:

- **Session ID.** The session in which the exception occurred.
- **Severity.** The severity of the exception: error or warning. By default, only errors are captured. To capture warnings, you must set the warning flag to true, while connecting to the appliance.
- **Error code.** The status of the NITRO request. An error code of 0 indicates that the NITRO request is successful. A non-zero error code indicates an error in processing the NITRO request.
- **Error message.** Provides a brief description of the exception.

For a list of error codes, see the errorlisting.html file available in the <NITRO_SDK_HOME>/doc/api_reference folder.

.NET API

NetScaler NITRO APIs are categorized depending on the scope and purpose of the APIs into system APIs, feature configuration APIs, and feature statistics APIs. Additionally, you can import and export AppExpert applications. You can also troubleshoot NITRO operations.

Tutorials

These tutorials demonstrate the end-to-end usage of NITRO to achieve the following:

- Create Your First NITRO Application
- Create a NetScaler Cluster

Create Your First NITRO Application

After completing this tutorial, you will understand and be able to perform the following tasks:

- Integrate NITRO with the IDE
- Log in to the appliance
- Create a load balancing virtual server (lbvserver)
- Retrieve details of an lbvserver
- Delete an lbvserver
- Save the configurations on the appliance
- Log out of the appliance
- Debug the NITRO application

Before you begin, make sure that you have the latest NITRO SDK and that the client application satisfies the prerequisites for using the NITRO SDK.

Sample Code

For the executable code, see the <NITRO_SDK_HOME>/sample/MyFirstNitroApplication.cs sample file.

To create your first NITRO application:

1. Copy the libraries from <NITRO_SDK_HOME>/lib folder to the project classpath.

2. Create a new class and name it **MyFirstNitroApplication**.

3. Create an instance of `com.citrix.netscaler.nitro.service.nitro_service` class. This instance is used to perform all operations on the appliance:

   ```
   nitro_service ns_session = new nitro_service("10.102.29.170", "http");
   ```

   This code establishes a connection with an appliance that has IP address 10.102.29.170 and uses the HTTP protocol. Replace 10.102.29.170 with the IP address of the NetScaler appliance that you have access to.
4. Use the `nitro_service` instance to log in to the appliance using your credentials:

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

   This code logs into the appliance, with user name as `admin` and password as `verysecret`. Replace the credentials with your login credentials.
5. Enable the load balancing feature:

   ```
   String[] features_to_be_enabled = {"lb"};
   ns_session.enable_features(features_to_be_enabled);
   ```

   This code enables load balancing on the appliance.
6. Create an instance of the `com.citrix.netscaler.nitro.resource.config.lb.lbvserver` class. You will use this instance to perform operations on the lbvserver.

   ```
   lbvserver new_lbvserver_obj = new lbvserver();
   ```

7. Use the `lbvserver` instance to create a new lbvserver:

   ```
   new_lbvserver_obj.name = "MyFirstLbVServer";
   new_lbvserver_obj.ipv46 = "10.102.29.88";
   new_lbvserver_obj.servicetype = "HTTP";
   new_lbvserver_obj.port = 80;
   new_lbvserver_obj.lbmethod = "ROUNDROBIN";
   lbvserver.add(ns_session,new_lbvserver_obj);
   ```

   This code first sets the attributes (name, IP address, service type, port, and load balancing method) of the lbvserver locally and then adds it to the appliance by using the corresponding `add()` method.
8. Retrieve the details of the lbvserver you have created:

   ```
   lbvserver new_lbvserver_obj1 = lbvserver.get(ns_session,new_lbvserver_obj.name);
   System.Console.Out.WriteLine("Name : " +new_lbvserver_obj1.name +"\n" +"Protocol : " +new_lbvserver_
   ```

   This code first retrieves the details of the lbvserver as an object from the NetScaler, extracts the required attributes (name and service type) from the object, and displays the results.
9. Delete the lbvserver you created in the above steps:

   ```
   lbvserver.delete(ns_session, new_lbvserver_obj.name);
   ```

10. Save the configurations:

    ns_session.save_config();

11. Log out of the appliance:

    ns_session.logout();

Debug the NITRO application

All NITRO exceptions are captured by the `com.citrix.netscaler.nitro.exception.nitro_exception` class. For a more detailed description, see Exception Handling.

Create a NetScaler Cluster

After completing this tutorial you will be able to create a two-node NetScaler cluster. To add more appliances to the cluster you must repeat the procedure that adds and joins the node to the cluster.

Sample Code

For the executable code, see the <NITRO_SDK_HOME>/sample/CreateCluster.cs sample file.

To create a cluster

1. Copy the libraries from <NITRO_SDK_HOME>/lib folder to the project classpath.

2. Create a new class and name it CreateCluster.

3. Log on to one of the appliances that you want to add to the cluster and create a cluster:

   ```
   //Connect to the first appliance that you want to add to the cluster
   nitro_service nonClipSession0 = new nitro_service(nsipAddress0,protocol);
   nonClipSession0.login(uName,password);

   //Create a cluster instance
   clusterinstance newClusterInstance = new clusterinstance();
   newClusterInstance.clid = 1;
   clusterinstance.add(nonClipSession0,newClusterInstance);

   //Add the appliance to the cluster
   clusternode ClusterNode0 = new clusternode();
   ClusterNode0.nodeid = 0;
   ClusterNode0.ipaddress = nsipAddress0;
   ClusterNode0.state = "ACTIVE";
   ClusterNode0.backplane = "0/1/1";
   clusternode.add(nonClipSession0,ClusterNode0);

   //Add the cluster IP address
   nsip newNSIPAddress = new nsip();
   newNSIPAddress.ipaddress = clipAddress;
   newNSIPAddress.netmask = "255.255.255.255";
   newNSIPAddress.type = "CLIP";
   nsip.add(nonClipSession0,newNSIPAddress);

   //Enable the cluster instance
   clusterinstance.enable(nonClipSession0, newClusterInstance);

   //Save the configurations
   nonClipSession0.save_config();

   //Warm reboot the appliance
   nonClipSession0.reboot(true);
   ```

   The cluster is created and the first node is added to the cluster. This node becomes the initial configuration coordinator of the cluster.

4. Log on to the cluster IP address to add other appliances to the cluster:

   ```
   //Connect to the cluster IP address
   nitro_service clipSession = new nitro_service(clipAddress,protocol);
   clipSession.login(uName,password);

   //Add the node to the cluster
   clusternode ClusterNode1 = new clusternode();
   ClusterNode1.nodeid = 1;
   ClusterNode1.ipaddress = nsipAddress1;
   ```

```
ClusterNode1.state = "ACTIVE";
ClusterNode1.backplane = "1/1/1";
clusternode.add(clipSession,ClusterNode1);

//Save the configurations
clipSession.save_config();
```

5. Log on to the appliance that you added in the previous step and join it to the cluster:

```
//Connect to the node that you have just added to the cluster
nitro_service nonClipSession1 = new nitro_service(nsipAddress1,protocol);
nonClipSession1.login(uName,password);

//Join the node to the cluster
cluster newCluster = new cluster();
newCluster.clip = clipAddress;
newCluster.password = password;
cluster.join(nonClipSession1,newCluster);

//Save the configurations
nonClipSession1.save_config();

//Warm reboot the appliance
nonClipSession1.reboot(true);
```

   The second node is now a part of the cluster.

6. Verify the details of the cluster by logging on to the cluster IP address

```
//Retrieving the cluster node details
uint id = 1;
clusternode node= clusternode.get(clipSession, id);
System.Console.Out.WriteLine("Node ID: " + node.nodeid + " | Admin state: " + node.state + " | Backplan

//Retrieving the cluster instance details
uint id1 = 1;
clusterinstance instance= clusterinstance.get(clipSession, id1);
System.Console.Out.WriteLine("Cluster instance ID: "+ instance.clid + " | Operational state: " +instance.c
```

System APIs

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

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

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

The following sample code establishes a session with a NetScaler appliance with IP address 10.102.29.60 by using the HTTPS protocol:

```
//Specify the NetScaler appliance IP address and protocol
nitro_service ns_session = new nitro_service("10.102.29.60","https");

//Specify the login credentials
ns_session.login("admin","verysecret");
```

Note: By default, the connection to the appliance expires after 30 minutes of inactivity. You can modify the timeout period by specifying a new timeout period (in seconds) in the `login` method. For example, to modify the timeout period to 60 minutes:

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

You must use the `nitro_service` object in all further NITRO operations on the appliance. For example to save the configurations on the appliance, you must use the `nitro_service` object as follows:

```
ns_session.save_config();
```

The `nitro_service` class also provides APIs to perform other system-level operations such as enabling and disabling NetScaler features and modes, saving and clearing NetScaler configurations, setting the session timeout, setting the severity of the exceptions to be handled, setting the behavior of bulk operations, and disconnecting from the appliance.

Feature Configuration APIs

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

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

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

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

A resource class provides APIs to perform the following operations:

Create | Retrieve | Update | Delete | Enable/Disable | Unset | Bind/Unbind | Global bind | Bulk operations

Create

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

The following sample code creates a load balancing virtual server:

```
//Create an instance of the lbvserver class
lbvserver new_lbvserver_obj = new lbvserver();

//Set the properties of the resource locally
new_lbvserver_obj.name = "MyFirstLbVServer";
new_lbvserver_obj.ipv46 = "10.102.29.88";
new_lbvserver_obj.port = 88;
new_lbvserver_obj.servicetype = "HTTP";
new_lbvserver_obj.lbmethod = "ROUNDROBIN";

//Upload the resource to NetScaler
lbvserver.add(ns_session,new_lbvserver_obj);
```

Retrieve

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

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

```
//Retrieve the resource object from the NetScaler
new_lbvserver_obj = lbvserver.get(ns_session,"MyFirstLbVServer");

//Extract the properties of the resource from the object locally
Console.WriteLine(new_lbvserver_obj.name);
Console.WriteLine(new_lbvserver_obj.servicetype);
```

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

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

```
filtervalue[] filter = new filtervalue[2];
filter[0] = new filtervalue("port","80");
filter[1] = new filtervalue("servicetype","HTTP");
lbvserver[] result = lbvserver.get_filtered(ns_session,filter);
```

You can also retrieve all NetScaler resources of a certain type, such as all services in the NetScaler appliance, by calling the static `get()` method on the service class, without providing a second parameter, as follows:

```
service[] resources = service.get(ns_session);
```

Update

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

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

```
//Create an instance of the lbvserver class
lbvserver update_lb = new lbvserver();

//Specify the name of the lbvserver to be updated
update_lb.name = "MyFirstLbVServer";

//Specify the updated service type and lb method
update_lb.servicetype = "https";
update_lb.lbmethod = "LEASTRESPONSETIME";

//Upload the resource to NetScaler
lbvserver.update(ns_session, update_lb);
```

Note: Some properties in some NetScaler resources are not allowed to be modified after creation. The port number or the service type (protocol) of a load balancing virtual server or a service, are examples of such properties. Even though the update method

appears to succeed, these properties retain their original values on the appliance.

Delete

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

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

```
lbvserver remove_lb = new lbvserver();
remove_lb.name("MyFirstLbVServer");
lbvserver.delete(ns_session, remove_lb);
```

Enable/Disable

To enable a resource, invoke the `enable()` method.

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

```
lbvserver obj = new lbvserver();
obj.name = "lb_vip";
lbvserver.enable(ns_session, obj);
```

Note: To disable a resource, invoke the `disable()` method.

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

Unset

To unset the value that is set to a parameter, invoke the `unset()` method on the resource class, by passing the name of the resource and the parameters to be unset. If the parameter has a default value, the value is reset to that value.

The following sample code unsets the load balancing method and the comments of a load balancing virtual server named "lb_123":

```
lbvserver obj = new lbvserver();
obj.name = "lb_123";
String[] args = { "lbmethod","comment" };
lbvserver.unset(ns_session, lb1, args);
```

Bind/Unbind

NetScaler resources form relationships with each other through the process of binding. This is how services are associated with a load balancing virtual server (by binding them to it), or how various policies are bound to a load balancing virtual server. Each binding relationship is represented in NITRO by its own class.

To bind one NetScaler resource to another, you must instantiate the appropriate binding class (for example, to bind a service to a load balancing virtual server, you must instantiate the `lbvserver_service_binding` class) and add it to the NetScaler configuration (by

using the static `add()` method on this class).

Binding classes have a property representing the name of each resource in the binding relationship. They can also have other properties related to that relationship (for example, the weight of the binding between a load balancing virtual server and a service).

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

```
lbvserver_service_binding bindObj = new lbvserver_service_binding();
bindObj.name = "MyFirstLbVServer";
bindObj.servicename = "svc_prod";
bindObj.weight = 20;
lbvserver_service_binding.add(ns_session,bindObj);
```

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

The following code sample unbinds a service from a server:

```
lbvserver_service_binding bindObj = new lbvserver_service_binding();
bindObj.name("MyFirstLbVServer");
bindObj.servicename("svc_prod");
lbvserver_service_binding.delete(ns_session,bindObj);
```

Global bind

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

Some NITRO classes can be used to bind resources globally. These classes have names that follow the following pattern: `<featurename>global_<resourcetype>_binding`.

For example, the class `aaaglobal_preauthenticationpolicy_binding` is used to bind preauthentication policies globally.

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

```
aaapreauthenticationaction preauth_act1;
aaapreauthenticationpolicy preauth_pol1;
aaaglobal_aaapreauthenticationpolicy_binding glob_binding;
preauth_act1 = new aaapreauthenticationaction();
preauth_act1.name = "preauth_act1";
preauth_act1.preauthenticationaction = "ALLOW";
aaapreauthenticationaction.add(ns_session, preauth_act1);

preauth_pol1 = new aaapreauthenticationpolicy();
preauth_pol1.name = "preauth_pol1";
```

```
preauth_pol1.rule = "CLIENT.APPLICATION.PROCESS(antivirus.exe) EXISTS";
preauth_pol1.reqaction = "preauth_act1";
aaapreauthenticationpolicy.add(ns_session, preauth_pol1);

glob_binding = new aaaglobal_aaapreauthenticationpolicy_binding();
glob_binding.policy = "preauth_pol1";
glob_binding.priority = 200;
aaaglobal_aaapreauthenticationpolicy_binding.add(ns_session,glob_binding);
```

Bulk operations

You can create, retrieve, update, and delete multiple resources simultaneously and thus minimize network traffic. For example, you can add multiple load balancing virtual servers in the same operation. To perform a bulk operation, you instantiate an array of the resource class, configure the properties of all the instances locally, and then upload all the instances to the NetScaler with one command.

To account for the failure of some operations within the bulk operation, NITRO allows you to configure one of the following behaviors:

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

Note: You must configure the required behavior while establishing a connection with the appliance.

```
nitro_service ns_session = new nitro_service("10.102.29.60","http");
ns_session.onerror = OnerrorEnum.CONTINUE;
ns_session.login("admin","verysecret");
```

The following sample code creates two load balancing virtual servers:

```
//Create an array of lbvserver instances
lbvserver[] lbs = new lbvserver[2];

//Specify details of first lbvserver
lbs[0] = new lbvserver();
lbs[0].name = "lbvserv1";
lbs[0].servicetype = "http";
lbs[0].ipv46 = "10.70.136.5";
lbs[0].port = 80;

//Specify details of second lbvserver
lbs[1] = new lbvserver();
lbs[1].name = "lbvserv2";
lbs[1].servicetype = "https";
lbs[1].ipv46 = "10.70.136.5";
lbs[1].port = 443;
```

```
//upload the details of the lbvservers to the NITRO server
lbvserver.add(ns_session,lbs);
```

Cluster APIs

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

Cluster Instance Operations

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

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

```
clusterinstance new_cl_inst_obj = new clusterinstance();
//Set the properties of the cluster instance locally
new_cl_inst_obj.clid = 1;
new_cl_inst_obj.preemption = "ENABLED";

//Upload the cluster instance
clusterinstance.add(ns_session,new_cl_inst_obj);
```

Cluster Node Operations

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

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

```
clusternode new_cl_node_obj = new clusternode();
//Set the properties of the cluster node locally
new_cl_node_obj.nodeid = 0;
new_cl_node_obj.ipaddress = "10.102.29.60";
new_cl_node_obj.state = "ACTIVE";
new_cl_node_obj.backplane = "0/1/1";

//Upload the cluster node
clusternode.add(ns_session,new_cl_node_obj);
```

Add a Cluster IP Address

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

The following sample code configures a cluster IP address on NetScaler appliance with IP address 10.102.29.60:

```
nsip new_nsip_obj = new nsip();
//Set the properties locally
new_nsip_obj.ipaddress = "10.102.29.61";
new_nsip_obj.netmask = "255.255.255.255";
new_nsip_obj.type = "CLIP";

//Upload the cluster node
nsip.add(ns_session,new_nsip_obj);
```

Add a Spotted IP Address

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

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

```
nsip new_nsip_obj = new nsip();
//Set the properties locally
new_nsip_obj.ipaddress = "10.102.29.77";
new_nsip_obj.netmask = "255.255.255.0";
new_nsip_obj.type = "SNIP";
new_nsip_obj.ownernode = 1;

//Upload the cluster node
nsip.add(ns_session,new_nsip_obj);
```

Join NetScaler Appliance to Cluster

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

The following sample code joins a NetScaler appliance to a cluster:

```
cluster new_cl_obj = new cluster();
//Set the properties of the cluster locally
new_cl_obj.clip = "10.102.29.61";
new_cl_obj.password = "verysecret";

//Upload the cluster node
cluster.add(ns_session,new_cl_node_obj);
```

Linkset Operations

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

To configure a linkset, do the following:

1. Add a linkset by invoking the `add()` method of the `linkset` class.

2. Bind the interfaces to the linkset using the `add()` method of the `linkset_interface_binding` class.

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

```
//Create the linkset
linkset new_linkset_obj = new linkset();
new_linkset_obj.id = "LS/1";
linkset.add(ns_session,new_linkset_obj);

//Bind the interfaces to the linkset
linkset_interface_binding new_linkif_obj = new linkset_interface_binding();
new_linkif_obj.id = "LS/1";
new_linkif_obj.ifnum = "1/1/2 2/1/2";
linkset_interface_binding.add(ns_session,new_linkif_obj);
```

Feature Statistics APIs

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

The APIs to retrieve statistics of NetScaler features are available in namespaces that have the following pattern: `com.citrix.netscaler.nitro.resource.stat.<feature>`.

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

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

```
lbvserver_stats stats = lbvserver_stats.get(ns_session,"MyFirstLbVServer");
Console.WriteLine(stats.curclntconnections);
Console.WriteLine(stats.deferredreqrate);
```

Note: Not all NetScaler features and resources have statistic objects associated with them.

AppExpert Application APIs

To export an AppExpert application, you must instantiate the `com.citrix.netscaler.nitro.resource.config.app.application` class, configure the properties of the AppExpert locally, and then export the AppExpert application.

The following sample code exports an AppExpert application named "MyApp1":

```
application myapp = new application();
myapp.appname = "MyApp1";
myapp.apptemplatefilename = "myapp_template";
application.export(ns_session,myapp);
```

You can also import an AppExpert application. You must instantiate the `com.citrix.netscaler.nitro.resource.config.app.application` class, configure the properties of the AppExpert locally, and then import the AppExpert application.

The following sample code imports an AppExpert application named "MyApp1":

```
application myapp = new application();
myapp.appname = "MyApp1";
myapp.apptemplatefilename = "myapp_template";
application.Import(ns_session,myapp);
```

Exception Handling

The status of a NITRO request is captured in the `com.citrix.netscaler.nitro.exception.nitro_exception` class. This class provides the following details of the exception:

- **Session ID.** The session in which the exception occurred.
- **Severity.** The severity of the exception: error or warning. By default, only errors are captured. To capture warnings, you must set the warning flag to true, while connecting to the appliance.
- **Error code.** The status of the NITRO request. An error code of 0 indicates that the NITRO request is successful. A non-zero error code indicates an error in processing the NITRO request.
- **Error message.** Provides a brief description of the exception.

For a list of error codes, see the errorlisting.html file available in the <NITRO_SDK_HOME>/doc/api_reference folder.

REST Web Services

REST (REpresentational State Transfer) is an architectural style based on simple HTTP requests and responses between the client and the server. REST is used to query or change the state of objects on the server side. In REST, the server side is modeled as a set of entities where each entity is identified by a unique URL. For example, the load balancing virtual server entity is identified by the URL http://<NSIP>/nitro/v1/config/<lbvserver>/<lbvserver_name>.

Each resource also has a state on which the following operations can be performed:

- **Create.** Clients can create new server-side resources on a "container" resource. You can think of container resources as folders, and child resources as files or subfolders. The calling client provides the state for the resource to be created. The state can be specified in the request by using XML or JSON format. The client can also specify the unique URL that will identify the new object. Alternatively, the server can choose and return a unique URL identifying the created object. The HTTP method used for Create requests is POST.

- **Read.** Clients can retrieve the state of a resource by specifying its URL with the HTTP GET method. The response message contains the resource state, expressed in JSON format.

- **Update.** You can update the state of an existing resource by specifying the URL that identifies that object and its new state in JSON or XML, using the PUT HTTP method.

- **Delete.** You can destroy a resource that exists on the server-side by using the DELETE HTTP method and the URL identifying the resource to be removed.

In addition to these four CRUD operations (Create, Read, Update, and Delete), resources can support other operations or actions. These operations use the HTTP POST method, with the URL specifying the operation to be performed and the request body specifying the parameters for that operation.

NetScaler NITRO APIs are categorized depending on the scope and purpose of the APIs into system APIs, feature configuration APIs, and feature statistics APIs.

Performing System Level Operations

The first step towards using NITRO is to establish a session with the NetScaler appliance and then authenticate the session by using the NetScaler administrator's credentials. You must specify the username and password in the `login` object. The session ID that is created must be specified in the request header of all further operations in the session.

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

To connect to a NetScaler appliance with NSIP address 10.102.29.60 by using the HTTP protocol:

- **URL.** https://10.102.29.60/nitro/v1/config/login/
- **Method.** POST
- **Request.**
  - **Header.**

    Content-Type:application/vnd.com.citrix.netscaler.login+json

    Note: Content types such as 'application/x-www-form-urlencoded' that were supported in earlier versions of NITRO can also be used. You must make sure that the payload is the same as used in earlier versions. The payloads provided in this documentation are only applicable if the content type is of the form 'application/vnd.com.citrix.netscaler.login+json'.
  - **Payload.**

```
{
   "login":
   {
      "username":"admin",
      "password":"verysecret"
   }
}
```

- **Response.**
  - **Header.**

```
HTTP/1.0 201 Created
Set-Cookie:
NITRO_AUTH_TOKEN=##87305E9C51B06C848F0942; path=/nitro/v1
```

Note: By default, the connection to the appliance expires after 30 minutes of inactivity. You can modify the timeout period by specifying a new timeout period (in seconds) in the `login` object. For example, to modify the timeout period to 60 minutes, the request payload is:

```
{
   "login":
   {
      "username":"admin",
      "password":"verysecret",
      "timeout":3600
   }
}
```

You can also connect to the appliance to perform a single operation, by specifying the username and password in the request header of the operation. For example, to connect to an appliance while adding a load balancing virtual server:

- **URL.** https://10.102.29.60/nitro/v1/config/lbvserver/
- **Method.** POST
- **Request.**
  - **Header.**

    X-NITRO-USER:admin
    X-NITRO-PASS:verysecret
    Content-Type:application/vnd.com.citrix.netscaler.lbvserver
    +json

  - **Payload.**

    ```
    {
      "lbvserver":
      {
        ...
        ...
        ...
      }
    ```

- **Response.**
  - **Header.**

    HTTP/1.0 201 Created

You can also perform other system-level operations such as enabling NetScaler features and modes, saving and clearing NetScaler configurations, setting the session timeout, setting the severity of the exceptions to be handled, setting the behavior of bulk operations, and disconnecting from the appliance.

For more information on the REST messages, see the Configuration node of the <NITRO_SDK_HOME>/index.html file.

Example 1: Enable the load balancing feature

- **URL.** http://10.102.29.60/nitro/v1/config/nsfeature?action=enable
- **HTTP Method.** POST
- **Request.**

- **Header**

  Cookie:NITRO_AUTH_TOKEN=tokenvalue
  Content-Type:application/vnd.com.citrix.netscaler.nsfeature+json

- **Payload**

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

Example 2: Save NetScaler configurations

- **URL.** http://10.102.29.60/nitro/v1/config/nsconfig?action=save
- **HTTP Method.** POST
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.nsconfig+json

  - **Payload**

```
{
   "nsconfig":{}
}
```

Example 3: Disconnecting from the appliance

- **URL.** https://10.102.29.60/nitro/v1/config/logout/
- **HTTP Method.** POST
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.logout+json

  - **Payload**

```
{
   "logout":{}
}
```

Note: Make sure that you have saved the configurations before performing this operation.

Configuring NetScaler Features

A NetScaler appliance has multiple features, and each feature has multiple resources. Each NetScaler resource, depending on the operation to be performed on it, has a unique URL associated with it. URLs for configuration operations have the format `http://<NSIP>/nitro/v1/config/<resource_type>/<resource_name>`. For example, to access the lbvserver named MyFirstLbVServer on a NetScaler with IP 10.102.29.60, the URL is `http://10.102.29.60/nitro/v1/config/lbvserver/MyFirstLbVServer`.

Using NITRO you can perform the following operations:

Create | Retrieve | Update | Delete | Enable/Disable | Unset | Bind/Unbind | Bulk operations

For more information on the REST messages, see the Configuration node of the <NITRO_SDK_HOME>/index.html file.

Create

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

To create an lbvserver named "MyFirstLbVServer":

- **URL.** http://10.102.29.60/nitro/v1/config/lbvserver/
- **HTTP Method.** POST
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.lbvserver+json

  - **Payload**

```
{
   "lbvserver":
   {
      "name":"MyFirstLbVServer",
      "servicetype":"http"
   }
}
```

Retrieve

NetScaler resource properties can be retrieved as follows:

- To retrieve details of all resources of a specific type, specify the resource type in the URL.

  URL format: `http://<NSIP>/nitro/v1/config/<resource_type>`

- To retrieve details of a specific resource on the NetScaler appliance, specify the resource name in the URL.

  URL format:
  `http://<NSIP>/nitro/v1/config/<resource_type>/<resource_name>`

- To retrieve specific details of a resource, specify the resource details that you want to view in the URL.

  URL format: `http://<NSIP>/nitro/v1/config/<resource_type>/<resource_name>?attrs=<attrib1>,<attrib2>`

- To retrieve details of resources on the basis of some filter, specify the filter conditions in the URL.

  URL format: `http://<NSIP>/nitro/v1/config/<resource_type>?filter=<attrib1>:<value>,<attrib2>:<value>`

- If the request is likely to result in a large number of resources, you can divide the results into pages and retrieve them page by page.

  For example, assume that you have a NetScaler that has 53 lbvservers and you want to retrieve all the lbvservers. So, instead of retrieving all 53 in one response, you can configure the results to be divided into pages of 10 lbvservers each (6 pages total), and retrieve them from the NetScaler page by page.

  URL format: `http://<NSIP>/nitro/v1/config/<resource_type>?pageno=<value>&pagesize=<value>`

  You specify the page count with the `pagesize` parameter and the page number that you want to retrieve with the `pageno` parameter.

- To get the number of resources that are likely to be returned by a request, you can use the `count` query string parameter to ask for a count of the resources to be returned, rather than the resources themselves.

  URL format: `http://<NSIP>/nitro/v1/config/<resource_type>?count=yes`

To retrieve the details of an lbvserver named "MyFirstLbVServer":

- **URL.** http://10.102.29.60/nitro/v1/config/lbvserver/MyFirstLbVServer/
- **HTTP Method.** GET
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
- **Response.**

- **Header**

  HTTP/1.0 200 OK
  Content-Type:application/vnd.com.citrix.netscaler.lbvserver+json

- **Payload**

```
{
   "lbvserver":
   [
      {
         "name":"MyFirstLbVServer",
         "servicetype":"http",
         "insertvserveripport":"OFF",
         "ip":"0.0.0.0",
         "port":80,
         ...
      }
   ]
}
```

Update

To update the details of an existing resource on the NetScaler appliance, specify the resource name, and the arguments to be updated, in the specific resource object.

To change the load balancing method to ROUNDROBIN and update the comment property for a load balancing virtual server named "MyFirstLbVServer":

- **URL.** http://10.102.29.60/nitro/v1/config/lbvserver/MyFirstLbVServer/

- **HTTP Method.** PUT

- **Request.**

  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.lbvserver+json

  - **Payload**

```
{
   "lbvserver":
   {
      "name":"MyFirstLbVServer",
      "lbmethod":"ROUNDROBIN",
      "comment":"Updated comments"
   }
}
```

Delete

To delete a NetScaler resource, specify the resource name in the URL.

To delete a load balancing virtual server named "MyFirstLbVServer":

- **URL.** http://10.102.29.60/nitro/v1/config/lbvserver/MyFirstLbVServer
- **HTTP Method.** DELETE

Enable/Disable

To enable a resource on the NetScaler appliance, specify the resource name in the specific resource object.

To enable a load balancing virtual server named "MyFirstLbVServer":

- **URL.** http://10.102.29.60/nitro/v1/config/lbvserver?action=enable
- **HTTP Method.** POST
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.lbvserver+json

  - **Payload**

```
{
   "lbvserver":
   {
      "name":"MyFirstLbVServer"
   }
}
```

Note: To disable a resource, in the URL specify the action as "disable".

Unset

To unset the value that is set to a parameter, specify the action as "unset" and in the payload, specify the parameters to be unset.

To unset the load balancing method and the comments specified for a load balancing virtual server named "MyFirstLbVServer":

- **URL.** http://10.102.29.60/nitro/v1/config/lbvserver?action=unset
- **HTTP Method.** POST
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.lbvserver+json

  - **Payload**

```
{
   "lbvserver":
```

```
    {
        "name":"MyFirstLbVServer",
        "lbmethod":true,
        "comment":true,
    }
}
```

Bind/Unbind

To bind a resource to another, specify the name of the two resources and specify the weight for the binding.

To bind a service named "svc_prod" to a load balancing virtual server named "MyFirstLbVServer", by specifying a certain weight for the binding:

- **URL.** http://10.102.29.60/nitro/v1/config/lbvserver_service_binding/
- **HTTP Method.** PUT
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.lbvserver_service_binding+json
  - **Payload**

```
{
    "lbvserver_service_binding":
    {
        "name":"MyFirstLbVServer",
        "servicename":"svc_prod",
        "weight":111,
    }
}
```

Note: To unbind, specify the arguments in the URL as follows:

- **URL.** http://10.102.29.60/nitro/v1/config/lbvserver_service_binding/MyFirstLbVServer?args=servicename:svc_prod
- **HTTP Method.** DELETE

Bulk operations

You can create, retrieve, update, and delete multiple resources simultaneously and thus minimize network traffic. For example, you can add multiple load balancing virtual servers in the same operation. To perform a bulk operation, specify the required parameters in the same request payload.

To account for the failure of some operations within the bulk operation, NITRO allows you to configure one of the following behaviors:

- **Exit.** When the first error is encountered, the execution stops. The commands that were executed before the error are committed.

- **Rollback.** When the first error is encountered, the execution stops. The commands that were executed before the error are rolled back. Rollback is only supported for add and bind commands.

- **Continue.** All the commands in the list are executed even if some commands fail.

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

To add two load balancing virtual servers in one operation and continue if one command fails:

- **URL.** http://10.102.29.60/nitro/v1/config/lbvserver/

- **HTTP Method.** POST

- **Request.**

  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.lbvserver_list+json
    X-NITRO-ONERROR:continue

  - **Payload**

```
{
   "lbvserver":
   [
      {
         "name":"new_lbvserver1",
         "servicetype":"http"
      },

      {
         "name":"new_lbvserver2",
         "servicetype":"http"
      }
   ]
}
```

- **Response**

  - **Header**

    HTTP/1.0 207 Multi Status

  - **Payload**

```
{
   "errorcode":273,
   "message":"Resource already exists",
   "severity":"ERROR",
   "response":
   [
      {
         "errorcode": 0,
```

```
            "message": "Done",
            "severity": "NONE"
         },
         {
            "errorcode": 273,
            "message":"Resource already exists",
            "severity": "ERROR"
         }
      ]
   }
```

Binding NetScaler Resources

NetScaler resources form relationships with each other through the process of binding. This is how services are associated with an lbvserver (by binding them to it), or how various policies are bound to an lbvserver. Each binding relationship is represented by its own object. A binding resource has properties representing the name of each NetScaler resource in the binding relationship. It can also have other properties related to that relationship (for example, the weight of the binding between an lbvserver resource and a service resource).

Note: Unlike for NetScaler entities, you use a PUT HTTP method, instead of POST, for adding new binding resources.

For more information on the REST messages, see the Configuration node of the <NITRO_SDK_HOME>/index.html file.

To bind a service to a load balancing virtual server named "MyFirstLbVServer" and specify a weight for the binding:

- **URL.** http://10.102.29.60/nitro/v1/config/lbvserver_service_binding/MyFirstLbVServer?action=bind
- **HTTP Method.** PUT
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.lbvserver_service_binding+json

  - **Payload**

```
{
   "lbvserver_service_binding":
   {
      "servicename":"svc_prod",
      "weight":20,
      "name":"MyFirstLbVServer"
   }
}
```

To retrieve list of all the services bound to a virtual server "lbv1":

- **URL.**
  http://10.102.29.60/nitro/v1/config/lbvserver_service_binding/lbv1?attrs=servicename
- **HTTP Method.** GET

For more information on retrieving information, see the "Retrieving properties of a resource" section in Configuring NetScaler Features.

Globally Bind Resources

Some NetScaler resources can be bound globally to affect the whole system. For example, if a compression policy is bound to an lbvserver, the policy affects only the traffic on that lbvserver. However, if bound globally, it can affect any traffic on the appliance, regardless of which virtual servers handle the traffic.

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

To bind the policy named preautpol1 globally at priority 200:

- **URL.** http://10.102.29.60/nitro/v1/config/aaaglobal_aaapreauthenticationpolicy_binding?action=bind
- **HTTP Method.** PUT
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.aaaglobal_aaapreauthenticationpolicy_binding+j
  - **Payload**

```
{
   "aaaglobal_aaapreauthenticationpolicy_binding":
   {
      "policy":"preautpol1",
      "priority":200
   }
}
```

Configuring a NetScaler Cluster

You can use NITRO to add or create and manage a NetScaler cluster.

Cluster Instance Operations

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

To create a cluster instance with ID 1:

- **URL.** http://10.102.29.60/nitro/v1/config/clusterinstance/
- **HTTP Method.** POST
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.clusterinstance+json

  - **Payload**

```
{
   "clusterinstance":
   {
      "clid":1,
      "preemption":"ENABLED"
   }
}
```

Cluster Node Operations

All operations on a cluster node must be performed on the `clusternode` object.

To add a cluster node with NSIP address 10.102.29.60:

- **URL.** http://10.102.29.60/nitro/v1/config/clusternode/
- **HTTP Method.** POST
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.clusternode+json

  - **Payload**

```
{
   "clusternode":
   {
      "nodeid":1,
      "ipaddress":"10.102.29.60",
      "state":"ACTIVE",
      "backplane":"1/1/2"
   }
}
```

Add a Cluster IP Address

To define a cluster IP address, specify the required parameters in the `nsip` object.

To configure a cluster IP address on NetScaler appliance with IP address 10.102.29.60:

- **URL.** http://10.102.29.60/nitro/v1/config/nsip/
- **HTTP Method.** POST
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.nsip+json
  - **Payload**

```
{
   "nsip":
   {
      "ipaddress":"10.102.29.61",
      "netmask":"255.255.255.255",
      "type":"CLIP"
   }
}
```

Add a Spotted IP Address

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

To configure a spotted SNIP address on a node with ID 1:

- **URL.** http://10.102.29.60/nitro/v1/config/nsip/
- **HTTP Method.** POST
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.nsip+json
  - **Payload**

```
{
   "nsip":
   {
      "ipaddress":"10.102.29.77",
      "netmask":"255.255.255.0",
      "type":"SNIP",
      "ownernode":1
   }
}
```

Join NetScaler Appliance to Cluster

To join an appliance to a cluster, specify the required parameters in the `cluster` object.

To join a NetScaler appliance to a cluster:

- **URL.** http://10.102.29.60/nitro/v1/config/cluster/
- **HTTP Method.** POST
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.cluster+json

  - **Payload**

```
{
   "cluster":
   {
      "clip":"10.102.29.61",
      "password":"verysecret"
   }
}
```

Linkset Operations

To configure a linkset, do the following:

1. Create a linkset by specifying the required parameters in the `linkset` object.

   To add a linkset LS/1:

   - **URL.** http://10.102.29.60/nitro/v1/config/linkset/
   - **HTTP Method.** POST
   - **Request.**
     - **Header**

       Cookie:NITRO_AUTH_TOKEN=tokenvalue
       Content-Type:application/vnd.com.citrix.netscaler.linkset+json

     - **Payload**

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

2. Bind the required interfaces to the linkset by specifying the interfaces in the `linkset_interface_binding` object.

   To bind interfaces 1/1/2 and 2/1/2 to linkset LS/1:

   - **URL.** http://10.102.29.60/nitro/v1/config/linkset_interface_binding/LS%2F1?action=bind
   - **HTTP Method.** PUT
   - **Request.**
     - **Header**

       Cookie:NITRO_AUTH_TOKEN=tokenvalue
       Content-Type:application/vnd.com.citrix.netscaler.linkset_interface_binding+json

     - **Payload**

```
{
   "linkset_interface_binding":
   {
      "id":"LS/1",
      "ifnum":"1/1/2 2/1/2"
   }
}
```

Retrieving Feature Statistics

The NetScaler appliance collects statistics about the usage of its features and the corresponding resources. NITRO can retrieve these statistics.

- URL to get statistics of a feature must have the format `http://<NSIP>/nitro/v1/stat/<feature_name>`.
- URL to get the statistics of a resource must have the format: `http://<NSIP>/nitro/v1/stat/<resource_type>/<resource_name>`.

For more information on the REST messages, see the Statistics node of the <NITRO_SDK_HOME>/index.html file.

To get the statistics of a lbvserver named "MyFirstLbVServer":

- **URL.** http://10.102.29.60/nitro/v1/stat/lbvserver/MyFirstLbVServer
- **HTTP Method.** GET
- **Request.**
  - **Header.**

    Content-Type:application/vnd.com.citrix.netscaler.lbvserver+json
- **Response.**
  - **Header**

    HTTP/1.0 200 OK
  - **Payload**

```
{
   "lbvserver":
   [
      {
         "name":"MyFirstLbVServer",
         "establishedconn":0,
         "vslbhealth":0,
         "primaryipaddress":"0.0.0.0",
         ...
      }
   ]
}
```

Note: Not all NetScaler features and resources have statistic objects associated with them.

Managing AppExpert Applications

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

To export an AppExpert application named "MyApp1":

- **URL.** http://10.102.29.60/nitro/v1/config/apptemplateinfo?action=export
- **HTTP Method.** POST
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.apptemplateinfo+json

  - **Payload**

```
{
   "apptemplateinfo":
   {
      "appname":"MyApp1",
      "apptemplatefilename":"BizAp.xml",
      "template_info":
      {
          "templateversion_major":"2",
          "templateversion_minor":"1",
          "author":"XYZ",
          "introduction":"Intro",
          "summary":"Summary"
      },
   }
}
```

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

To import an AppExpert application named "MyApp1":

- **URL.** http://10.102.29.60/nitro/v1/config/apptemplateinfo?action=import
- **HTTP Method.** POST
- **Request.**
  - **Header**

Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.netscaler.apptemplateinfo+json
X-NITRO-ONERROR:rollback

- **Payload**

```
{
  "apptemplateinfo":
  {
     "apptemplatefilename":"BizAp.xml",
     "deploymentfilename":"BizAp_deployment.xml",
     "appname":"MyApp1"
  }
}
```

To import an AppExpert application by specifying different deployment settings:

- **URL.** http://10.102.29.60/nitro/v1/config/apptemplateinfo?action=import
- **HTTP Method.** POST
- **Request.**
  - **Header**

    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.netscaler.apptemplateinfo+json
    X-NITRO-ONERROR:rollback

  - **Payload**

```
{
  "apptemplateinfo":
  {
     "apptemplatefilename":"BizAp.xml",
     "appname":"Myapp2"
      "deploymentinfo":
      {
         "appendpoint":
         [
            {
               "ipv46":"11.2.3.8",
               "port":80,
               "servicetype":"HTTP"
            }
         ],
         "service":
         [
            {
               "ip":"12.3.3.15",
               "port":80,
               "servicetype":"SSL"
            },
            {
               "ip":"14.5.5.16",
               "port":443,
```

```
                    "servicetype":"SSL"
                }
            ],
        }
    }
}
```

Handling Exceptions

The response header provides the status of an operation by using HTTP status codes and the response payload provides the requested resource object (for GET method) and error details (for unsuccessful operation). NITRO does not provide a response payload for successful POST, PUT and DELETE methods. For successful GET method, the response payload consists only the requested resource object.

The following table provides the HTTP status codes:

Status	HTTP Status Code	Description
Success	200 OK	Request successfully executed.
	201 CREATED	Entity created.
Failure	400 Bad Request	Incorrect request provided.
	401 unauthorized	Not provided login credentials.
	403 forbidden	User is unauthorized
	404 Not Found	User is trying to access a resource not present in the NetScaler.
	405 Method Not Allowed	User is trying to access request methods not supported by NITRO.
	406 Not Acceptable	None of the values supplied by the user in the Accept header can be satisfied by the server.
	409 Conflict	The resource already exists on the NetScaler.
	503 Service Unavailable	The service is not available.
	599	NetScaler specific error code.
Warning	209 X-NITRO-WARNING	Warnings are captured by specifying the login URL as http://<nsip>/nitro/v1/config/login/?warning=yes.
Combination of success and failure (for bulk operation with X-NITRO-ONERROR set as continue)	207 Multi Status	Some commands are executed successfully and some have failed.

Note: The content-type in the response header of an unsuccessful operation, consists of error MIME type instead of resource MIME type.

For a more detailed description of the error codes, see the API reference available in the <NITRO_SDK_HOME>/doc folder.

NITRO Changes Across NetScaler Releases

NetScaler has introduced some changes in the NITRO API since the NetScaler 9.3 release. This could raise some compatibility issues for the following users:

- Users migrating from NetScaler 9.3 to 10.1
- Users migrating from NetScaler 9.3 to 10.5

Note: There are no changes introduced since the NetScaler 10.1 release. Therefore, you should not face any compatibility issues when migrating from NetScaler 10.1 to 10.5.

These NITRO changes from 9.3 to 10.1 or 10.5 are categorized as follows:

Note: Unless otherwise specified, these changes are applicable to both REST and SDKs.

Resources Removed

Resource	Replace with...	Comments
lbmonitor_lbmetrictable_binding	lbmonitor_metric_binding	

APIs Removed

Resource	API	Comments
vserver	GET	Perform the GET operation on specific virtual server types such as lb/cr/cs.
filterpolicy	POST with "action=unset"	This API is removed as unsetting the attributes('action') of a policy makes it invalid.
auditsyslogpolicy	POST with "action=unset"	This API is removed as unsetting the attributes('action') of a policy makes it invalid.
auditnslogpolicy	POST with "action=unset"	This API is removed as unsetting the attributes('action') of a policy makes it invalid.
authorizationpolicy	POST with "action=unset"	This API is removed as unsetting the attributes('action') of a policy makes it invalid.

API Return Type Changed

Resource	API	Comments
snmpengineid	GET	Return type changed to an array.
nshostname	GET	Return type changed to an array.

Attribute Type Changed

Resource	Attribute	Comments
appfwpolicy_lbvserver_binding	activepolicy	Data type changed from Boolean to Integer.
appfwpolicy_appfwglobal_binding	activepolicy	Data type changed from Boolean to Integer.
vlan	portbitmap	Data type changed from uint to ulong.
vlan	tagbitmap	Data type changed from uint to ulong.

Attributes Removed

Resource	Attribute	Replace with...	Comments
policypatset_pattern_binding	indextype	- NA -	This attribute is moved to 'policypatset' resource as this attribute is applicable at patset level.
system_stats	powersupply1failure	powersupply1status	Change is applicable from NetScaler 9.3 (65.8).
system_stats	powersupply2failure	powersupply2status	Change is applicable from NetScaler 9.3 (65.8).
server_servicegroup_binding	servicetype	svctype	
server_service_binding	servicetype	svctype	
crvserver	hits	- NA -	Hits are calculated per policy binding hence moved this parameter to binding resources.
crvserver	dstvsvr	destinationvserver	
crvserver	destvserver	domain	
crvserver	dnsvserver	dnsvservername	
appflowpolicylabel	type	policylabeltype	
sslcipher	ciphgrpals	ciphergroupname	This change is applicable for sslcipher_*_binding resources also.
csvserver_cspolicy_binding	targetvserver	targetlbvserver	
csvserver_cspolicy_binding	targetvserver	targetlbvserver	
rewriteaction	allow_unsafe_pi1, allow_unsafe_pi	bypassSafetyCheck	

SDK Specific Changes

Class	Method	Replace with...	Comments
Routerbgp	- NA -	- NA -	This class is removed as all router configurations are deprecated in 9.2.
dnsptrrec	get(dnsptrrec obj, nitro_service session)	get(nitro_service session, String reversedomain)	
dnsaddrec	get(dnsaddrec obj, nitro_service session)	get(nitro_service session, String hostname)	
dnsnsrec	get(dnsnsrec obj, nitro_service session)	get(nitro_service session, String domain)	
snmpengineid	unset(nitro_service session, String[] args)	unset(nitro_service session, snmpengineid resource, String[] args)	
arp	arp.get(nitro_service session, String ipaddress)	arp.get(nitro_service session, arp resource)	
nsip	get(nitro_service session, String ipaddress)	get(nitro_service client, nsip resource)	
nsip6	get(nitro_service session, String ipv6address)	get(nitro_service session, nsip6 resource)	
dnsmxrec	dnsmxrec.get(dnsmxrec obj, nitro_service session)	dnsmxrec[] get(nitro_service service, dnsmxrec_args args)	

Unsupported NetScaler Operations

Some NetScaler operations that are available through the command line interface and through the configuration utility, are not available through NITRO APIs. The following list provides the NetScaler operations not supported by NITRO:

- install API
- diff API on nsconfig resource
- UI-internal APIs (update, unset, and get)
- show ns info
- Application firewall APIs:
  - importwsdl
  - importcustom
  - importxmlschema
  - importxmlerrorpage
  - importhtmlerrorpage
  - rmwsdl
  - rmcustom
  - rmxmlschema
  - rmxmlerrorpage
  - rmhtmlerrorpage
- CLI-specific APIs:
  - ping
  - ping6
  - traceroute
  - traceroute6
  - nstrace
  - scp
  - configaudit

- show defaults
- show permission
- batch
- source

XML API

Developers and administrators can use the NetScaler Application Programming Interface (API), nsconfig, to implement customized client applications. The nsconfig API, which mirrors the NetScaler command line interface (CLI), is based on the Web Services Description (WSDL) specification. It includes a filterwsdl command to reduce compilation time and file size. You can secure your API applications at the NetScaler IP address or at the IP address of the subnet on which the NetScaler is deployed.

The following topics describe the properties and use of the API.

Introduction	General information about the API, requirements, and software-version information.
The NS Config Interface	How to use the API.
Examples of API Usage	Basic examples of how to use the API.
The Web Service Description Language (WSDL)	How to use the WSDL-based interface schema to support your client applications, and how to use WSDL Filter to reduce file size and compilation time.
Securing API Access	How to secure API access.

Introduction to the API

The API enables programmatic communications between client applications and the NetScaler appliance, providing the following benefits:

- Developers can control the NetScaler from a custom application. The API enables the client application to configure and monitor the NetScaler.
- Developers can create client applications easily and quickly, using a language and platform with which they are comfortable.
- The API provides a secure, end-to-end, standards-based framework that integrates into the existing infrastructure.

Based on the Simple Object Access Protocol (SOAP) over HTTP, the API consists of the NSConfig interface. NSConfig includes methods for setting and querying the configuration. These methods allow the client application using the NSConfig interface to perform almost all operations that an administrator would normally perform with the CLI or GUI.

In addition, the NetScaler provides an interface description, based on the Web Services Definition Language (WSDL), that facilitates the development of client applications.

Hardware and Software Requirements

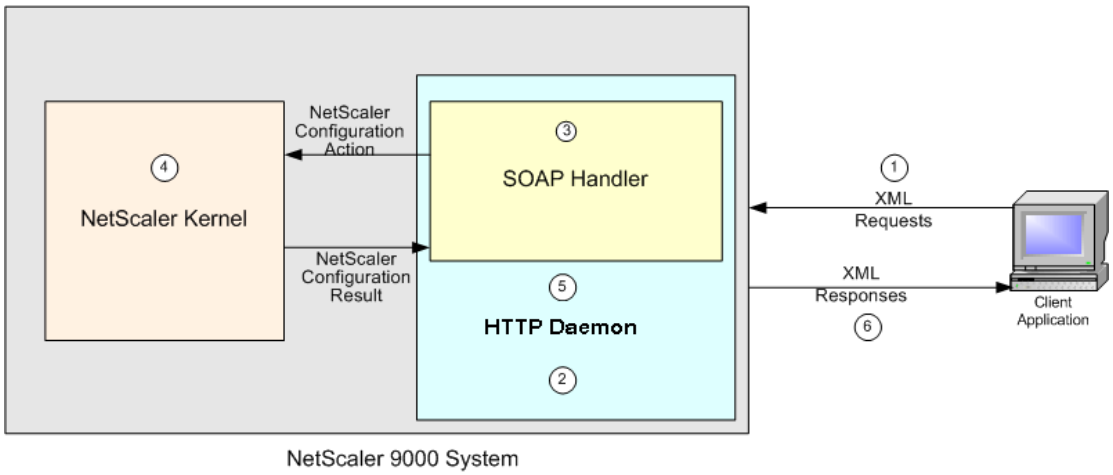
To work with the API, your system needs to meet the following hardware and software setup and requirements:

- A client workstation.
- Access to a NetScaler, version 8.0 or higher.
- A SOAP client tool kit (supporting SOAP version 1.1 and above), and the development environment for the tool kit. For example, if you use a Visual Basic tool kit, you must have Visual Basic installed on your system.

API Architecture

The API architecture is designed to allow NSConfig client requests to be routed, through the HTTP daemon running on the target NetScaler, to a SOAP handler that translates the SOAP request into a call to the (internal) kernel configuration API.

Figure 1. The API Architecture



The order in which the NetScaler processes requests through the API is as follows:

- The client formats a request containing XML conforming to the SOAP protocol and sends it to the NetScaler.
- The HTTPD server instance on the NetScaler routes this request to a SOAP handler.
- The SOAP handler interprets the SOAP headers and maps the enclosed request to an internal configuration function.
- The kernel acts on the request and returns one or more responses.
- The SOAP handler translates the response(s) to a SOAP response message.
- The XML response is sent back to the client in an HTTP response.

The NSConfig Interface

The NSConfig interface closely mirrors the structure of the NetScaler command line interface (CLI). Administrators and programmers who are familiar with the CLI can easily create and implement custom applications to query or set the configuration on their NetScaler.

The NSConfig interface includes methods for most of the CLI commands. In most cases the method and the command name are the same. See the PortType section of the WSDL for a complete list of methods and their names.

For example, you use the add lb vserver CLI command to create a load balancing virtual server, as follows:

add lb vserver <vServerName> <serviceType> [<IPAddress> <port>]

where:

<vServerName> = A name for the virtual server.

<serviceType> = (HTTP | FTP | TCP | UDP).

<IPAddress> = The IP address used by the virtual server.

<port> = The port that the virtual server listens on.

Following is the corresponding API call, in the C language:

```
int ns__addlbvserver(void *handle,
      string vServerName,
      string serviceType,
      string IPAddress,
      unsignedShort port,
    ns__addlbvserverResponse *out);
```

Note: The exact syntax of the API call depends on the language used to write the client program. The above `ns__addlbvserver` function prototype is similar to the one that would be generated by the gSOAP package at http://www.cs.fsu.edu/~engelen/soap.html.

The result returned for all NSConfig requests consists of:

Rc

An integer return code. The value is zero if the request succeeded. A non-zero value indicates that the request failed.

Message

A string message. Contains meaningful information only if the request fails (rc is non-zero) (for example, “Required argument missing”).

List

A type-specific list of result entities. This element is present only for requests that retrieve information from the NetScaler. For example, the API method names starting with get, which correspond to the CLI show commands, return a list.

Command names in the NetScaler CLI typically consist of three terms, separated by spaces, identifying the operation, the feature that is being operated on, and the specific item that is being operated on. For example, to create a new application firewall profile, you type add appfw profile, followed by the command arguments. The corresponding API methods omit the spaces. For example, the API method for add appfw profile is `addappfwprofile`. The same principle applies to CLI command names that have only two terms. For example, add monitor becomes `addmonitor`. The other exceptions to this pattern are as follows:

1. The CLI show command is changed to get in the API, as shown below.

   show lb vserver => `getlbvserver`

   show service => `getservice`

2. The following commands are omitted from the API:

   - Commands that apply to the CLI itself (for example, clear CLI prompt).
   - The batch, ping, grep, more, shell, and scp commands.
   - The show router bgp and show router map commands.
   - All stat commands.

3. Message "part" names in the API are the same as the corresponding CLI argument names. As in the CLI, case does not matter, and these names can be abbreviated. For more information, *Citrix NetScaler Command Reference Guide* at http://support.citrix.com/article/CTX132384

4. The result of a GET method (which corresponds to a show command in the CLI) is always an array of a type defined in the WSDL. The elements of these complex types generally correspond to arguments to the corresponding add/set command/method.

5. Authorization must be performed once, by sending a login request. The response contains a Set-Cookie HTTP header, and the cookie must be sent with each subsequent request. This is addressed in the Perl examples using by HTTP::Cookies. HTTP::Cookies are used for API client authentication purposes (to log into the NetScaler). In Perl, SOAP::Lite cannot perform this authentication process; HTTP::Cookies are used instead.

6. In some programming languages, such as Perl, it is possible to invoke the programming language API without using the WSDL.

Examples of API Usage

The following examples show how to develop an API call from a standard CLI command, how to generate the SOAP request, and how the NetScaler responds to that request:

Example: Setting the Configuration

Example: Querying the Configuration

Example: Setting the Configuration

This example shows a CLI command, the corresponding API method, the resulting XML request, and the XML response that is sent back to the client.

Note: The actual API method and the XML SOAP message contents may differ from the example shown below. The XML shown will be encased in a SOAP envelope, which will in turn be carried in an HTTP message. For more information, see the W3C web site at http://www.w3.org/TR/SOAP.

The following CLI command creates a Load Balancing virtual server:

> add lb vserver vipLB1 HTTP 10.100.101.1 80

Following is the corresponding API method:

> ns__addlbvserver (handle, “vipLB1”, “HTTP”, “10.100.101.1”, 80, &out);

The XML generated for this request is as follows.

```
<ns:addlbvserver>
<vServerName xsi:type="xsd:string" >vipLB1</vServerName>
<serviceType xsi:type="ns:vservicetypeEnum>HTTP</ serviceType>
<IPAddress xsi:type="xsd:string">10.100.101.1</IPAddress>
<port xsi:type="xsd:unsignedInt" >80</port>
< /ns:addlbvserver >
```

The XML response to the above request is as follows.

```
<ns:addlbvserverResponse>
<rc xsi:type="xsd:unsignedInt">0</rc>
<message xsi:type="xsd:string">Done</message>
</ns:addlbvserverResponse>
```

Example: Querying the Configuration

This example shows an API request that queries the configuration and receives a list of entities.

Note: The actual API method and the XML SOAP message contents may differ from the example shown below.

The following CLI command shows the configured Load Balancing virtual servers:

> show lb vservers

Sample output of the show lb vservers command is as follows.

```
> show lb vservers
2 configured virtual servers:
1)  vipLB1 (10.100.101.1:80) - HTTP Type: ADDRESS State:
   DOWN
   Method: LEASTCONNECTION Mode: IP
   Persistence: NONE
2)  vipLB2 (10.100.101.2:80) - HTTP Type: ADDRESS State:
   DOWN
   Method: LEASTCONNECTION Mode: IP
   Persistence: NONE
Done
```

Following is the corresponding API method to show the list of Load Balancing virtual servers.

ns__getlbvserver(handle, NULL, &out)

The XML generated for this request is as follows.

```
<ns:getlbvserver></ns:getlbvserver>
```

The XML response to the above request is as follows.

```
<ns:getlbvserverResponse>
   <rc xsi:type="xsd:unsignedInt">0</rc>
   <message xsi:type="xsd:string">Done</message>
   <List xsi:type="SOAP-ENC:Array"
      SOAP-ENC:arrayType="ns:lbvserver[2]">
      <item xsi:type="ns:lbvserver">
      <vServerName xsi:type="xsd:string>vipLB1
         </vServerName>
         <serviceType xsi:type="xsd:string>HTTP</ serviceType>
         <IPAddress xsi:type="xsd:string >10.100.101.1
         </IPAddress>
      <port xsi:type="xsd:unsignedInt">80</port>
   </item>
   <item xsi:type="ns:lbvserver">
```

```
            <vServerName xsi:type="xsd:string>vipLB2
            </vServerName>
            <serviceType xsi:type="xsd:string>HTTP</ serviceType>
            <IPAddress xsi:type="xsd:string >10.100.101.2
            </IPAddress>
               <port xsi:type="xsd:unsignedInt">80</port>
            </item>
         </List>
      </ns:getlbvserverResponse>
```

The Web Service Definition Language (WSDL)

The NetScaler WSDL describes services for the entire range of NetScaler services. The NetScaler provides two WSDL files:

NSConfig.wsdl

Configuration APIs are defined in this file. The NSConfig.wsdl file is found on the NetScaler at http://<NSIP>/api/NSConfig.wsdl, where <NSIP> is the IP address of your NetScaler. This file is much larger than the NSStat.wsdl file. With the help of a third-party tool (such as gSOAP), developers can use this file to generate client stubs. A custom application can then call the stubs to send requests to the NetScaler. The application can be in any standard programming language that is supported by the third-party tool. Common programming languages for this purpose include Perl, Java, C, and C#. You can use the filterwsdl command to select only the service definitions that are relevant to the API calls made in your script.

NSStat.wsdl

Statistical APIs are defined in this file. The NSStat.wsdl file is found on the NetScaler at http://<NSIP>/api/NSStat.wsdl, where <NSIP> is the IP address of your NetScaler.

Creating Client Applications with the NSConfig.wsdl File

A client application can be created by importing the NSConfig.wsdl file with the gSOAP WSDL Importer to create a header file with C or C++ declarations of the SOAP methods. The gSOAP compiler is then used to translate this header file into stubs for the client application.

1. Get the NSConfig.h header file from the WSDL file.

   a. Run the wsdl2h program that comes with gSOAP on the WSDL file. The wsdl2h program is in the following location.

      > ./wsdl2h NSConfig.wsdl

      The output of wsdl2h is as follows:

      ```
      **  The gSOAP WSDL parser for C and C++ 1.0.2
      **  Copyright (C) 2001-2004 Robert van Engelen, Genivia, Inc.
      **  All Rights Reserved. This product is provided "as is", without any warranty.
      Saving NSConfig.h
      Reading file 'NSConfig.wsdl'
      Cannot open file 'typemap.dat'
      Problem reading type map file typemap.dat.
      Using internal type definitions for C instead.
      ```

   b. Run the soapcpp2 program to compile the header file and complete the process, as shown below. > soapcpp2 NSConfig.h
2. Generate the XML files and stubs as follows:

   > ./soapcpp2 -c -i NSConfig.h

   Following is sample output for this command:

   ```
   **  The gSOAP Stub and Skeleton Compiler for C and C++ 2.4.1
   **  Copyright (C) 2001-2004 Robert van Engelen, Genivia, Inc.
   **  All Rights Reserved. This product is provided "as is", without any warranty.
   Saving soapStub.h
   Saving soapH.h
   Saving soapC.c
   Saving soapClient.c
   Saving soapServer.c
   Saving soapClientLib.c
   Saving soapServerLib.c
   Using ns1 service name: NSConfigBinding
   Using ns1 service location: http://NetScaler.com/api Using ns1 schema namespace: urn:NSConfig
   Saving soapNSConfigBindingProxy.h client proxy
   Saving soapNSConfigBindingObject.h server object
   ```

```
Saving NSConfigBinding.addserver.req.xml sample SOAP/XML request
Saving NSConfigBinding.addserver.res.xml sample SOAP/XML response
Saving NSConfigBinding.disableserver.req.xml sample SOAP/ XML request
Saving NSConfigBinding.disableserver.res.xml sample SOAP/ XML response
Saving NSConfigBinding.enableserver.req.xml sample SOAP/ XML request
Saving NSConfigBinding.enableserver.res.xml sample SOAP/ XML response
[ ... Similar lines clipped ... ]
Saving NSConfigBinding.nsmap namespace mapping table
Compilation successful
```

This creates the stub files soapC.c, soapClient.c and stdsoap2.c.

3. Link the stub files you created with your source code to create a stand-alone binary that invokes the API.

Filter WSDL

The NetScaler WSDL describes services for the entire range of NetScaler services. When you use the NetScaler API in your scripts, by linking to the WSDL and attempting to compile the application, the entire WSDL is included, unnecessarily increasing compilation time and the size of the program.

Filter WSDL is a tool for selecting only those service definitions from the NetScaler WSDL that are relevant to the API calls made in the script. You can use the filter WSDL tool to filter NSConfig.wsdl and NSStat.wsdl files.

The NetScaler provides two WSDL files, one for the configuration APIs (NSConfig.wsdl) and the other for statistical APIs (NSStat.wsdl). The WSDL file for the configuration API is much larger. Therefore, it is important to use filter WSDL when compiling programs written with the configuration API.

Filter WSDL is a program that works on the Windows, FreeBSD and Linux platforms, and it can be run from the CLI.

The syntax for running filter WSDL is as follows:

filterwsdl <fromwsdl> <pattern>

where:

fromwsdl = The wsdl file that you want to filter

pattern = API method names or patterns that should be filtered

For example, if you want to filter all the service definitions for the API method addlbvserver from the NetScaler WSDL file, NSConfig.wsdl, you can use the command:

> filterwsdl NSConfig.wsdl "addlbvserver"

The output of this command is sent to the screen by default, but it can be redirected to a file on the NetScaler by using the UNIX redirect operator (>). The output of the previous command can be saved into a file called NSConfig-Custom.wsdl by using the command as follows:

> filterwsdl NSConfig.wsdl "addlbvserver" > NSConfig-Custom.wsdl

In this case, the original WSDL file is 1.58 MB, but the filtered WSDL file is 6 KB.

The pattern used in the filterwsdl command can include the + and - operators and the wildcard operator (*) to create more generic filters.

For example, if you want to filter the service definitions for all the available load balancing methods, you can use the following command:

> filterwsdl NSConfig.wsdl "*lb"*

This command will filter all the Load Balancing methods but will also include GSLB methods, because the pattern lb will be matched by all GSLB methods also. To include only LB methods and exclude all GSLB methods, use the command as follows:

> filterwsdl NSConfig.wsdl +"*lb" -"glsb"*

Securing API Access

Secure access to CLI objects can be based on the NetScaler IP address or on the subnet IP address on which the NetScaler is deployed. To provide secured API access based on the NetScaler IP address, you must configure the NetScaler to use transparent SSL mode with clear text port.

To configure secure API access based on the NetScaler IP

1. Create a loopback SSL service and configure it use transparent SSL mode with clear text port:

   add service secure_xmlaccess 127.0.0.1 SSL 443 -clearTextPort 80

2. Add certificate and key:

   add certkey cert1 –cert /nsconfig/ssl/ssl/cert1024.pem –key /nsconfig/ssl/ssl/rsakey.pem

   Note: You can use an existing certificate and key or use the NetScaler Certificate Authority Tool to create a key and test certificate for secure access.

3. Bind the certificate and key to the service:

   bind certkey secure_xmlaccess cert1 -Service

4. Add a custom TCP monitor to monitor the SSL service you have added:

   add monitor ssl_mon TCP -destport 80

5. Bind the custom TCP monitor to the SSL service:

   bind monitor ssl_mon secure_xmlaccess

To configure secure API access based on the subnet IP

1. Create an SSL VIP in the appropriate subnet:

   add vserver <vServerName> SSL <Subnet-IP> 443

2. Create a loopback HTTP service:

   add service <serviceName> 127.0.0.1 HTTP 80

3. Bind the service to the SSL VIP:

   bind lb vserver <vServerName> <serviceName>

4. Add the certificate and the key:

   add certkey cert1 –cert /nsconfig/ssl/ssl/cert1024.pem –key /nsconfig/ssl/ssl/rsakey.pem

   Note: You can use an existing certificate and key or use the NetScaler Certificate Authority Tool to create a key and test certificate.

5. Bind the Certificate and the Key to the SSL VIP:

   bind certkey <vServerName> cert1

AppExpert

2015-05-17 05:03:59 UTC

Contents

AppExpert

The following topics provide a conceptual reference and configuration instructions for the AppExpert and other features of the NetScaler appliance.

Action Analytics	Collects run-time statistics on the basis of pre-defined criteria. When used with policies, the feature also provides you with the infrastructure for automatic, real-time traffic optimization.
AppExpert Applications and Templates	Simplify configuration steps for the Citrix® NetScaler® appliance by using applications, application templates, Access Gateway applications, and entity templates.
Entity Templates	Describes how to use entity templates to set up and configure individual NetScaler entities, such as a policy or virtual server. An entity template provides a specification and a set of defaults for the object.
HTTP Callouts	An HTTP request that the NetScaler appliance generates and sends to an external application when certain criteria are met during policy evaluation.
Pattern Sets	Allow string matching during the evaluation of a default syntax policy.
Policies and Expressions	Rules that determine the operations that the NetScaler appliance must perform.
Rate Limiting	Defines the maximum load for a given network entity or virtual entity on the NetScaler appliance.
Responder	Bases responses on who sends the request, where it is sent from, and other criteria with security and system management implications.
Rewrite	Rewrites information in the requests or responses handled by the NetScaler appliance.
String Maps	Perform pattern matching in all NetScaler features that use the default policy syntax.

Action Analytics

The performance of your website or application depends on how well you optimize the delivery of the most frequently requested content. Techniques such as caching and compression help accelerate the delivery of services to clients, but you need to be able to identify the resources that are requested most frequently, and then cache or compress those resources. You can identify the most frequently used resources by aggregating real-time statistics about website or application traffic. Statistics such as how frequently a resource is accessed relative to other resources and how much bandwidth is consumed by those resources help you determine whether those resources need to be cached or compressed to improve server performance and network utilization. Statistics such as response times and the number of concurrent connections to the application help you determine whether you must enhance server-side resources.

If the website or application does not change frequently, you can use products that collect statistical data, and then manually analyze the statistics and optimize the delivery of content. However, if you do not want to perform manual optimizations, or if your website or application is dynamic in nature, you need infrastructure that can not only collect statistical data but can also automatically optimize the delivery of resources on the basis of the statistics. On the NetScaler appliance, this functionality is provided by the action analytics feature. The feature operates on a single NetScaler appliance and collects run-time statistics on the basis of criteria that you define. When used with NetScaler policies, the feature also provides you with the infrastructure that you need for automatic, real-time traffic optimization.

When configuring the action analytics feature, you specify the request attributes for which you want to collect statistical data (for example, URLs and HTTP methods) by configuring default syntax expressions in an entity called a selector. Then, you configure an identifier to configure settings such as the sampling interval and sample count. You also configure a policy that enables the appliance to evaluate traffic as specified by the selector-identifier pair. Finally, you bind the policy to a bind point to begin collecting statistics.

The appliance also provides you with a set of built-in selectors, identifiers, and responder policies that you can use to get started with the feature.

The appliance aggregates the following statistics:

- The number of requests.
- The bandwidth consumed by the requests.
- The response time.
- The number of concurrent connections.

You can configure the feature to perform run-time sorting of the records on an attribute of your choice. You can view the statistical data by using either the command-line interface or the Stream Sessions tool in the configuration utility.

Action Analytics

The performance of your website or application depends on how well you optimize the delivery of the most frequently requested content. Techniques such as caching and compression help accelerate the delivery of services to clients, but you need to be able to identify the resources that are requested most frequently, and then cache or compress those resources. You can identify the most frequently used resources by aggregating real-time statistics about website or application traffic. Statistics such as how frequently a resource is accessed relative to other resources and how much bandwidth is consumed by those resources help you determine whether those resources need to be cached or compressed to improve server performance and network utilization. Statistics such as response times and the number of concurrent connections to the application help you determine whether you must enhance server-side resources.

If the website or application does not change frequently, you can use products that collect statistical data, and then manually analyze the statistics and optimize the delivery of content. However, if you do not want to perform manual optimizations, or if your website or application is dynamic in nature, you need infrastructure that can not only collect statistical data but can also automatically optimize the delivery of resources on the basis of the statistics. On the NetScaler appliance, this functionality is provided by the action analytics feature. The feature operates on a single NetScaler appliance and collects run-time statistics on the basis of criteria that you define. When used with NetScaler policies, the feature also provides you with the infrastructure that you need for automatic, real-time traffic optimization.

When configuring the action analytics feature, you specify the request attributes for which you want to collect statistical data (for example, URLs and HTTP methods) by configuring default syntax expressions in an entity called a selector. Then, you configure an identifier to configure settings such as the sampling interval and sample count. You also configure a policy that enables the appliance to evaluate traffic as specified by the selector-identifier pair. Finally, you bind the policy to a bind point to begin collecting statistics.

The appliance also provides you with a set of built-in selectors, identifiers, and responder policies that you can use to get started with the feature.

The appliance aggregates the following statistics:

- The number of requests.
- The bandwidth consumed by the requests.
- The response time.
- The number of concurrent connections.

You can configure the feature to perform run-time sorting of the records on an attribute of your choice. You can view the statistical data by using either the command-line interface or the Stream Sessions tool in the configuration utility.

Configuring a Selector

A selector is a filter for identifying requests. It consists of up to five individual default syntax expressions that identify request attributes such as the client IP address and the URL in the request. Each expression is a non-compound default syntax expression and is considered to be in an AND relationship with the other expressions. Following are some examples of selector expressions:

- `HTTP.REQ.URL`
- `CLIENT.IP.SRC`
- `HTTP.RES.BODY(1000).AFTER_STR(\"<string>\").BEFORE_STR(\"<string>\")"`
- `CLIENT.IP.SRC.SUBNET(24)`

Selectors are used in rate limiting and action analytics configurations. A selector is optional in a rate limiting configuration, but is required in a action analytics configuration.

The order in which you specify parameters is significant. For example, if you configure an IP address and a domain (in that order) in one selector, and then specify the domain and the IP address (in the reverse order) in another selector, the NetScaler considers these values to be unique. This can lead to the same transaction being counted twice. Also, if multiple policies invoke the same selector, the NetScaler, again, can count the same transaction more than once.

If you modify an expression in a selector, you may get an error if any policy that invokes it is bound to a new policy label or bind point. For example, suppose that you create a selector named myLimitSelector1, invoke it from myLimitID1, and invoke the identifier from a DNS policy named dnsRateLimit1. If you change the expression in myLimitSelector1, you might receive an error when binding dnsRateLimit1 to a new bind point. The workaround is to modify these expressions before creating the policies that invoke them.

The NetScaler appliance provides the following built-in selectors for some of the most common use cases:

Table 1. Built-in Selectors

Selector	Selector Expressions
`Top_URL`	`HTTP.REQ.URL`
`Top_CLIENTS`	`CLIENT.IP.SRC`
`Top_URL_CLIENTS_LBVSERVER`	1. `HTTP.REQ.URL` 2. `CLIENT.IP.SRC` 3. `HTTP.REQ.LB_VSERVER.NAME`

Top_URL_CLIENTS_CSVSERVER	1. HTTP.REQ.URL 2. CLIENT.IP.SRC 3. HTTP.REQ.CS_VSERVER.NAME
Top_MSSQL_QUERY_DB_LBVSERVER	1. MSSQL.REQ.QUERY.TEXT 2. MSSQL.REQ.LB_VSERVER.NAME
Top_MYSQL_QUERY_DB_LBVSERVER	1. MYSQL.REQ.QUERY.TEXT 2. MYSQL.REQ.LB_VSERVER.NAME

You can also configure a selector with expressions that identify the request attributes of your choice. For example, you might want to create a record for a request that arrives with a specific header. To evaluate the header, you can add `HTTP.REQ.HEADER("<header_name>")` to the selector that you intend to use.

To configure a selector by using the command line interface

At the command prompt, type the following commands to configure a selector and verify the configuration:

- add stream selector <*name*> <*rule*> ...
- show stream selector

Example

```
> add stream selector myselector HTTP.REQ.URL CLIENT.IP.SRC
 Done
> show stream selector myselector
    Name: myselector
    Expressions:
        1) HTTP.REQ.URL
        2) CLIENT.IP.SRC
 Done
>
```

To modify or remove a selector by using the command line interface

- To modify a selector, type the set stream selector command, the name of the selector, and the rule parameter with the expressions. Enter the existing expressions that you want to retain, along with the new expressions that you want to add.
- To remove a selector, type the rm stream selector command and the name of the selector.

Parameters for configuring a selector

name

The name of the selector. Must begin with a letter, a number, or the underscore character (_). Additional characters allowed, after the first character, are the number sign (#), period (.), space ( ), colon (:), at sign (@), equal sign (=) and hyphen (-). If the name includes one or more spaces, enclose the name in quotation marks or single quotes (for example, "my selector" or 'my selector'). Maximum length: 31 characters.

rule

A set of up to five individual, non-compound default syntax expressions that are treated as being in a logical AND relationship with one another. Each expression identifies one component of a request or response. For example, the expression HTTP.REQ.URL identifies the URL component in the request, and CLIENT.IP.SRC identifies the client IP address.

You can change an expression if the selector is not yet specified in an identifier. If the selector is specified in an identifier, you can only change the order of the expressions, not the expressions themselves.

To configure a selector by using the configuration utility

1. Navigate to AppExpert > Action Analytics > Selectors.
2. In the details pane, do one of the following:
   - To create a selector, click Add.
   - To modify a selector, select the selector, and then click Open.
3. In the Create Limit Selector or Configure Limit Selector dialog box, set one or more of the following parameters:
   - Name
   - Expressions

     To add the expression to the selector configuration, click Add. To remove an expression from the selector configuration, in the Expression box, select the expression, and then click Remove.

     Note: In the Expressions box, enter a valid parameter. For example, enter `HTTP`. Then, enter a period after this parameter. A drop-down menu appears. The contents of this menu provide the keywords that can follow the initial keyword that you entered. To select the next keyword in this expression prefix, double-click the selection in the drop-down menu. The Expressions text box displays both the first and second keywords for the expression prefix, for example, `HTTP.REQ`. Continue adding expression components until the complete expression is formed.
4. Click Add.
5. Continue adding up to five non-compound expressions.
6. Click Create or OK.

Configuring a Stream Identifier

You configure a stream identifier to specify parameters for collecting statistical data from requests identified by a given selector. An identifier specifies the selector to be used, the statistics collection interval, the sample count, and the field on which the records are to be sorted.

The NetScaler appliance includes the following built-in stream identifiers for common use cases. All the built-in identifiers specify a sample count of 1 and an interval of 1 minute. Additionally, they sort the data on the REQUESTS attribute. They differ only in being associated with different built-in selectors. Each built-in identifier is associated with a built-in selector of the same name (for example, the built in identifier Top_URL is associated with the built-in selector Top_URL). Following are the built-in identifiers:

- Top_URL
- Top_CLIENTS
- Top_URL_CLIENTS_LBVSERVER
- Top_URL_CLIENTS_CSVSERVER
- Top_MSSQL_QUERY_DB_LBVSERVER
- Top_MYSQL_QUERY_DB_LBVSERVER

For more information about the built-in selectors, see "Configuring a Selector."

Note: The maximum length for storing string results of selectors (for example, HTTP.REQ.URL) is 60 characters. If the string (for example, URL) is 1000 characters long, of which 50 characters are enough to uniquely identify a string, use an expression to extract only the required 50 characters.

You cannot modify a built-in identifier's configuration. However, you can create an identifier with a configuration of your choice.

To configure a stream identifier by using the command line interface

At the command prompt, type the following commands to configure a stream identifier and verify the configuration:

- add stream identifier <*name*> <*selectorName*> [-interval <*positive_integer*>] [-SampleCount <*positive_integer*>] [-sort <*sort*>]
- show stream identifier <*name*>

Example

```
> add stream identifier myidentifier Top_URL -interval 10 -sampleCount 100
 Done
```

Parameters for configuring a stream identifier

name (Name)

A name for the stream identifier. Must begin with an ASCII alphabetic character or an underscore (_). After the first character, use only ASCII alphanumeric characters and underscores. Maximum length: 31 characters.

selectorName (Selector)

The name of the selector. Must begin with a letter, a number, or the underscore character (_). Additional characters allowed, after the first character, are the number sign (#), period (.), space ( ), colon (:), at sign (@), equal sign (=) and hyphen (-). If the name includes one or more spaces, enclose the name in quotation marks or single quotes (for example, "my selector" or 'my selector').

When this parameter is modified, the appliance flushes all the records that have been created for the stream identifier, including any records that have been created for pending or in-progress responses. For an in-progress response, the appliance does not replace the flushed record, and the data associated with that data transfer is lost.

Maximum length: 31 characters.

interval (Interval)

The number of minutes up to which an inactive record must be retained. Therefore, this is a record's expiry time. The interval is divided into four subintervals. When the interval progresses by a subinterval, the appliance discards one fourth of the data that it collected during the trailing subinterval. For example, an interval of 2 minutes is divided into four subintervals of 30 seconds each. Every 30 seconds, the appliance discards one-fourth of the data collected during the previous 30 seconds. Statistics for response times and concurrent connections are dynamic in nature, and depend on recent activity. Statistics for the number of requests and bandwidth consumption are also aged over the interval to eliminate stale data.

When this parameter is modified, the appliance flushes all accumulated session records, except any records that might be associated with pending or in-progress responses at the moment the parameter is modified. For records that might be associated with pending or in-progress responses, the appliance only updates the expiry time (interval time).

Maximum value: 4294967295. Default: 1.

sampleCount (Sample Count)

The size of the sample from which a request should be selected for evaluation. The smaller the sample count, the more accurate is the statistical data. If you want the appliance to evaluate all requests, set the sample count to 1. However, a setting of 1

can result in the consumption of a considerable amount of memory and processing resources.

When this parameter is modified, the appliance flushes all accumulated session records, except any records that might be associated with pending or in-progress responses at the moment the parameter is modified. For records that might be associated with pending or in-progress responses, the appliance only updates the expiry time (interval time).

Minimum value: 1. Maximum value: 4294967295. Default: 1.

sort (Sort)

Sort the records, in descending order of their values in the specified statistics column. This sorting is performed during data collection, and it enables the evaluation of the data through NetScaler policies (for example, compression and caching policies) that use functions such as `IS_TOP(n)`.

When this parameter is modified, the appliance flushes all accumulated session records, except any records that might be associated with pending or in-progress responses at the moment the parameter is modified. For records that might be associated with pending or in-progress responses, the appliance only updates the expiry time (interval time).

Possible values: REQUESTS, CONNECTIONS, RESPTIME, BANDWIDTH, NONE. Default: REQUESTS.

To configure a stream identifier by using the configuration utility

1. Navigate to AppExpert > Action Analytics > Stream Identifiers.
2. In the details pane, do one of the following:
   - To create a stream identifier, click Add.
   - To modify a stream identifier, select the identifier, and then click Open.
3. In the Configure Stream Identifier dialog box, set one or more of the following parameters:
   - Name
   - Selector
   - Interval
   - Sample Count
   - Sort
4. Click Create or OK, and then click Close.

Viewing Statistics

You can view the collected statistics in tabular format in the command-line interface and in graphical format in the configuration utility.

The following table describes the collected statistics:

Table 1. Statistical Information Displayed for a Stream Identifier

Statistics	Column name in the output of the stat stream identifier <*identifier name*> command	Description
Number of requests	`Req`	The number of requests for which records were created in the last `<interval>` number of minutes.
Bandwidth consumed	`BandW`	The total bandwidth consumed by the requests that were received in the last `<interval>` number of minutes. The total bandwidth of a request is the bandwidth consumed by the request and its response. The value is rounded off to the next higher or next lower integer value. Consequently, it might differ slightly from the expected value. For example, if a request's total bandwidth consumption is 2.2 KB, one instance of the request might be shown as having consumed 2 KB and two instances might be shown as having consumed 4 KB, but three instances might be shown as having consumed 7 KB.
Response time	`RspTime`	The average response time for all the requests received in the last `<interval>` number of minutes.

Concurrent connections	Conn	The total number of concurrent connections that are currently open.

To view the statistical data collected for a stream identifier by using the command line

At the command prompt, type:

stat stream identifier <name> [<pattern> ...] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-sortBy <sortBy> [<sortOrder>]

Examples

Example 1 sorts the output on the BandW column, in the descending order. Example 2 sorts the output in Example 1, on the Req column, and in the ascending order

Example 1

```
> stat stream identifier myidentifier -sortBy BandW Descending -fullValues
Stream Session statistics
              Req          BandW
User1         508         125924
User2        5020          12692
User3        2025           4316

           RspTime          Conn
User1        5694             0
User2         109             0
User3           3             0
 Done
```

Example 2

```
> stat stream identifier myidentifier -sortBy Req Ascending –fullValues
Stream Session statistics
              Req          BandW
User1         508         125924
User3        2025           4316
User2        5020          12692

           RspTime          Conn
User1        5694             0
User3           3             0
User2         109             0
 Done
```

Parameters for viewing the statistical data collected for a stream identifier

name (Name)

The name of the identifier. Maximum length: 127.

fullValues

Display the complete row title. If you do not specify this option, the row title is shortened to reduce the width of the display. Only the first few characters and the last few characters of each row title are displayed, separated by a string of periods. For example, the row title `/mypagename.html` is shortened to `/myp....html`.

ntimes

Run the command `n` times, once every 7 seconds.

logFile

The name of a log file that contains the data that you want the appliance to analyze. Possible values: `NSLOG`, `NONE`. Default: `NSLOG`.

sortBy

Sort the output on the specified attribute, in the order specified for the sortOrder parameter. Possible values: `BandW`, `Conn`, `Req`, and `RspTime`.

sortOrder

The order in which you want to sort the output. Possible values: Ascending, Descending. Default: Descending.

To view the statistical data collected for a stream identifier by using the configuration utility

1. Navigate to AppExpert > Action Analytics > Stream Identifiers.
2. Select the stream identifier whose sessions you want to view, and then click Stream Sessions. For information about how you can group the output on the basis of the values collected for various selector expressions, see "Grouping Records on Attribute Values."

Grouping Records on Attribute Values

Statistical information such as the number of times a particular URL has been accessed overall and per client, and the total number of GET and POST requests per client can provide valuable insights into whether any of your resources need to be expanded to meet the demand or be optimized for delivery. To obtain such statistics, you must use an appropriate set of selector expressions, and then use the pattern parameter in the stat stream identifier command. The grouping is based on the pattern that is specified in the command. Grouping can be performed concurrently on the values of multiple expressions.

In the command-line interface, you can group the output by using patterns of your choice. In the configuration utility, the pattern depends on the choices you make when drilling down through the values of various selector expressions. For example, consider a selector that has the expressions `HTTP.REQ.URL`, `CLIENT.IP.SRC`, and `HTTP.REQ.LB_VSERVER.NAME`, in that order. The statistics home page displays icons for each of these expressions. If you click the icon for `CLIENT.IP.SRC`, the output is based on the patterns `* ? *`. The output displays statistics for each client IP address. If you click an IP address, the output is based on the patterns `* <IP address> ?` and `? <IP address> *` where `<IP address>` is the IP address you selected. In the resulting output, if you click a URL, the pattern used is `<URL> <IP address> ?`.

To group the records on the values of selector expressions by using the command line interface

At the command prompt, enter the following command to group the records on the basis of a selector expression:

stat stream identifier <name> [<pattern> ...]

Examples

Each example uses a different pattern to demonstrate the effect of the pattern on the output of the stat stream identifier command. The selector expressions are `HTTP.REQ.URL` and `HTTP.REQ.HEADER("UserHeader")`, in that order. The requests contain a custom header whose name is `UserHeader`. Note that in the examples, a given statistical value changes as determined by the grouping, but the sum total of the values for a given field remains the same.

Example 1

In the following command, the pattern used is `? ?`. The appliance groups the output on the values collected for both selector expressions. The row headers consist of the expression values separated by a question mark (?). The row with the header `/mysite/mypage1.html?Ed` displays statistics for requests made by user `Ed` for the URL `/mysite/mypage1.html`.

> stat stream identifier myidentifier ? ? -fullValues
Stream Session statistics

```
                                  Req             BandW
/mysite/mypage2.html?Grace          1              2553
/mysite/mypage1.html?Grace          2                 4
/mysite/mypage1.html?Ed             8                16
/mysite/mypage2.html?Joe            1              2554
/mysite/mypage1.html?Joe            5                10
/mysite/?Joe                    1               4

                               RspTime            Conn
/mysite/mypage2.html?Grace          0                 0
/mysite/mypage1.html?Grace          0                 0
/mysite/mypage1.html?Ed             0                 0
/mysite/mypage2.html?Joe            0                 0
/mysite/mypage1.html?Joe            0                 0
/mysite/?Joe                    6               0
 Done
```

Example 2

In the following command, the pattern used is `* ?`. The appliance groups the output on the values accumulated for the second expression `HTTP.REQ.HEADER("UserHeader")`. The rows display statistics for all requests made by users `Grace`, `Ed`, and `Joe`.

```
> stat stream identifier myidentifier * ?
Stream Session statistics
            Req    BandW  RspTime    Conn
Grace         3     2557       0       0
Ed            8       16       0       0
Joe           7     2568       6       0
 Done
```

Example 3

In the following command, the pattern used is `? *`, which is the default pattern. The output is grouped on the values collected for the first selector expression. Each row displays statistics for one URL.

```
> stat stream identifier myidentifier ? * -fullValues
Stream Session statistics
                              Req             BandW
/mysite/mypage2.html            2              5107
/mysite/mypage1.html           15                30
/mysite/                        1                 4

                              RspTime            Conn
/mysite/mypage2.html            0                 0
/mysite/mypage1.html            0                 0
/mysite/                        6                 0
 Done
```

Example 4

In the following command, the pattern used is `* *`. The appliance displays one set of collective statistics for all the requests received, with no row title.

```
> stat stream identifier myidentifier * *
Stream Session statistics
            Req    BandW  RspTime     Conn
             18     5141        6        0
 Done
```

Example 5

In the following command, the pattern is `/mysite/mypage1.html *`. The appliance displays one set of collective statistics for all the requests received for the URL `/mysite/mypage1.html`, with no row title.

```
> stat stream identifier myidentifier /mysite/mypage1.html *
Stream Session statistics
            Req    BandW  RspTime     Conn
             15       30        0        0
 Done
```

Parameters for grouping records on the values of selector expressions

name

The name of the stream identifier for which you want to view statistics.

pattern

A pattern consisting of asterisks (*) and question marks (?). The pattern can also begin with a text string. Each element in the pattern has a one-to-one correspondence with the expressions in the selector that is configured for the stream identifier. A question mark specifies that the values accumulated for the corresponding selector expression must be considered when grouping is performed on the records. Values on which grouping is performed are displayed in the output as row titles. If two or more fields have to be considered for grouping, they are separated by a question mark in the output. An asterisk specifies that the values accumulated for the corresponding expression must not be considered when grouping is performed on the records.

As an example, consider that you have configured a selector that consists of the expressions `HTTP.REQ.URL` and `CLIENT.IP.SRC` (in that order), and that the appliance has accumulated records of a number of requests for two URLs, `example.com/abc.html` and `example.com/def.html`, from two client IP addresses, 192.0.2.10 and 192.0.2.11.

With a pattern of `? ?`, the appliance performs grouping on both fields and displays statistics for the following:

- Requests for `example.com/abc.html` from 192.0.2.10, with a row title of `example.com/abc.html?192.0.2.10`.
- Requests for `example.com/abc.html` from 192.0.2.11, with a row title of `example.com/abc.html?192.0.2.11`.
- Requests for `example.com/def.html` from 192.0.2.10, with a row title of `example.com/def.html?192.0.2.10`.
- Requests for `example.com/def.html` from 192.0.2.11, with a row title of `example.com/def.html?192.0.2.11`.

With a pattern of `* ?`, the appliance performs grouping on only the client IP address values and displays statistics for the following requests:

- All requests from 192.0.2.10, with the IP address as the row title.
- All requests from 192.0.2.11, with the IP address as the row title.

With a pattern of `? *`, the appliance performs grouping on only the URL values and displays statistics for the following requests:

- All requests for `example.com/abc.html`, with the URL as the row title.
- All requests for `example.com/def.html`, with the URL as the row title.

With a pattern of `* *`, the appliance displays one set of collective statistics for all the requests received, with no row title.

If the pattern begins with a text string, the appliance performs a lookup for all the records that have the string in the first field. For example, if the pattern in the previous example is changed to `example.com/abc.html ?`, the appliance displays statistics for requests for `example.com/abc.html` from each unique client IP address. A string can be used only for the first selector expression.

The one-to-one correspondence with the selector expressions means that the pattern can have a maximum of five elements. If you do not specify a pattern, the appliance assumes a pattern of `? * * * *` and groups the records on the values of the first expression in the selector. Maximum length: 639.

To group the records on the values of selector expressions by using the configuration utility

1. Navigate to AppExpert > Action Analytics > Stream Identifiers.
2. In the details pane, click the stream identifier for which you want to view statistics, and then click Stream Sessions.
3. On the Home page, click the icon for the stream selector by which you want to group the output.
4. To return to the Home page from the statistics page for a selector expression, click Home.
5. To view statistics for the value of a given selector expression, click the value. You can repeat this step for a selector expression value in each subsequent output until you obtain the statistics you want.

Clearing a Stream Session

You can flush all the records that have been accumulated for a stream identifier.

To clear a stream session by using the command line interface

At the command prompt, enter the following commands to clear a stream session and verify the results:

- clear stream session <name>
- stat stream identifier <name>

Example

This example uses the stat stream identifier command first, so that a comparison can be made with the stat stream identifier command that is used for verifying the result of the clear stream session command.

```
>stat stream identifier myidentifier
Stream Session statistics
                Req    BandW  RspTime     Conn
/aed....html      2        0        0        0
/               636      303       12        0
 Done
>clear stream session myidentifier
 Done
>stat stream identifier myidentifier
 Done
```

To clear a stream session by using the configuration utility

1. Navigate to AppExpert > Action Analytics > Stream Identifiers.
2. Select the stream identifier whose sessions you want to clear, and then click Clear Sessions.

Configuring a Policy for Analyzing and Optimizing Traffic

To put the selector-identifier pair in your action analytics configuration into effect, you must associate the pair with the point in the traffic flow at which you want to collect statistics. You can do so by configuring a default syntax policy and referencing the stream identifier from the policy rule. You can use compression policies, caching policies, rewrite policies, application firewall policies, responder policies, and any other policies whose action is based on a Boolean expression.

The action analytics feature introduces a set of default syntax expressions and functions for collecting and evaluating data. The expression `ANALYTICS.STREAM(<identifier_name>)` is used for referencing the identifier that you want to use. The expression `COLLECT_STATS` is used to collect statistical data. Functions such as `IS_TOP(<uint>)` and `IS_TOP_FREQUENTS(<uint>)` are used for making automatic, real-time traffic optimization decisions.

- **IS_TOP(<number>).** Finds if a given object is in the top <number> of elements. For example, is the element among the top 10 elements. When multiple elements have the count, they are considered to be similar in nature. The sort function must be turned on to avoid an undef condition.

- **IS_TOP_FREQUENTS(<frequency>).** Finds if a given object is in the top <frequency> of the elements that are in the top elements. For example, is the element among the top 50% of all the top elements maintained. Elements having the same values are considered similar in nature. The sort function must be turned on to avoid an undef condition.

It is your policy configuration that determines whether the NetScaler appliance must only collect data from traffic or also perform an action. If the appliance must only collect statistical data, you can configure a policy with the rule `ANALYTICS.STREAM(<identifier_name>).COLLECT_STATS` and the action `NOOP`. The NOOP policy must be the policy with the highest priority at the bind point. This policy is sufficient if you are only collecting statistics. Traffic optimization decisions, such as what to compress or cache, must be based on manual, periodic evaluation of the statistical data.

If, in addition to collecting statistics, the appliance must also perform an action on the traffic, you must configure the gotoPriorityExpression parameter of the NOOP policy such that another policy that has the desired rule and action is evaluated subsequently. This second policy must have a rule that begins with the `ANALYTICS.STREAM(<identifier_name>)` prefix and a function that evaluates the data.

Following is an example of two responder policies that are configured and bound globally. The policy `responder_stat_collection` enables the appliance to collect statistics based on the identifier, `myidentifier`. The policy `responder_notify` evaluates the data that is collected.

Example

```
> add responder action send_notification respondwith '"You are in the Top 10 list for bandwidth consumption
 Done
> add responder policy responder_stat_collection' ANALYTICS.STREAM("myidentifier").COLLECT_STATS' NOOP
Done
> add responder policy responder_notify 'ANALYTICS.STREAM("myidentifier").BANDWIDTH.IS_TOP(10)' send_n
 Done
> bind responder global responder_stat_collection 10 NEXT
 Done
> bind responder global responder_notify 20 END
 Done
```

Use Case: Limiting Bandwidth Consumption per User or Client Device

Your web site, application, or file hosting service has finite network and server resources available to it to serve all its users. One of the most important resources is bandwidth. Substantial bandwidth consumption by only a subset of the user base can result in network congestion and reduced resource availability to other users. To prevent network congestion, you might have to limit a client's bandwidth consumption by using temporary service denial techniques such as responding to a client request with an HTML page if it has exceeded a preconfigured bandwidth value over a fixed time period leading up to the request.

In general, you can regulate bandwidth consumption either per client device or per user. This use case demonstrates how you can limit bandwidth consumption per client to 100 MB over a time period of one hour. The use case also demonstrates how you can regulate bandwidth consumption per user to 100 MB over a time period of one hour, by using a custom header that provides the user name. In both cases, the tracking of bandwidth consumption over a moving time period of one hour is achieved by setting the interval parameter in the stream identifier to 60 minutes. The use cases also demonstrate how you can import an HTML page to send to a client that has exceeded the limit. Importing an HTML page not only simplifies the configuration of the responder action in these use cases, but also simplifies the configuration of all responder actions that need the same response.

To limit bandwidth consumption per user or client device by using the command line interface

In the command-line interface, perform the following tasks to configure action analytics for limiting a client's or user's bandwidth consumption. Each step includes sample commands and their output.

1. **Set up your load balancing configuration.** Configure load balancing virtual server `mysitevip`, and then configure all the services that you need. Bind the services to the virtual server. The following example creates ten services and binds the services to `mysitevip`.

   ```
   > add lb vserver mysitevip HTTP 192.0.2.17 80
    Done
   > add service service[1-10] 192.0.2.[240-249] HTTP 80
   service "service1" added
   service "service2" added
   service "service3" added
   .
   .
   .
   service "service10" added
    Done
   > bind lb vserver vserver1 service[1-10]
   service "service1" bound
   ```

```
service "service2" bound
service "service3" bound
.
.
.
service "service10" bound
 Done
```

2. **Configure the stream selector.** Configure one of the following stream selectors:

   - To limit bandwidth consumption per client, configure a stream selector that identifies the client IP address.

     ```
     > add stream selector myselector CLIENT.IP.SRC
      Done
     ```

   - To limit bandwidth consumption per user on the basis of the value of a request header that provides the user name, configure a stream selector that identifies the header. In the following example, the name of the header is `UserHeader`.

     ```
     > add stream selector myselector HTTP.REQ.HEADER(“UserHeader”)
      Done
     ```

3. **Configure a stream identifier.** Configure a stream identifier that uses the stream selector. Set the interval parameter to 60 minutes.

   ```
   > add stream identifier myidentifier myselector -interval 60 -sampleCount 1 -sort BANDWIDTH
    Done
   ```

4. **Configure the responder action.** Import the HTML page that you want to send to users or clients that have exceeded the bandwidth consumption limit, and then use the page in responder action `crossed_limits`.

   ```
   > import responder htmlpage http://192.0.2.20:80/stdpages/wait.html crossed-limits.html
   This operation may take some time, Please wait...

    Done
   > add responder action crossed_limits respondwithhtmlpage crossed-limits.html
    Done
   ```

5. **Configure the responder policies.** Configure responder policy `myrespol1` with the rule `ANALYTICS.STREAM("myidentifier").COLLECT_STATS` and the action `NOOP`. Then, configure policy `myrespol2` for determining whether a client or user has crossed the 100 MB limit. The policy `myrespol2` is configured with the responder action `crossed_limits`.

   ```
   > add responder policy myrespol1 'ANALYTICS.STREAM("myidentifier").COLLECT_STATS' NOOP
    Done
   > add responder policy myrespol2 'ANALYTICS.STREAM("myidentifier").BANDWIDTH.GT(1048576)' crossed_
    Done
   ```

6. **Bind the responder policies to the load balancing virtual server.** The policy `myrespol1`, which only collects statistical data, must have the higher priority and a GOTO expression of `NEXT`.

```
> bind lb vserver mysitevip -policyName myrespol1 -priority 1 -gotoPriorityExpression NEXT
 Done
> bind lb vserver mysitevip -policyName myrespol2 -priority 2 -gotoPriorityExpression END
 Done
```

7. **Test the configuration.** Test the configuration by sending test HTTP requests, from multiple clients or users, to the load balancing virtual server and using the stat stream identifier command to view the statistics that are collected for the specified identifier. The following output displays statistics for clients.

```
> stat stream identifier myidentifier -sortBy BandW –fullValues
Stream Session statistics
                    Req         BandW
192.0.2.30          5000         3761
192.0.2.31          29          2602
192.0.2.32          25          51

                    RspTime     Conn
192.0.2.30          2           0
192.0.2.31          0           0
192.0.2.32          0           0
 Done
>
```

AppExpert Applications and Templates

An AppExpert application is a collection of configuration information that you set up on the Citrix NetScaler appliance for securing and optimizing traffic for a Web application, such as Microsoft SharePoint. Managing AppExpert applications is simplified by a graphical user interface (GUI) that allows you to specify application traffic subsets and a distinct set of security and optimization policies for processing each traffic subset. Additionally, it consolidates all deployment tasks in one view, so you can quickly configure target IP addresses for clients and specify host servers.

Prebuilt application templates for widely used Web applications, such as Microsoft Outlook Web Access and Microsoft SharePoint, are available on the AppExpert Templates page of the Citrix Community website at "http://community.citrix.com/display/ns/AppExpert+Templates."

Each prebuilt template provides you with an initial configuration for managing the associated Web application. You can customize prebuilt application templates for your organization. If a prebuilt application template does not suit your requirements, you can create a custom application without using a template.

Regardless of whether you use a prebuilt application template or you create a custom application, you can export the configuration to a template file. You can then share the template with other administrators or import the template to other NetScaler appliances that require a similar AppExpert application configuration.

To get started with an AppExpert application, you must first obtain the appropriate application template and import the template to the NetScaler appliance. After the AppExpert application is set up, you must verify that the application is working correctly. If required, you can customize the configuration to suit your requirements.

Periodically, you can verify and monitor the configuration by viewing the hit counters for various application components, statistics, and the Application Visualizer. You can also configure authentication, authorization, and auditing (AAA) policies for the application.

AppExpert Application Terminology

Following are the terms used in the AppExpert applications feature and the descriptions of the entities for which the terms are used:

Public Endpoint. The IP address and port combination at which the NetScaler appliance receives client requests for the associated web application. A public endpoint can be configured to receive either HTTP or secure HTTP (HTTPS) traffic. All client requests for the web application must be sent to a public endpoint. An AppExpert application can be assigned multiple endpoints. You configure public endpoints after you import a template.

Application Unit. An AppExpert application entity that processes a subset of web application traffic and load balances a set of services that host the associated content. The subset of traffic that an application unit must manage is defined by a rule. Each application unit also defines its own set of traffic optimization and security policies for the requests and responses that it manages. The NetScaler services associated with these policies are Compression, Caching, Rewrite, Responder, and application firewall.

By default, every AppExpert application with at least one application unit includes a default application unit, which cannot be deleted. The default application unit is not associated with a rule for identifying requests and is always placed last in the order of application units. It defines a set of policies for processing any request that does not match the rules that are configured for the other application units, thereby ensuring that all client requests are processed.

Application units and their associated rules, policies, and actions are included in AppExpert application templates.

Service. The combination of the IP address of the server that hosts the web application instance and the port to which the application is mapped on the server, in the format <IP address>:<Port>. A web application that serves a large number of requests is usually hosted on multiple servers. Each server is said to host an instance of the web application, and each such instance of the web application is represented by a service on the NetScaler appliance. Services are deployment-specific, and are therefore not included in templates. You must configure services after you import a template.

Application Unit Rule. Either a classic expression or a default syntax expression that defines the characteristics of a traffic subset for an application unit. The following example rule is a default syntax expression that identifies a traffic subset that consists of four image types:

```
HTTP.REQ.URL.SUFFIX.EQ("bmp") || HTTP.REQ.URL.SUFFIX.EQ("gif") ||
HTTP.REQ.URL.SUFFIX.EQ("png") || HTTP.REQ.URL.SUFFIX.EQ("jpg")
```

For more information about default syntax expressions and classic policy expressions, see "Policies and Expressions."

Traffic Subset. A set of client requests that require a common set of traffic optimization and security policies. A traffic subset is managed by an application unit and is defined by a rule.

How an AppExpert Application Works

When the endpoint receives a client request, the NetScaler appliance evaluates the request against the rule that is configured for the topmost application unit. If the request satisfies this rule, the request is processed by the policies that are configured for the application unit, and then forwarded to a service. The choice of service depends on which services are configured for the application, and on settings such as the load balancing algorithm and persistence method configured for the application unit.

If the request does not satisfy the rule, the request is evaluated against the rule for the next topmost application unit. In this order, the request is evaluated against each application unit rule until the request satisfies a rule. If the request does not satisfy any of the configured rules, it is processed by the default application unit, which is always the last application unit.

You can configure multiple public endpoints for an AppExpert application. In such a configuration, by default, each application unit processes requests received by all the public endpoints and load balances all the services that are configured for the application. However, you can specify that an application unit processes traffic from only a subset of the public endpoints and load balances only a subset of the services that are configured for the AppExpert application.

Getting Started with an AppExpert Application

The process of setting up an AppExpert application begins with downloading the appropriate AppExpert application template from the Citrix Community Web site at "http://community.citrix.com/display/ns/AppExpert+Templates." The template that you need depends on the NetScaler release running on your appliance.

After you download the template, you must import the template to the NetScaler appliance, configure deployment settings, and then verify the configuration to make sure that the AppExpert application is working as expected.

Importing an AppExpert Application Template

You can either import the template file directly from your local computer or upload the template to the appliance and then import it. For more information about uploading a template to the NetScaler appliance, see "Uploading and Downloading Template Files."

During import, along with the template file that you specify in the AppExpert Template Wizard, you can include a deployment file that contains deployment details. If you choose to include a deployment file, you do not have to provide any additional information. All application-configuration information is imported from the template file, and all deployment-specific information for the application is imported from the deployment file. The NetScaler appliance imports all configuration settings from the deployment file through the NITRO API, and the wizard displays the configuration summary screen for your verification. If you do not include a deployment file, the wizard displays screens on which you can specify deployment information. During import, if an error occurs, any changes are automatically rolled back, preserving the configuration that was in place before you attempted to import the AppExpert application. For more information about the format of application templates and deployment files, see "Understanding NetScaler Application Templates and Deployment Files." For more information about how the template and deployment files are imported through the NITRO API, see "NITRO API."

Note: The deployment file must contain information about only one public endpoint. Additionally, the application template file and the deployment file must be valid XML files. You cannot import a template file that is in GZIP format.

During import, you can configure only one public endpoint, but you can specify as many services and service groups as you want the AppExpert application to manage. After you import the template, you can specify additional endpoints, services, and service groups for the configuration. If the public endpoint that you configure during import uses the HTTPS protocol, and you are not providing a deployment file, you must also specify a server certificate for the public endpoint. Additionally, if variables have been configured for the template, a Specify Variable Values page appears in the wizard. On this page, you can choose to specify new values for the variables. Configuring deployment settings (a minimum of one public endpoint and one or more services) during template import is not mandatory; you can choose to skip these steps during import and, instead, configure these settings after you import the template. Note, however, that you can configure additional AppExpert

application features, such as AAA, only after you specify at least one public endpoint.

For more information about configuring endpoints after you import a template, see "Configuring Public Endpoints." For more information about configuring services and service groups after you import a template, see "Configuring Services and Service Groups." For more information about configuring variables for a NetScaler application, see "Creating Variables in Application Templates."

To import an AppExpert application template to the NetScaler appliance

1. Navigate to AppExpert > Applications.
2. In the details pane, click Applications, and then click Import.
3. Follow the instructions in the AppExpert Template Wizard.

Verifying and Testing the Configuration

Verification is an important step in the process of setting up the NetScaler application. Before you proceed with other configuration tasks, you must verify that the state of the entities, such as endpoints and application units, are UP, and then test the entities for correct processing.

Verifying the Configuration

The graphical user interface (GUI) includes icons that indicate the states of the entities in the AppExpert application. These icons are displayed for applications and application units and are based on the health checks that the NetScaler appliance performs periodically on services and entities. The following table lists the icons and describes their meanings.

Table 1. Descriptions of State Indicator Icons

Icon	Entity	Indicates that
	Application	At least one public endpoint is up. The application will accept client requests from the public endpoints that are up.
	Application unit	The application unit is up. The application unit is up when at least one service or service group is up.
	Application	The public endpoint is out of service (disabled). This indicator is displayed when only one public endpoint is configured for the AppExpert application.
	Application	All the endpoints that are configured for the application are out of service. This indicator is displayed only when multiple endpoints are configured for the application.
	Application unit	All the services configured for the application unit are down.

You must ensure that the icons for each application and its application units are green at all times. If the icon that is displayed for an application is not green, verify that you have

configured the public endpoints correctly. If the icon that is displayed for an application unit is not green, verify that the services are configured correctly. However, note that a green indicator does not mean that the state of all associated entities is UP. It only means that the application has sufficient resources (endpoints and services) to serve client requests. To verify that the state of all associated entities is UP, check the health of all the entities on the statistics page for the application. For more information about viewing the application statistics page, see "Viewing Application Statistics."

Testing the Configuration by Using Hit Counters

You can test the configuration by sending test HTTP requests for web application content through the NetScaler appliance, and then verifying that the requests are being processed by the right application units, by viewing the hit counters for the various AppExpert application entities. For example, to verify that the endpoint is receiving requests, you can view the hit counter for the AppExpert application. To verify that the configured application unit rules are being matched as expected, you can view the hit counters for the AppExpert application units.

Note: To view hit counters for policies and actions that are configured for AppExpert applications, you must go to the associated feature node. For example, to view the hit counter for a Rewrite policy that is configured for an AppExpert application, you must go to the Rewrite feature node in the NetScaler configuration utility.

For a test example, consider an AppExpert application that includes an application unit called "WebPages" for processing web page content, and an application unit called "Images" for processing images. In this example, the rule that is configured for the WebPages application unit includes an expression that checks whether an HTML file is being requested. The Images application unit includes an expression that checks whether an image file is being requested.

Consider an HTML file called sitehome.html, located at /var/www/html/myapplicationpages/, on a backend server with an IP address of 192.0.2.10. In addition to HTML content, the HTML file also references images stored on the server. An HTTP request for the HTML file, sent directly to the server, would be as follows:

```
http://192.0.2.10/myapplicationpages/sitehome.html
```

To send a test request for this file through the NetScaler appliance, in the URL, replace the IP address of the server with the IP address of the public endpoint that is configured for the AppExpert application. For example, if the IP address of the public endpoint is 192.0.2.11, your test URL would be as follows:

```
http://192.0.2.11/myapplicationpages/sitehome.html
```

After you send the request, you must view the hit counter for the application to verify that the public endpoint received the request, view the hit counter for the WebPages application unit to verify that the request for the HTML file matched the rule configured for the application unit, and view the hit counter for the Images application unit to verify that the requests for the images matched the rule configured for the application unit.

For the application, the Hits dialog box displays the total number of requests received by each configured public endpoint. For an application unit, the Hits dialog box displays the number of requests that the application unit processed from each of the public endpoints, and the total hit count.

To view the hit counter for an application or application unit

1. Navigate to AppExpert > Applications.
2. In the details pane, click the application or application unit for which you want to view the hit counter.
3. Click Hits.

Customizing the Configuration

After you verify that the AppExpert application is working correctly, you can customize the configuration to suit your requirements.

You can configure public endpoints and services for the AppExpert application and specify only a subset of the endpoints and services for each application unit. When you want the AppExpert application to manage a traffic subset that is not included in the template, you can either add an application unit for the new traffic subset or modify an existing application unit rule. You can also specify the order of evaluation of the traffic subsets that the AppExpert application manages.

Finally, you can modify the policies that the template provided. If the AppExpert application template does not include policies for a particular NetScaler feature, such as Rewrite or application firewall, you can configure your own policies.

The order in which you perform these tasks depends on your requirement. However, before you configure a service for an application, you must configure the service for the parent application.

Configuring Public Endpoints

If you did not specify a public endpoint when importing an AppExpert application, you can specify public endpoints after you create the application. A public endpoint can be configured to receive either HTTP or secure HTTP (HTTPS) traffic.

If endpoints are already configured for the application, you can dissociate endpoints from the AppExpert application and delete any endpoints that you no longer need. Note that when you dissociate a public endpoint from the AppExpert application, the endpoint is automatically unbound from the associated application unit, but it is not deleted from the system.

To configure public endpoints for an AppExpert application

1. Navigate to AppExpert > Applications.
2. In the details pane, right-click the application for which you want to configure public endpoints, and then click Configure Public Endpoints.
3. In the Choose Public Endpoints dialog box for the application, do one of the following:
   - If the endpoints you want are listed in the dialog box, click the corresponding check boxes.
   - If you want to specify all the public endpoints, click Activate All.
   - If you want to dissociate endpoints from the AppExpert application, clear the corresponding check boxes.
   - If you want to create a new public endpoint, click Add. Then, in the Create public endpoint dialog box, configure endpoint settings, and then click OK.

     In the Create public endpoint dialog box, you can specify only the name, IP address, port, and protocol for the endpoint. You can specify additional endpoint settings after you create the public endpoint. To specify additional endpoint settings, after you create the endpoint, in the Choose Public Endpoints dialog box, click the endpoint, and then click Open. Then, in the Configure Public Endpoint dialog box, provide additional settings, and then click OK.

     For more information about the parameters in the Create public endpoint and Configure Public Endpoint dialog boxes, see "Content Switching."
   - If you want to modify a public endpoint, click the endpoint, and then click Open. Then, in the Configure Public Endpoint dialog box, modify settings for the endpoint, and then click OK.

     For more information about the parameters in the Configure Public Endpoint dialog box, see "Content Switching."
4. Click Close.

Configuring Endpoints for an Application Unit

When you configure multiple public endpoints for an AppExpert application, by default, all endpoints are bound to each application unit, and each application unit processes the requests received by all the endpoints. However, you can specify that a given application unit manages the traffic that is received by only a subset of the endpoints that are configured for the AppExpert application.

To configure endpoints for an application unit

1. Navigate to AppExpert > Applications.
2. In the details pane, right-click the application unit for which you want to specify public endpoints, and then click Configure Public Endpoints.
3. In the Choose Public Endpoints dialog box for the application unit, do one of the following:
   - If you are specifying endpoints for the application unit for the first time, clear the check boxes that correspond to the endpoints that you do not want to be bound to the application unit.
   - If you want to specify endpoints that are listed in the dialog box but not currently bound to the application unit, click the corresponding check boxes.
4. Click OK.

Configuring Services and Service Groups

When you configure a service or service group, you either modify an existing service or service group, or add new services to the AppExpert application. You add services or service groups if you did not specify them when you imported the application template. You also add services and service groups when you increase the number of servers that host instances of the application. You can configure a service and service group for an application unit only after you configure the service or service group for the AppExpert application.

To configure a service or service group for the AppExpert application

1. Navigate to AppExpert > Applications.
2. In the details pane, right-click the application for which you want to configure services or service groups, and then click Configure Backend Services.
3. In the Configure Backend Services dialog box, do one of the following:
   - To configure services, click the Services tab.
   - To configure service groups, click the Service Groups tab.
4. On the Service or Service Groups tab, do one of the following:
   - If the services or service groups that you want are listed on the tab, click the corresponding check boxes.
   - If you want to specify all the services or service groups, click Activate All.
   - If you want to create a new service or service group, click Add. Then, in the Create Service dialog box or Create Service Group dialog box, configure settings for the service or service group, respectively, and then click Create.
   - If you want to modify a service, click the service, and then click Open. Then, in the Configure Service dialog box or Create Service Group dialog box, configure settings for the service or service group, respectively, and then click OK.

For information about the settings in the Create Service, Configure Service, and Create Service Group dialog boxes, see "Load Balancing."

Configuring Services, Service Groups, and Load Balancing Parameters for an Application Unit

When you configure services and service groups for an AppExpert application, by default, all the services and service groups are bound to each application unit. However, depending on how you have configured your web application, the application resources that are managed by an application unit might be hosted on only some of the servers that are configured as services for the AppExpert application. Or, a set of servers might host content that is meant for the requests received at one or more specific public endpoints. In such scenarios, if all the services and service groups that are configured for the AppExpert application are associated with the application unit, a request that is forwarded to a server that does not host the requested content might not be served or might be served incorrect content. Therefore, you must ensure that each application unit is configured to manage only those services that can serve the requested content.

When configuring services and service groups for an application unit, you might choose to specify load balancing settings such as the weights that services must be assigned and the desired load balancing, persistence, and spillover methods. For more information about these settings, see Load Balancing.

To configure services or service groups for an application unit

1. Navigate to AppExpert > Applications.
2. In the details pane, right-click the application unit for which you want to configure a service or service group, and then click Configure Backend Services.
3. In the Configure Backend Services dialog box, do one of the following:
   - To configure services, click the Services tab.
   - To configure service groups, click the Service Groups tab.
4. In the Services or Service Groups tab, do one of the following:
   - Clear the check boxes that correspond to the services or service groups that you do not want configured for the application unit. Make sure that the check boxes that correspond to the services or service groups that you want configured for the application unit are selected. Then, in the Weight column, specify the weight that you want to assign to each configured service.
   - To specify all services or service groups, click Activate All.
5. On the Method and Persistence and Advanced tabs, specify the desired parameters.
6. Click OK.

Creating Application Units

You might need to add application units for traffic subsets that are either specific to your web application implementation or not defined in the template. When creating an application unit, you must configure a rule for the application unit.

To create an application unit for the AppExpert application

1. Navigate to AppExpert > Applications.
2. In the details pane, right-click the application for which you want to add an application unit, and then click Add.
3. In the **Create** Application Unit dialog box, specify values for the following parameters:
   - Name*—The name that you want to assign to the application unit.
   - Rule*—The rule that identifies the traffic subset that the application unit will manage.
   - Classic Syntax—To specify that you want to configure a classic expression in the Rule box, click this option button.
   - Default Syntax—To specify that you want to configure a default syntax expression in the Rule box, click this option button.

   *A required parameter
4. Click Create.

Configuring Application Unit Rules

You might want to configure an application unit rule to include or exclude certain types of traffic. When you configure the rule, you can also define the syntax of the expression.

To configure an application unit rule

1. In the navigation pane of the NetScaler configuration utility, expand AppExpert, and then click Applications.
2. In the details pane, right-click the application unit for which you want to modify the rule, and then click Open.
3. In the Configure Application Unit dialog box, do the following:
   a. To specify the format of the new expression, do one of the following:
      - To specify that you want to configure a classic expression in the Rule box, click Classic Syntax.
      - To specify that you want to configure an advanced expression in the Rule box, click Default Syntax.
   b. In the Rule box, configure the expression.
4. Click OK.

Specifying the Order of Evaluation of Application Units

Application unit rules are evaluated in the order in which they are placed in the graphical user interface (GUI). The rule that is configured for the topmost application unit is always configured first, followed by the rule that is configured for the second topmost application unit, and so on. The default application unit is always evaluated last.

When a request matches the rule that is configured for an application unit, the request is processed by the application unit, and no further matching is performed. Therefore, the order of evaluation of application units becomes an important factor if the traffic subsets for two or more application units overlap. If the traffic subsets for two or more application units overlap, you must specify the order in which an incoming request is matched against the application unit rules.

To specify the order of evaluation of application units

1. Navigate to AppExpert > Applications.
2. In the details pane, do the following:
   - To move an application unit up by one step, right-click the application unit, and then click Move Up.
   - To move an application unit down by one step, right-click the application unit, and then click Move Down.

Configuring Policies for Application Units

For an AppExpert application, you can configure policies for Compression, Caching, Rewrite, Responder, and Application Firewall. The templates that you download from the Citrix Community web site provide you with a set of policies that fulfill the most common application management requirements. You might want to fine-tune or customize these policies. If the set of policies provided for a given application unit does not include policies for a particular feature, you can create and bind your own policies for that feature.

If you create an AppExpert application without using a template, you must configure all the policies that the web application needs.

The GUI uses various icons to indicate whether or not policies are configured for a feature. For an application unit, if a policy is configured for a given feature, an icon that represents the feature is displayed. For example, if a compression policy is configured for an application unit, a compression icon is displayed in the Compression column for the application unit. For features for which no policy is configured, an icon depicting a plus sign (+) is displayed.

Note: When configuring policies for application units, you might need to configure policies and expressions that are either in the classic or default syntax. Additionally, when you configure default syntax policies, you might need to specify parameters such as Goto expressions and invoke policy banks. For information about configuring policies and expressions in both formats, see "Policies and Expressions."

Configuring Compression Policies

You can use either classic policies or advanced policies to configure compression, but you cannot bind compression policies of both types to the same application unit.

To configure a compression policy for an application unit

1. Navigate to AppExpert > Applications.
2. In the details pane, in the row for the application unit you want to configure, click the icon provided in the Compression column.
3. In the Configure Compression Policies dialog box, do one or more of the following, depending on the configuration tasks you want to perform:
   - Click Switch to Default Syntax if you want to configure a default syntax compression policy. If you want to bind or configure classic compression policies, and if you are in the default syntax view, you can click Switch to Classic Syntax to return to the classic policy view and begin modifying bound classic policies or create and bind new classic compression policies.

     Important: This setting also determines what policies are displayed when you want to insert a policy. For example, if you are in the default syntax view, when you click Insert Policy, the list that appears in the Policy Name column will include only default syntax policies. You cannot bind policies of both types to an application unit.
   - If you want to configure classic policies, click either Request or Response, depending on whether you want the policy to be evaluated at request-time or at response-time.

     You can configure both request-time and response-time classic compression policies for an application unit. After evaluating all of the request-time policies, if no match is found, the appliance evaluates response-time policies.
   - To modify a compression policy that is already bound to the application unit, click the name of the policy, and then click Modify Policy. Then, in the Configure Compression Policy dialog box, modify the policy, and then click OK.

     For information about modifying a compression policy, see "Compression."
   - To unbind a policy, click the name of the policy, and then click Unbind Policy.
   - To modify the priority assigned to a policy, double-click the priority value, and then enter a new value.
   - To regenerate assigned priorities, click Regenerate Priorities.
   - To insert a new policy, click Insert Policy and, in the list that is displayed in the Policy Name column, click New Policy. Then, in the Create Compression Policy dialog box, configure the policy, and then click Create.

     For information about modifying a compression policy, see "Compression."
   - If you are configuring a default syntax expression, do the following:
     - In the Goto Expression column, select a Goto expression.
     - In the Invoke column, specify the policy bank that you want to invoke if the current policy evaluates to TRUE.
4. Click Apply Changes, and then click Close.

Configuring Caching Policies

You can use only default syntax policies and expressions to configure Caching policies.

To configure Caching policies for an application unit

1. Navigate to AppExpert > Applications.
2. In the details pane, in the row for the application unit you want to configure, click the icon provided in the Caching column.
3. In the Configure Cache Policies dialog box, do one or more of the following, depending on the configuration tasks you want to perform:
   - Click either Request or Response, depending on whether you want the policy to be evaluated at request-time or at response-time.

     You can configure both request-time and response-time Caching policies for an application unit. After evaluating all of the request-time policies, if no match is found, the appliance evaluates response-time policies.
   - To modify a Caching policy that is already bound to the application unit, click the name of the policy, and then click Modify Policy. Then, in the Configure Cache Policy dialog box, modify the policy, and then click OK.

     For information about modifying a Caching policy, see "Integrated Caching."
   - To unbind a policy, click the name of the policy, and then click Unbind Policy.
   - To modify the priority assigned to a policy, double-click the priority value, and then enter a new value.
   - To regenerate assigned priorities, click Regenerate Priorities.
   - To insert a new policy, click Insert Policy and, in the list that is displayed in the Policy Name column, click New Policy. Then, in the Create Cache Policy dialog box, configure the policy, and then click Create.

     For information about modifying a Caching policy, see "Integrated Caching."
   - In the Goto Expression column, select a Goto expression.
   - In the Invoke column, specify the policy bank that you want to invoke if the current policy evaluates to TRUE.
4. Click Apply Changes, and then click Close.

Configuring Rewrite Policies

You can use only default syntax policies and expressions to configure Rewrite policies.

To configure Rewrite policies for an application unit

1. Navigate to AppExpert > Applications.
2. In the details pane, in the row for the application unit you want to configure, click the icon provided in the Rewrite column.
3. In the Configure Rewrite Policies dialog box, do one or more of the following, depending on the configuration tasks you want to perform:
   - Click either Request or Response, depending on whether you want the policy to be evaluated at request-time or at response-time.

     You can configure both request-time and response-time Rewrite policies for an application unit. After evaluating all of the request-time policies, if no match is found, the appliance evaluates response-time policies.
   - To modify a Rewrite policy that is already bound to the application unit, click the name of the policy, and then click Modify Policy. Then, in the Configure Rewrite Policy dialog box, modify the policy, and then click OK.

     For information about modifying a Rewrite policy, see "Rewrite."
   - To unbind a policy, click the name of the policy, and then click Unbind Policy.
   - To modify the priority assigned to a policy, double-click the priority value, and then enter a new value.
   - To regenerate assigned priorities, click Regenerate Priorities.
   - To insert a new policy, click Insert Policy and, in the list that is displayed in the Policy Name column, click New Policy. Then, in the Create Rewrite Policy dialog box, configure the policy, and then click Create.

     For information about modifying a Rewrite policy, see "Rewrite."
   - In the Goto Expression column, select a Goto expression.
   - In the Invoke column, specify the policy bank that you want to invoke if the current policy evaluates to TRUE.
4. Click Apply Changes, and then click Close.

Configuring Responder Policies

You can use only default syntax policies and expressions to configure Responder policies.

To configure Responder policies for an application unit

1. Navigate to AppExpert > Applications.
2. In the details pane, in the row for the application unit you want to configure, click the icon provided in the Responder column.
3. In the Configure Responder Policies dialog box, do one or more of the following, depending on the configuration tasks you want to perform:
   - To modify a Filter policy that is already bound to the application unit, click the name of the policy, and then click Modify Policy. Then, in the Configure Responder Policy dialog box, modify the policy, and then click OK.

     For information about modifying a Responder policy, see "Responder."
   - To unbind a policy, click the name of the policy, and then click Unbind Policy.
   - To modify the priority assigned to a policy, double-click the priority value, and then enter a new value.
   - To regenerate assigned priorities, click Regenerate Priorities.
   - To insert a new policy, click Insert Policy and, in the list that is displayed in the Policy Name column, click New Policy. Then, in the Create Responder Policy dialog box, configure the policy, and then click Create.

     For information about modifying a Responder policy, see "Responder."
   - In the Goto Expression column, select a Goto expression.
   - In the Invoke column, specify the policy bank that you want to invoke if the current policy evaluates to TRUE.
4. Click Apply Changes, and then click Close.

Configuring Application Firewall Policies

You can configure both classic and default syntax policies and expressions for Application Firewall. However, if a policy of one type is already bound globally or to a virtual server that is configured on the appliance, you cannot bind a policy of the other type to an application unit. For example, if a default syntax policy is already bound either globally or to a virtual server, you cannot bind a classic policy to an application unit.

To configure Application Firewall policies for an application unit

1. Navigate to AppExpert > Applications.
2. In the details pane, in the row for the application unit you want to configure, click the icon provided in the Application Firewall column.
3. In the Configure Application Firewall Policies dialog box, do one or more of the following, depending on the configuration tasks you want to perform:
   - Click either Classic Expression or Advanced Expression depending on the type of expression you want to configure for the Application Firewall policy.

     Important: This setting also determines what policies are displayed when you want to insert a policy. For example, if you select Advanced Expression, when you click Insert Policy, the list that appears in the Policy Name column will include only default syntax policies. You cannot bind policies of both types to an application unit. This option is not available if a policy of either type is already bound either globally or to a virtual server.
   - To modify an application firewall policy that is already bound to the application unit, click the name of the policy, and then click Modify Policy. Then, in the Configure Application Firewall Policy dialog box, modify the policy, and then click OK.

     For information about modifying a application firewall policy, see "Policies."
   - To unbind a policy, click the name of the policy, and then click Unbind Policy.
   - To modify the priority assigned to a policy, double-click the priority value, and then enter a new value.
   - To regenerate assigned priorities, click Regenerate Priorities.
   - To insert a new policy, click Insert Policy and, in the list that is displayed in the Policy Name column, click New Policy. Then, in the Create Application Firewall Policy dialog box, configure the policy, and then click Create.

     For information about modifying a application firewall policy, see "Policies."
4. Click Apply Changes, and then click Close.

Viewing AppExpert Applications and Configuring Entities by Using the Application Visualizer

The Application Visualizer is a graphical representation of an AppExpert application. The Visualizer displays the public endpoints, application units, backend services, and policies that are configured for the application. You can use the Visualizer to obtain a visual overview of an AppExpert application's configuration and configure some of the displayed entities. By default, the Visualizer displays application units, services, and monitors for the selected application.

You can also use the Application Visualizer to monitor some AppExpert application parameters. For more information about monitoring application parameters by using the Application Visualizer, see "Monitoring an Application by Using the Application Visualizer."

To view an AppExpert application by using the Application Visualizer

1. Navigate to AppExpert > Applications.

2. In the details pane, click the name of the application that you want to view, and then click Visualizer.

3. Do one or more of the following:

   - To optimize the display area, choose Best Fit, Zoom In, or Zoom out. If an item that you want to see disappears from view after zooming in, you can click and drag the viewable area.
   - To save the graph as an image file, click Save Image.
   - To find a particular entity, in the Search in field, type an entity name. In the view area, the entity names that begin with the search string are highlighted. To restrict the search, click the drop-down menu and select the specific entity that you want to search for.
   - To view the policies that an application uses, click one or more icons to display feature-specific policies. The policy types are Compression, Filter, Rewrite, Responder, Cache, application firewall, Authorization, Auditing, HTML Injection, SureConnect, Priority Queuing, and Traffic.
   - To view the rule that is configured for an application unit, click the curve that connects the public endpoint to the application unit. The rule is displayed on the Related Tasks tab.
   - To view the binding information for an application unit, policy, or monitor, click the displayed icon, click the Related Tasks tab, and then click Show Bindings
   - To view member services, click the icon for the service, click the Related Tasks tab, and then click Show Member Services.
   - To view detailed statistics for a public endpoint or application unit, click the icon that is displayed, click the Related Tasks tab, and then click Statistics.
   - To view the Load Balancing Visualizer for an application unit, click the application unit, click Related Tasks, and then click Visualizer.

   - To view the number of requests received per second at a given point in time by the load balancing virtual server and the number of hits per second at a given point in time for rewrite, responder, and cache policies, click Show Stats. The statistical information is displayed on the respective nodes in the Visualizer. This information is not updated in real time and has to be refreshed manually. To refresh this information, click Refresh Stats.

To configure and view entities in an AppExpert application by using the Application Visualizer

1. Navigate to AppExpert > Applications.

2. In the details pane, click the name of the application that you want to configure or view, and then click Visualizer.

3. Do one or more of the following:

   - To configure an entity that is displayed in the viewing area, click the icon for the entity, click the Related Tasks tab, and then click Modify public endpoint.

     In the Application Visualizer, you can modify only public endpoints and services.
   - To bind additional monitors to a service, click the Available Resources tab, select Monitors from the drop-down list, and then click and drag a monitor to a service.
   - To unbind a service from an application unit, click the curve that connects the application unit and the service, click Related Tasks, and then click Unbind.
   - To unbind a monitor from a service, click the curve that connects the service and the monitor, click Related Tasks, and then click Unbind.
   - To modify a monitor, click the monitor, click Related Tasks, and then click Open.
   - To modify the binding parameters for a monitor, click the curve that connects the monitor to the associated service, click Related Tasks, and then click Modify Parameters.
   - To apply a common service configuration across multiple service containers that are displayed when the services bound to a vserver do not have the same configuration, click the service container whose configuration you want to apply to all the containers, and then, in Related Tasks, click Apply Configuration.
   - To view a comparative list of the parameters whose values differ across service containers, click the icon for a container, click the Related Tasks tab, and then click Service Attributes Diff. The comparative list helps you determine which service container has the service configuration that you want to apply to all the containers. After you determine which service container has the configuration you want, right-click the container, and then click Apply this Configuration.
   - To copy the configuration of an entity (other than the configuration of the AppExpert application) to the local computer’s clipboard, click the entity, click the Related Tasks tab, and then click Copy Properties. You can then paste the configuration information in a word processing document or spreadsheet.

Monitoring a NetScaler Application

After you customize the AppExpert application, you can view application statistics to make sure that the application and all its entities are working correctly. You can also use the Application Visualizer to monitor statistics associated with certain entities such as policies and virtual servers.

You can also view the hit counters for various entities at regular intervals to make sure that counters are being updated.

Viewing Application Statistics

In the Applications node, you can select an application and view the Statistics page for the application. On the Statistics page, you can monitor the health and states of public endpoints and application units, and view the following statistical information:

- Requests and responses per second for each of the public endpoints and application units.
- Bytes per second, at each endpoint, for incoming and outgoing traffic.
- Application unit hit counters and the number of client and server connections for each application unit.
- Statistics for the services that are bound to the application units.

On the Statistics page, you can also view CPU usage, memory usage, and system logs.

To view statistics for an application

1. Navigate to AppExpert > Applications.
2. In the details pane, click the application for which you want to view statistics, and then click Statistics.

Monitoring an Application by Using the Application Visualizer

You can use the Application Visualizer to monitor the number of requests received per second at a given point in time by the vservers and the number of hits per second at a given point in time for Rewrite, Responder, and Cache policies.

To view statistical information for vservers, Rewrite policies, Responder policies, and Cache policies in the Visualizer

1. Navigate to AppExpert > Applications.
2. In the details pane, select the application for which you want to view statistical information, and then click Visualizer.
3. In the Application Visualizer window, do the following:
   - To view the statistics, click Show Stats.

     The statistical information is displayed on the respective nodes in the Visualizer. This information is not updated in real time and has to be refreshed manually.
   - To refresh the statistical information, click Refresh Stats.

Viewing Hits

The hit counters that are provided for various AppExpert application entities enable you to monitor the functioning of public endpoints and application units. For an application, the Hits dialog box displays the total number of requests received by each configured public endpoint. For an application unit, the Hits dialog box displays the number of requests that the application unit processed from each of the public endpoints and the total hit count. For instructions on viewing hit counters, see "Verifying and Testing the Configuration."

Deleting an Application

If you no longer need an application and its application units, you can delete it. When you delete an AppExpert application, backend services are not deleted, and any public endpoints that the application used become available for use by other applications.

When deleting an application, you are also prompted to specify whether you want to delete any bound policies and actions that are not used elsewhere.

To delete an application

1. Navigate to AppExpert > Applications.
2. In the details pane, click the name of the application that you want to delete, and then click Remove.

Configuring Authentication, Authorization, and Auditing

You can configure Authentication, Authorization, and Auditing (AAA) for the applications that you configure on the appliance. An authentication policy that is configured for an application defines the type of authentication to apply when a user or group attempts to access the application. If external authentication is used, the policy also specifies the external authentication server. Authorization policies configured for an application specify whether a particular user or group can access the application. Auditing policies define the audit log type, the level at which logging is performed, and other audit server settings. Authentication and auditing policies use the classic policy format.

Authentication policies, authorization policies, and auditing policies can be configured in any order. However, before you configure AAA for an application, you must configure a public endpoint for the application.

Configuring Authentication

Configuring authentication for an application involves specifying an authentication FQDN, an authentication virtual server, a server certificate, and authentication and session policies. Authentication policies are automatically bound to the authentication virtual server specified for the application.

To configure authentication for an AppExpert application

1. Navigate to AppExpert > Applications.
2. In the details pane, click the name of the application for which you want to configure authentication, and then click Authentication.
3. In the Authentication Wizard, on the Introduction page, click Next.
4. Follow the instructions in the Authentication Wizard.

Configuring Authorization

You can configure authorization for users and groups to enable then to access an AppExpert application. If the AAA user or group for which you want to configure permissions has not already been created, you can create it from AppExpert and then configure permissions for application access.

To configure permissions for a AAA user or group to access an AppExpert application

1. Navigate to AppExpert > Applications.
2. In the details pane, click the AppExpert application for which you want to configure user or group access, and then click Authorization.
3. Do one of the following:
   - If the AAA user or group for which you want to configure permissions is already in the Groups/Users tree, drag the user or group from the Groups/Users tree to the Users or Groups node in the application tree. Then, right-click the user or group and click Allow.
   - If the AAA user or group for which you want to configure permissions is not configured on the appliance, in the application tree, right-click Users or Groups, and then click Add. In the Create AAA Group or Create AAA User dialog box, fill in the values, click Create, and then click Close.

     The user or group is created with the permission set to Allow. To change the permission setting, right-click the group or user, and then click the permission setting.
4. Click Close.

Configuring Auditing

When you configure auditing policies for an application, you must specify the server to which the log messages must be directed, the format of the messages logged, and the log level. Optionally, you can configure other settings, such as the log facility and date format. Auditing policies are automatically bound to all the AppExpert application’s public endpoints.

To configure auditing policies for an application

1. Navigate to AppExpert > Applications.
2. In the details pane, click the application for which you want to configure auditing policies, and then click Auditing.
3. In the Configure Auditing Policies dialog box, click Insert Policy.
   - To specify an existing auditing policy, under Policy Name, click the name of the policy, and then do the following:
     - To modify the priority that is assigned to the policy by default, under Priority, double-click the priority, and then type a new priority value.
     - To modify the settings of the audit server, under Server, double-click the name of the server, and then, in the Configure Auditing Server dialog box, modify the settings as appropriate. You can modify all the settings in this dialog box except the name of the audit server and the audit type. For more information about the settings in the Configure Auditing Server dialog box, see "Auditing Policies."
   - To create a new auditing policy, under Policy Name, click New Policy, and then, in the Create Auditing Policy dialog box, do the following:
     - In the Name box, type a name for the policy.
     - The Name box already contains the string that is required at the beginning of the server name. You cannot modify the string.
     - From the Auditing Type list, select the auditing type (either SYSLOG or NSLOG).
     - If the audit server you want to specify is already listed in the Server list, select the server from the list, and then, if you want to modify the server settings, click Modify. In the Configure Auditing Server dialog box, modify the settings as appropriate, and then click OK. For more information about the settings in the Configure Auditing Server dialog box, see "Auditing Policies."
     - If you want to configure a new audit server, click New, and then, in the Create Auditing Server dialog box, type a name for the server, specify the server IP address, port number, and other settings as appropriate. When finished, click OK.
     - Click Create.
   - To change the priorities for the new auditing policies you created, under Priority, for each policy for which you want to change the priority, double-click the priority value and type new priority value.
   - To regenerate priorities, click Regenerate Priorities.
   - To unbind a policy, click the policy, and then click Unbind Policy.
   - To modify a policy, click the policy, and then click Modify Policy.
4. Click Apply Changes, and then click Close.

Disabling AAA for an Application

After you configure AAA for an application, you can disable the AAA configuration for that application. When you disable AAA for an application, the configuration is not lost. You can enable AAA for the application when you want to reapply the configuration.

To enable or disable AAA for an application

1. Navigate to AppExpert > Applications.
2. In the details pane, click the application for which you want to enable or disable AAA, and then do one of the following:
   - To disable AAA for the application, click Turn Off AAA.
   - To enable AAA for the application, click Turn On AAA.

Setting Up a Custom NetScaler Application

If an AppExpert application template is not available for the Web application that you want to manage through the NetScaler appliance, or if available AppExpert application templates do not suit your requirements, you can create an AppExpert application without a template.

To create an AppExpert application without a template, you must first create an application and application units. Then, you configure public endpoints, services, and service groups. Finally, you configure the policies that determine how application traffic is evaluated and processed.

After you create the application and application units and configure policies, you must verify the configuration and test it to make sure that it is working correctly, just as you would when you configure an application by using a prebuilt AppExpert application template. Then, you must monitor the application to make sure that the application and its entities are working correctly.

Creating an Application

When you create an AppExpert application, the appliance creates a container to which you can add application units. The *default* application unit is not created until you create the first application unit.

To create an AppExpert application

1. Navigate to AppExpert > Applications.
2. In the details pane, right-click Applications, and then click Add.
3. In the Create Application dialog box, in Name, enter a name for the application, and then click OK.

Creating Application Units

For each subset of traffic associated with your web application, you must create an application unit.

To create an application unit for the AppExpert application

1. Navigate to AppExpert > Applications.
2. In the details pane, right-click the application for which you want to add an application unit, and then click Add.
3. In the **Create** Application Unit dialog box, specify values for the following parameters:
   - Name*—The name that you want to assign to the application unit.
   - Rule*—The rule that identifies the traffic subset that the application unit will manage.
   - Classic Syntax—To specify that you want to configure a classic expression in the Rule box, click this option button.
   - Default Syntax—To specify that you want to configure a default syntax expression in the Rule box, click this option button.

   *A required parameter
4. Click Create.

Configuring Public Endpoints for an AppExpert Application

After you have created all the application units that you require, you must configure one or more public endpoints to enable clients to access the web application through the NetScaler appliance.

To configure public endpoints for an AppExpert application

1. Navigate to AppExpert > Applications.
2. In the details pane, right-click the application for which you want to configure public endpoints, and then click Configure Public Endpoints.
3. In the Choose Public Endpoints dialog box for the application, do one of the following:
   - If the endpoints you want are listed in the dialog box, click the corresponding check boxes.
   - If you want to specify all the public endpoints, click Activate All.
   - If you want to dissociate endpoints from the AppExpert application, clear the corresponding check boxes.
   - If you want to create a new public endpoint, click Add. Then, in the Create public endpoint dialog box, configure endpoint settings, and then click OK.

     In the Create public endpoint dialog box, you can specify only the name, IP address, port, and protocol for the endpoint. You can specify additional endpoint settings after you create the public endpoint. To specify additional endpoint settings, after you create the endpoint, in the Choose Public Endpoints dialog box, click the endpoint, and then click Open. Then, in the Configure Public Endpoint dialog box, provide additional settings, and then click OK.

     For more information about the parameters in the Create public endpoint and Configure Public Endpoint dialog boxes, see "Content Switching."
   - If you want to modify a public endpoint, click the endpoint, and then click Open. Then, in the Configure Public Endpoint dialog box, modify settings for the endpoint, and then click OK.

     For more information about the parameters in the Configure Public Endpoint dialog box, see "Content Switching."
4. Click Close.

Configuring Public Endpoints for an Application Unit

For an application unit, you specify public endpoints in the same way as you would specify public endpoints for an application that is created from an AppExpert application template. For more information about specifying a subset of the endpoints for an application unit, see "Configuring Endpoints for an Application Unit."

To configure endpoints for an application unit

1. Navigate to AppExpert > Applications.
2. In the details pane, right-click the application unit for which you want to specify public endpoints, and then click Configure Public Endpoints.
3. In the Choose Public Endpoints dialog box for the application unit, do one of the following:
   - If you are specifying endpoints for the application unit for the first time, clear the check boxes that correspond to the endpoints that you do not want to be bound to the application unit.
   - If you want to specify endpoints that are listed in the dialog box but not currently bound to the application unit, click the corresponding check boxes.
4. Click OK.

Configuring Services and Service Groups for an AppExpert Application

Services and service groups are available for application units only after you configure the services and service groups for the AppExpert application. Therefore, you must configure services and service groups for the AppExpert application before you configure the services for the application units. All the services and service groups that you configure for an AppExpert application must use the same protocol (either HTTP or HTTPS). The procedure for configuring services and service groups for an AppExpert application that is not created from a template is the same as that for an application created from a template.

To configure a service or service group for the AppExpert application

1. Navigate to AppExpert > Applications.
2. In the details pane, right-click the application for which you want to configure services or service groups, and then click Configure Backend Services.
3. In the Configure Backend Services dialog box, do one of the following:
   - To configure services, click the Services tab.
   - To configure service groups, click the Service Groups tab.
4. On the Service or Service Groups tab, do one of the following:
   - If the services or service groups that you want are listed on the tab, click the corresponding check boxes.
   - If you want to specify all the services or service groups, click Activate All.
   - If you want to create a new service or service group, click Add. Then, in the Create Service dialog box or Create Service Group dialog box, configure settings for the service or service group, respectively, and then click Create.
   - If you want to modify a service, click the service, and then click Open. Then, in the Configure Service dialog box or Create Service Group dialog box, configure settings for the service or service group, respectively, and then click OK.

For information about the settings in the Create Service, Configure Service, and Create Service Group dialog boxes, see "Load Balancing."

Configuring Services and Service Groups for an Application Unit

After you configure services and service groups, you must configure services and service groups for each application unit. However, this step is not necessary if each backend service hosts all the content associated with the web application. You configure services and service groups for an application unit if the content associated with the application unit is hosted on only a subset of the backend servers.

To configure services or service groups for an application unit

1. Navigate to AppExpert > Applications.
2. In the details pane, right-click the application unit for which you want to configure a service or service group, and then click Configure Backend Services.
3. In the Configure Backend Services dialog box, do one of the following:
   - To configure services, click the Services tab.
   - To configure service groups, click the Service Groups tab.
4. In the Services or Service Groups tab, do one of the following:
   - Clear the check boxes that correspond to the services or service groups that you do not want configured for the application unit. Make sure that the check boxes that correspond to the services or service groups that you want configured for the application unit are selected. Then, in the Weight column, specify the weight that you want to assign to each configured service.
   - To specify all services or service groups, click Activate All.
5. On the Method and Persistence and Advanced tabs, specify the desired parameters.
6. Click OK.

Configuring Policies

The procedures for configuring policies for an AppExpert application that is created without using a template are the same as those for an AppExpert application that was created from a template. For more information, see "Configuring Policies for Application Units."

Creating and Managing Template Files

After you set up an AppExpert application and customize it to suit your requirements, you can create a template from the application and then share the template with other administrators. Or, you can create a template and then import the template to other NetScaler appliances that require a similar AppExpert application configuration. This simplifies and expedites the process of setting up similar applications on other appliances. You can also export a content switching configuration to a template file. When creating a template file, you can configure variables in the policy expressions and actions that are configured for an application.

AppExpert application template files can be exported either to the template directory on the NetScaler appliance or to a folder on your local computer. You can then upload and download the templates to and from the NetScaler appliance and rename the templates that are stored in the AppExpert application templates directory on your appliance.

Exporting an AppExpert Application to a Template File

When you export an AppExpert application, all application-configuration information is exported to a template file and all deployment-specific information is exported to a deployment file. The string `_deployment` is automatically appended to the name of the template file to create the name of the deployment file. Both files are in XML format. If you choose to export the application template file to the NetScaler appliance, the template file is stored in the `/nsconfig/nstemplates/applications` directory on the NetScaler appliance and the deployment file is stored in the `/nsconfig/nstemplates/applications/deployment_files/` directory. For more information about the format of application templates and deployment files, see "Understanding NetScaler Application Templates and Deployment Files". If you have configured Access Gateway application, when you export the AppExpert configuration, you can choose to include the Access Gateway policies in the template.

To export an AppExpert application to a template file

1. Navigate to AppExpert > Applications.
2. In the details pane, click the name of the application that you want to export as a template file, and then click Export.
3. In the Export...as Template dialog box, do the following:
   a. In the Name box, modify the name of the template, if necessary.
   b. If you want to configure variables for the template, click Configure Variables, and then, in the Configure Variables dialog box, configure the variables that you want.

      For more information about configuring variables in application templates, see "Creating Variables in Application Templates".
   c. If you want to export the template file to the application templates directory on the appliance, make sure that Browse (Appliance) is displayed.
   d. If you want to export the template file to your computer, click the Browse (Appliance) drop-down menu, click Local, browse to the location to which you want to save the file, and then click Save.
   e. Provide the following information:
      - **Introduction Description**—Any text that introduces the AppExpert application template during import. This text is displayed on the Specify Application Name page of the AppExpert Template Wizard when the template is imported.
      - **Summary Description**—Any summary that you might want to display on the Summary page of the AppExpert Template Wizard when the template is imported.
      - **Author**—The name of the author of the template.
      - **Major**—The major version number of the template.
      - **Minor**—The minor version number of the template. This number is appended to the major version number and displayed on the Summary page of the AppExpert Template Wizard, during import, in the format Major.Minor.
   f. Click OK.

      If Access Gateway policies have been configured for the application, you will be prompted to include the Access Gateway configuration in the application template. If you want to include the Access Gateway configuration in the template, at the prompt, click Yes.

Exporting a Content Switching Virtual Server Configuration to a Template File

You can also export a content switching configuration as an application template. You can export a content switching virtual server configuration to an application template either from the Content Switching Virtual Servers pane or from the Content Switching Visualizer. Configuration information, which includes the content switching virtual server, all associated load balancing virtual servers, services, service groups, and policies, is exported to a template file and all deployment-specific information is exported to a deployment file. The string "_deployment" is automatically appended to the name of the template file to create the name of the deployment file. Both files are in XML format. If you choose to export the application template file to the NetScaler appliance, the template file is stored in the /nsconfig/nstemplates/applications directory on the NetScaler appliance and the deployment file is stored in the /nsconfig/nstemplates/applications/deployment_files/ directory. For more information about the format of application templates and deployment files, see "Understanding NetScaler Application Templates and Deployment Files." The configuration information that is exported includes the content switching virtual server, all associated load balancing virtual servers, services, service groups, and policies.

However, if the content switching virtual server is already configured as the public endpoint for an AppExpert application, you cannot export the configuration to a template file . In this scenario, you must export the associated AppExpert application to a template. For more information about exporting an AppExpert application to a template file, see "Exporting an AppExpert Application to a Template File."

To export a content switching configuration to an application template file from the Content Switching Visualizer

1. Navigate to Content Switching > Virtual Servers.
2. In the details pane, click the name of the content switching virtual server whose configuration you want to export as a template file, and then click Visualizer.
3. In the Content Switching Visualizer, click the icon for the content switching vserver, click Related Tasks, and then click Create Template.
4. In the Export...as Template dialog box, enter a name for the template file, and then do one of the following:
   - To export the template file to the appliance, make sure that Browse (Appliance) is displayed.
   - To export the template file to your computer, click the Browse (Appliance) drop-down menu, click Local, browse to the location to which you want to save the file, and then click Save.
5. Provide the following information:
   - **Introduction Description**—Any text that introduces the AppExpert application template during import. This text is displayed on the Specify Application Name page of the AppExpert Template Wizard when the template is imported.
   - **Summary Description**—Any summary that you might want to display on the Summary page of the AppExpert Template Wizard when the template is imported.
   - **Author**—The name of the author of the template.
   - **Major**—The major version number of the template.
   - **Minor**—The minor version number of the template. This number is appended to the major version number and displayed on the Summary page of the AppExpert Template Wizard, during import, in the format `Major.Minor`.
6. Click OK.

To export a content switching configuration to an application template file from the Content Switching Virtual Servers pane

1. Navigate to Content Switching > Virtual Servers.
2. In the details pane, click the name of the content switching virtual server whose configuration you want to export as a template file, and then click Create AppExpert Template.
3. Perform steps 4 through 6 described in "To export a content switching configuration to an application template file from the Content Switching Visualizer".

Creating Variables in Application Templates

Application templates support the declaration of variables in the policy expressions and actions that are configured for an application. The ability to declare variables in policy expressions and actions enables you to replace preconfigured values in expressions (for example, configurable parameters such as the host name of a server or the target for a Rewrite action) with values that suit the environment into which you are importing the template. If variables have been configured for an AppExpert application template, the AppExpert Template Wizard, which appears when you import an AppExpert application template, includes a Specify Variable Values page on which you can specify appropriate values for the variables that are configured for the template.

As an example, consider the following policy expression that is configured to evaluate the value of the Host header in an HTTP request:

```
HTTP.REQ.HEADER("Host").CONTAINS("server1")
```

If you want the server name to be configurable at import time, you can specify the string "server1" as a variable. When importing the template, you can specify a new value for the variable on the Variables tab.

After you create a variable, you can do the following:

- Assign additional strings to an existing variable. After you create a variable for a string, you can select and assign other parts of the same or different expression to the variable. The strings you assign to a variable need not be the same. At import time, all the strings that are assigned to the variable are replaced with the value that you provide.
- View the string or strings that are assigned to the variable.
- View a list of all the entities and parameters that use the variable.

In the export application template wizard, you can define variables in certain fields (fields with an adjacent  button) for the following entities:

- Cache policies
- Rewrite policies
- Rewrite actions
- Responder policies
- Responder actions

To configure a variable in a policy expression or action

1. Navigate to AppExpert > Applications.
2. In the details pane, right-click the application that you want to export to a template file, and then click Export.
3. In the Export...as Template dialog box, modify the default template file name if required, specify the location where you want to save the template, and then click Configure Variables.
4. In the Configure Variables dialog box, click the tab that lists the policy expression or action for which you want to configure a variable, select the expression, and then click Configure Variables.
5. In the Variables dialog box, click the  button next to the expression or value in which you want to create a variable.
6. In the Variables dialog box, do the following:
   - To create a variable, in the text box that displays the configured expression or value, select the string that you want to be configurable at import time, and then click Add. In the Add Variable dialog box, specify a name and a description for the variable, and then click Create.
   - The name of the variable, its value, and the description you provided appear in the Available Variables listing in the dialog box. The name you provide will be the name of the associated field in the template import wizard, and the description will appear as alt text when the user positions the mouse pointer over the field.
   - To modify a variable, in the Available Variables list, click the variable, and then click Open. In the Add Variable dialog box, modify the value and the description, and then click OK.
   - To view all the strings that are assigned to a given variable, in the Available Variables listing, click the name of the variable. The strings that are assigned to the variable are highlighted.
   - To view a list of all the entities and parameters in which the variable is used, in the Available Variables listing, click the variable whose references you want to view, and then click Show References.
   - To assign a string to an existing variable, in the text box that displays the expression you configured, select the string you want to assign to an existing variable, right-click the selection, click Use Existing Selection, and then click the name of the variable to which you want to assign the string.

     If a variable has multiple strings assigned to it, when you specify a new value for the variable during import, all strings assigned to the variable are replaced with the new value.
7. Click Close.

Uploading and Downloading Template Files

Template files can be uploaded from your local computer to the NetScaler appliance or downloaded from the appliance to your local computer. On the appliance, AppExpert application templates are always stored in the AppExpert application templates directory, which is `/nsconfig/nstemplates/applications/`.

To upload an AppExpert application template from your local computer to the NetScaler appliance

1. Navigate to AppExpert > Templates.
2. In the details pane, click Manage Templates.
3. In the Manage Application Templates dialog box, click Application Templates, and then click Upload.
4. In the Upload Application Template dialog box, browse to the directory in which the template file is stored, click the template file, and then click Select.

   The template file is uploaded to the AppExpert application template directory on the appliance.

To download an AppExpert application template from the NetScaler appliance to your local computer

1. Navigate to AppExpert > Templates.
2. In the details pane, click Manage Templates.
3. In the Manage Application Templates dialog box, click the AppExpert application template that you want to download, and click Download.
4. In the Download Application Template dialog box, browse to the location to which you want to save the file, and then click Save.

Renaming an Application Template

You can rename an application template that is stored in the AppExpert application templates folder on the appliance.

To rename an AppExpert applications template

1. Navigate to AppExpert > Templates.
2. In the details pane, click Manage Templates.
3. In the Manage Application Templates dialog box, click the AppExpert application template that you want to rename, and then click Rename.
4. Enter a new name for the template, and then click Close.

Deleting an AppExpert Application Template

You can delete an application template that you no longer need.

To delete an AppExpert application template

1. Navigate to AppExpert > Templates.
2. In the details pane, click the template that you want to delete, and then click Remove.

Understanding NetScaler Application Templates and Deployment Files

When you export a NetScaler application, the following two files are automatically created:

- **NetScaler application template file.** Contains application-configuration information such as application units, rules, and configured policies.
- **Deployment file.** Contains deployment-specific information such as public endpoints, services, associated IP addresses, and configured variables.

In the application template and deployment file, each unit of application-configuration information is encapsulated in a specific XML element that is meant for that unit type. For example, each public endpoint and associated endpoint details are encapsulated within the `<appendpoint>` and `</appendpoint>` tags, and all the endpoint elements are encapsulated within the `<appendpoint_list>` and `</appendpoint_list>` tags.

Note: After you export a NetScaler application, you can add elements, remove elements, and modify existing elements before importing the application to a NetScaler appliance.

Example of a NetScaler Application Template

Following is an example of a template file that was created from a NetScaler application called "SharePoint_Team_Site":

```
<?xml version="1.0" encoding="UTF-8" ?>
<template>
<template_info>
  <application_name>SharePoint_Team_Site</application_name>
  <templateversion_major>1</templateversion_major>
  <templateversion_minor>1</templateversion_minor>
  <author>Ed</author>
  <introduction>An application for managing a SharePoint team site with images, reports, and, XML content.
  <summary>This template includes variables</summary>
  <version_major>9</version_major>
  <version_minor>3</version_minor>
  <build_number>38</build_number>
</template_info>
<apptemplate>
  <rewrite>
    <rewriteaction_list>
      <rewriteaction>
        <name>Rw_name</name>
        <type>replace</type>
        <target>HTTP.REQ.BODY(10000).AFTER_REGEX(re/number/).BEFORE_REGEX(re/address/)</target>
        <stringbuilderexpr>"NA"</stringbuilderexpr>
        <allow_unsafe_pi1>NO</allow_unsafe_pi1>
```

```
        </rewriteaction>
        <rewriteaction>
          .
          .
          .
        </rewriteaction>
        .
        .
        .
      </rewriteaction_list>
      <rewritepolicy_list>
        <rewritepolicy>
          <name>Rw_number_NA</name>
          <rule>HTTP.REQ.BODY(100000).CONTAINS("admin")</rule>
          <action>Rw_name</action>
        </rewritepolicy>
        <rewritepolicy>
          .
          .
          .
        </rewritepolicy>
        .
        .
        .
      </rewritepolicy_list>
    </rewrite>
    <appunit_list>
      <appunit>
        <name>SharePoint_Team_Sitedefault</name>
        <rule />
        <expressiontype>PE</expressiontype>
        <servicetype>HTTP</servicetype>
        <ipv46>0.0.0.0</ipv46>
        <ipmask>*</ipmask>
        <port>0</port>
        <range>1</range>
        <persistencetype>NONE</persistencetype>
        <timeout>2</timeout>
        <persistencebackup>NONE</persistencebackup>
        <backuppersistencetimeout>2</backuppersistencetimeout>
        <lbmethod>LEASTCONNECTION</lbmethod>
        <persistmask>255.255.255.255</persistmask>
        <v6persistmasklen>128</v6persistmasklen>
        <pq>OFF</pq>
        <sc>OFF</sc>
        <m>IP</m>
        <datalength>0</datalength>
        <dataoffset>0</dataoffset>
        <sessionless>DISABLED</sessionless>
        <state>ENABLED</state>
        <connfailover>DISABLED</connfailover>
        <clttimeout>180</clttimeout>
        <somethod>NONE</somethod>
        <sopersistence>DISABLED</sopersistence>
        <redirectportrewrite>DISABLED</redirectportrewrite>
        <downstateflush>DISABLED</downstateflush>
```

```
        <gt2gb>DISABLED</gt2gb>
        <ipmapping>0.0.0.0</ipmapping>
        <disableprimaryondown>DISABLED</disableprimaryondown>
        <insertvserveripport>OFF</insertvserveripport>
        <authentication>OFF</authentication>
        <authn401>OFF</authn401>
        <push>DISABLED</push>
        <pushlabel>none</pushlabel>
        <l2conn>OFF</l2conn>
      </appunit>
      <appunit>
        .
        .
        .
      </appunit>
      .
      .
      .
    </appunit_list>
    </apptemplate>
    <parameters>
      <property_list>
        <property>
          <variable_definition_list>
            <variable_definition>
              <name>body_size</name>
              <defaultvalue>10000</defaultvalue>
              <description>Evaluation Scope</description>
              <startindex>14</startindex>
              <length>5</length>
            </variable_definition>
            .
            .
            .
          </variable_definition_list>
          <object_type>rewriteaction</object_type>
          <object_name>Rw_name</object_name>
          <name>target</name>
        </property>
        .
        .
        .
      </property_list>
    </parameters>
  </template>
```

Example of a Deployment File

Following is the deployment file associated with the "SharePoint_Team_Site" application in the preceding example:

```
<?xml version="1.0" encoding="UTF8" ?>
<template_deployment>
  <template_info>
    <application_name>SharePoint_Team_Site</application_name>
    <templateversion_major>1</templateversion_major>
    <templateversion_minor>1</templateversion_minor>
    <author>Ed</author>
    <introduction>An application for managing a SharePoint team site with images, reports, and, XML conter
    <summary>This template includes variables</summary>
    <version_major>9</version_major>
    <version_minor>3</version_minor>
    <build_number>38</build_number>
  </template_info>
  <appendpoint_list>
    <appendpoint>
      <ipv46>10.111.111.1</ipv46>
      <port>80</port>
      <servicetype>HTTP</servicetype>
    </appendpoint>
  </appendpoint_list>
  <service_list>
    <service>
      <ip>10.102.29.5</ip>
      <port>80</port>
      <servicetype>HTTP</servicetype>
    </service>
    <service>
      .
      .
      .
    </service>
    .
    .
    .
  </service_list>
  <variable_list>
    <variable>
      <name>body_size</name>
      <description>Evaluation Scope</description>
      <value>10000</value>
    </variable>
    <variable>
      .
      .
      .
    </variable>
    .
    .
    .
  </variable_list>
</template_deployment>
```

Access Gateway Applications

When you configure an AppExpert application to manage a web application through the Citrix® NetScaler® appliance, you also create a set of application units and configure a set of traffic optimization and security policies for each unit. The policies that you configure for each application unit (policies for features such as Compression, Caching, and Rewrite) evaluate traffic that is meant only for that unit. In addition to these policies, you might want to configure Access Gateway policies for the application as a whole to optimize the application traffic when accessed through the Access Gateway. The Access Gateway Applications feature enables you to configure Access Gateway policies (Authorization, Traffic, Clientless Access, and TCP Compression) for an AppExpert application. After you configure Access Gateway policies for AppExpert applications, you can include the policy configuration in the AppExpert application templates that you create.

You can also configure Access Gateway policies for intranet subnets, file shares, and other network resources.

Finally, you can create bookmarks for AppExpert applications and certain resources if you want users to be able to access them from the Access Gateway home page.

You can configure the entities in the Access Gateway Applications feature only by using the configuration utility.

How an Access Gateway Application Works

When you create an AppExpert application in the Applications node in the configuration utility, a corresponding Access Gateway application is automatically created in the Access Gateway Applications node. Additionally, a rule that uses the AppExpert application’s configured public endpoint is automatically created for the Access Gateway application entry. If multiple endpoints are configured for the AppExpert application, the rule includes all the configured public endpoints. The NetScaler appliance uses this rule to apply any configured Access Gateway policies to the traffic received at the AppExpert application's public endpoint. Traffic received at the AppExpert application’s public endpoint is first evaluated against the Access Gateway policies and then evaluated against the policies configured for AppExpert application’s application units.

The rule that is created for the Clientless Access policies for an Access Gateway application is an advanced expression that also uses the public endpoint that is configured for the AppExpert application. Therefore, before you configure Access Gateway policies for an AppExpert application, you must configure public endpoints for the AppExpert application.

When you include the Access Gateway configuration in an application template, deployment-specific information, such as IP address and port information, and the rule that is created from this information are not included in the template.

How a NetScaler Configuration for a File Share Works

On the NetScaler appliance, you can configure Authorization policies for a file share that is hosted on your organization's network.

When you create a file share, you specify a name for the file share and the network path to the file share. In the network path, you can specify either the name of the server or the server IP address. A rule that uses the components of the file share path is automatically created for the file share. This rule enables the appliance to identify requests for files hosted on the file share server. Any Authorization policies that are configured for the file share are applied to incoming requests.

The NetScaler configuration for a file share cannot be saved in AppExpert application templates.

How a NetScaler Configuration for an Intranet Subnet Works

For the intranet subnets that form a part of your network, you can configure policies for Authorization, Traffic, and TCP Compression on the NetScaler appliance. When adding an intranet subnet, you specify the IP address and the netmask of the intranet subnet. A rule that uses these two parameters is automatically created for the intranet subnet. The appliance applies the configured policies to any request that has a destination IP address and netmask set to the subnet's IP address and netmask, respectively.

The NetScaler configuration for an intranet subnet cannot be saved in AppExpert application templates.

How the Other Resources Category Works

The Other Resources category enables you to configure Access Gateway policies for any network resource by using a rule of your choice. When you configure the NetScaler appliance to process requests for the network resource, you configure a classic expression to identify the requests that are associated with the network resource. You can configure Authorization, Traffic, Clientless Access, and TCP Compression policies for a network resource in Other Resources. The NetScaler appliance applies the configured Access Gateway policies to any requests that match the configured rule.

The NetScaler configuration for a network resource in Other Resources cannot be saved in AppExpert application templates.

Entity Naming Conventions

The Access Gateway Applications feature enforces a naming convention for some of the entities that you create in this feature. For example, the names of the profiles that you create for Traffic policies for an intranet subnet always begin with a string that consists of the name of the intranet subnet followed by an underscore (_). The name that you provide for the entity is appended to this string. If the name of a subnet is "subnet1," the name of the profile begins with "subnet1_." When such a naming convention is required (in the text box in which you type the name of an entity, for example), the user interface automatically inserts the string with which the name of the entity must begin and does not allow you to modify it.

Adding File Shares

When creating a file share, you provide the network path to the file share. Any policies that you configure for a file share use the rule that is automatically created when you created the file share.

To configure a file share

1. In the navigation pane of the NetScaler configuration utility, expand AppExpert, and then click Access Gateway Applications.
2. In the details pane, click File Shares, and then do one of the following:
   - To add a file share, click File Shares, and then click Add.
   - To modify a file share, click File Shares, and then click Open.
3. In the Create File Share or Configure File Share dialog box, do the following:
   a. In the Name box, type a name for the file share you are adding. This parameter cannot be changed for an existing file share.
   b. In the Path box, type the path to the file share.

      The path to the file share may use either the name of the server or the IP address of the server.
   c. In Bookmark, in the Text to Display box, type a name for the file share as you would want it to appear on the Access Gateway home page.
   d. Click Create or OK, and then click Close.

Adding Intranet Subnets

You can specify authorization and Traffic policies for traffic that is bound for the intranet subnets that are configured in your network. The rules for these policies are automatically created by using the parameters you specify for the subnet.

To configure an intranet subnet

1. In the navigation pane of the NetScaler configuration utility, expand AppExpert, and then click Access Gateway Applications.
2. In the details pane, do one of the following:
   - To add an intranet subnet, click Intranet Subnets, and then click Add.
   - To modify an intranet subnet, click an intranet subnet, and then click Open.
3. In the Create Intranet Subnet or Configure Intranet Subnet dialog box, do the following:
   a. In the Name box, type a name for the intranet subnet you are adding. This parameter cannot be changed for an existing intranet subnet.
   b. In the IP Address box, type the IP address of the intranet subnet.
   c. In the Netmask box, type the netmask that will be used for the intranet subnet.
   d. Click Create or OK, and then click Close.

Adding Other Resources

For a network resource that you add to Other Resources, you must configure a classic expression that identifies the subset of traffic associated with the resource. For more information about configuring a classic expression, see the Policy Configuration and Reference.

To configure a resource in Other Resources

1. In the navigation pane of the NetScaler configuration utility, expand AppExpert, and then click Access Gateway Applications.
2. In the details pane, do one of the following:
   - To add a resource, click Other Resources, and then click Add.
   - To modify a resource, click a resource, and then click Open.
3. In the Create Resource or Configure Resource dialog box, do the following:
   a. In the Name box, type a name for the resource you are adding. This parameter cannot be changed for an existing resource.
   b. In the Rule box, type the rule that will identify the subset of traffic that is associated with the resource you are adding.

      Alternatively, click Configure, and then create the rule in the Create Expression dialog box.
   c. Click Create or OK, and then click Close.

Configuring Authorization Policies

You can configure Access Gateway authorization policies for AAA users and groups to access a resource.

To configure permissions for a AAA user or group to access a resource

1. In the navigation pane of the NetScaler configuration utility, expand AppExpert, and then click Access Gateway Applications.
2. In the details pane, in the Authorization column, click the icon for the application, file share, intranet subnet, or resource for which you want to configure authorization policies for AAA users and groups.
3. Do one of the following:
   - If the AAA user or group for which you want to configure permissions is already in the Groups/Users tree, drag the user or group from the Groups/Users tree to the Users or Groups node in the <application name> tree. Then, right-click the user or group and click Allow.
   - If the AAA user or group for which you want to configure permissions is not configured on the appliance, in the <application name> tree, right-click Users or Groups, and then click Add. In the Create AAA Group or Create AAA User dialog box, fill in the values, click Create, and then click Close.

     The user or group is created with the permission set to Allow. To change the permission setting, right-click the group or user, and then click the permission setting.
4. Click Close.

Configuring Traffic Policies

The traffic policies that you configure for the resources in the Access Gateway Applications node control client connections to the application. You do not have to configure a rule for the resource. The rule created automatically when you create the resource. You only need to associate a request profile with the traffic policy. In the traffic profile, you specify parameters such as the protocol, application time-out, and file type association.

To configure traffic policies for a resource

1. In the navigation pane of the NetScaler configuration utility, expand AppExpert, and then click Access Gateway Applications.

2. In the details pane, in the Traffic column, click the icon provided for the application, file share, intranet subnet, or resource for which you want to configure traffic policies.

3. In the Configure Traffic Policies dialog box, do the following:

   - To specify an existing traffic policy, click Insert Policy, and then, in the Policy Name column, click the name of the policy.

   - To configure a new policy, click Insert Policy, and then, in the Policy Name column, click New Policy. In the Create Traffic Policy dialog box, in the Name box, after the underscore (_), type a name for the policy. Then, in Request Profile, either select an existing request profile or click New to configure a new request profile. You can also select an existing profile and then click Modify to modify the profile.

     For more information about configuring a traffic policy or profile, see Access Gateway 10, Enterprise Edition at http://edocs.citrix.com/.

   - To modify a policy that you have inserted, in the Policy Name column, click the policy name, and then click Modify Policy. To modify only the associated profile, in the Profile column, click the name of the profile, and then click Modify Profile.

   - To regenerate the priorities assigned to the policies, click Regenerate Priorities.

   - To specify a new priority value for a policy, in the Priority column, double-click the assigned priority, and then enter the value you want.

   - To unbind a policy, click the policy, and then click Unbind Policy.

4. Click Apply Changes, and then click Close.

Configuring Clientless Access Policies

Clientless access, when configured for a resource on the NetScaler appliance, allows end-users to access the resource without using the Access Gateway client software. Users can use web browsers to access resources such as Outlook Web Access. You configure clientless access for a resource by configuring a clientless access policy that is associated with a clientless access profile.

To configure a clientless access policy for a resource in the Access Gateway Applications node

1. In the navigation pane of the NetScaler configuration utility, expand AppExpert, and then click Access Gateway Applications.
2. In the details pane, in the Clientless Access column, click the icon for the application, file share, intranet subnet, or resource for which you want to configure a clientless access policy.
3. In the Configure Clientless Access Policies dialog box, do the following:
   - To specify an existing clientless access policy, click Insert Policy, and then, in the Policy Name column, click the name of the policy.
   - To configure a new clientless access policy, click Insert Policy, and then, in the Policy Name column, click New Policy. In the Create Clientless Access Policy dialog box, in the Name box, after the underscore (_), type a name for the policy. Then, in Profile, either select an existing profile or click New to configure a new profile. You can also select an existing profile and then click Modify to modify the profile.

     For more information about configuring a clientless access policy or profile, see Access Gateway 10, Enterprise Edition at http://edocs.citrix.com/.
   - To modify a policy that you have inserted, in the Policy Name column, click the policy name, and then click Modify Policy. To modify only the associated profile, in the Profile column, click the name of the profile, and then click Modify Profile.
   - To specify a new priority value for a policy, in the Priority column, double-click the assigned priority, and then enter the value you want.
   - To unbind a policy, click the policy, and then click Unbind Policy.
4. Click Apply Changes, and then click Close.

Configuring TCP Compression Policies

You can configure TCP compression policies for an application to increase the performance of the application. TCP compression reduces network latency, reduces bandwidth requirements, and increases the speed of transmission. When configuring a TCP compression policy, you associate a compression action with the policy. The compression action specifies either Compress, GZIP, Deflate, or NoCompress as the compression type. For more information about the compression policies, and compression actions, see Access Gateway 10, Enterprise Edition at http://edocs.citrix.com/.

To configure a TCP compression policy for a resource in the Access Gateway Applications node

1. In the navigation pane of the NetScaler configuration utility, expand AppExpert, and then click Access Gateway Applications.

2. In the details pane, in the TCP Compression column, click the icon for the application, file share, intranet subnet, or resource for which you want to configure a TCP compression policy.

3. In the Configure TCP Compression Policies dialog box, do the following:

   - To specify an existing TCP compression policy, click Insert Policy, and then, in the Policy Name column, click the name of the policy.

   - To create a new TCP compression policy, click Insert Policy, and then, in the Policy Name column, click New Policy. In the Create TCP Compression Policy dialog box, in the Policy Name box, after the underscore ("_"), type a name for the policy. Then, in Action, either select an existing action or click New and configure a new action. You can also click View to view the configured compression type.

     For more information about configuring a TCP compression policy or action, see Access Gateway 10, Enterprise Edition at http://edocs.citrix.com/.

   - To modify a policy that you have inserted, in the Policy Name column, click the policy name, and then click Modify Policy.

   - To regenerate the priorities assigned to the policies, click Regenerate Priorities.

   - To specify a new priority value for a policy, in the Priority column, double-click the assigned priority, and then enter the value you want.

   - To unbind a policy, click the policy, and then click Unbind Policy.

4. Click Apply Changes, and then click Close.

Configuring Bookmarks

You can configure bookmarks for an application or for a resource that you configure in the Other Resources category if you want the application or resource to be accessible from the Access Gateway home page.

To configure a bookmark for an Access Gateway application or a resource in the Other Resources category

1. In the navigation pane of the NetScaler configuration utility, expand AppExpert, and then click Access Gateway Applications.
2. In the details pane, click the application or resource for which you want to configure a bookmark, and then click Configure Bookmark.
3. In the Create Bookmark dialog box, configure values for the parameters.

   For more information about the parameters in the Create Bookmark dialog box, see Access Gateway 10, Enterprise Edition at http://edocs.citrix.com/.
4. Click Create, and then click Close.

AppQoE

Application level Quality of Experience (AppQoE) integrates several existing policy-based security features of the NetScaler appliance into a single integrated feature that takes advantage of a new queuing mechanism, *fair queuing*. Fair queuing manages requests to load-balanced web servers and applications at the virtual server level instead of at the service level, allowing it to handle queuing of all requests to a web site or application as one group before load balancing, instead of as separate streams after load balancing.

The features that are integrated into AppQoE are HTTP Denial-of-Service Protection (HDOSP), Priority Queuing (PQ), SureConnectSureConnect and . Collectively these services provide protection against a number of problems:

- **Simple overload.** Any server, no matter how robust, can accept only a limited number of connections at one time. When a protected web site or application receives too many requests at once, the Surge Protection feature detects the overload and queues the excess connections til the server can accept them. The Priority Queuing feature ensures that whoever most needs access to a resource is provided access without having to wait behind other lower-priority requests. The SureConnect feature displays an alternate web page that notifies users that the resource that they requested is not available.

- **Denial-of-Service (DOS) attacks.** Any public-facing resource is vulnerable to attacks whose purpose is to bring that service down and deny legitimate users access to it. The Surge Protection, Priority Queuing, and SureConnect features help manage DOS attacks as well as other types of high load. In addition, the HTTP Denial-of-Service Protection feature targets DOS attacks against your web sites, sending challenges to suspected attackers and dropping connections if the clients do not send an appropriate response.

Until the current version of the NetScaler operating system, these features were implemented at the service level, which means that each service was assigned its own queues. While service-level queues work, they also have some disadvantages, most of which are due to the NetScaler appliance having to load balance requests before implementing any of the protection features that rely on queuing. Implementing protection features before queuing has a number of advantages, some of which are listed below:

- Absolute priority of connections as configured in the priority queuing feature can be maintained.

- Connections are not flushed if a service transitions state, as they are in a service-level queue.

- During periods of high load, such as a denial-of-service attack, HTTP DoS and SureConnect come into play before load balancing, allowing these features to detect and divert unwanted or lower-priority traffic from the load balancer before the load balancer must cope with it.

In addition to implementing fair queuing, AppQoE integrates a set of features that each provide a different set of tools to achieve a common goal: protecting your networked resources from excessive or inappropriate demand. Putting these features into a common framework enables you to configure and implement them more easily.

Enabling AppQoE

To configure AppQoE, you must first enable the feature.

To enable AppQoE by using the command line

At the command prompt, type the following commands:

- enable ns feature appqoe
- show ns feature

Example

```
> enable ns feature appqoe
 Done
> show ns feature

      Feature                 Acronym           Status
      -------                 -------           ------
 1)    Web Logging              WL               ON
 2)    Surge Protection         SP               ON
 3)    Load Balancing           LB               ON
...
29)   AppQoE                   AppQoE            ON
Done
```

To enable AppQoE by using the configuration utility

1. Navigate to System > Settings.
2. In the details pane, click Configure Advanced Features.
3. In the Configure Advanced Features dialog box, select the AppQoE check box.
4. Click OK.

AppQOE Actions

After enabling the AppQoE feature, you must configure one or more actions for handling requests.

Important: No specific individual parameters are required to create an action, but you must include at least one parameter or you cannot create the action.

To configure an AppQoE action by using the command line

At the command prompt, type the following commands:

- add appqoe action <name> [-priority <priority>] [-respondWith (ACS|NS) [<customfile>] [-altContentSvcName <string>] [-altContentPath <string>] [-maxConn <positive_integer>] [-delay <usecs>] [-polqDepth <positive_integer>] [-priqDepth <positive_integer>] [-dosTrigExpression <expression>] [-dosAction (SimpleResponse | HICResponse)]

- show appqoe action

Example

To configure priority queuing with policy queue depths of 10 and 1000 for medium and lowest priority queues, respectively:

```
> add appqoe action appqoe-act-basic-prhigh -priority HIGH
 Done

> add appqoe action appqoe-act-basic-prmedium -priority MEDIUM -polqDepth 10
 Done

> add appqoe action appqoe-act-basic-prlow -priority LOW -polqDepth 1000
 Done

> show appqoe action
1)     Name: appqoe-act-basic-prhigh
       ActionType: PRIORITY_QUEUING
       Priority: HIGH
       PolicyQdepth: 0
       Qdepth: 0

2)     Name: appqoe-act-basic-prmedium
       ActionType: PRIORITY_QUEUING
       Priority: MEDIUM
       PolicyQdepth: 10
       Qdepth: 0
```

3) Name: appqoe-act-basic-prlow
ActionType: PRIORITY_QUEUING
Priority: LOW
PolicyQdepth: 1000
Qdepth: 0
Done

To modify an existing AppQoE action by using the command line

At the command prompt, type the following commands:

- set appqoe action <name> [-priority <priority>] [-altContentSvcName <string>] [-altContentPath <string>] [-polqDepth <positive_integer>] [-priqDepth <positive_integer>] [-maxConn <positive_integer>] [-delay <usecs>] [-dosTrigExpression <expression>] [-dosAction (SimpleResponse | HICResponse)]
- show appqoe action

To remove an AppQoE action by using the command line

At the command prompt, type the following commands:

- rm appqoe action <name>
- show appqoe action

Parameters for configuring an AppQoE action

name

A name for the new action, or the name of the existing action that you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols.

priority

The priority queue to which the request is assigned. When a protected web server or application is heavily loaded and cannot accept additional requests, specifies the order in which waiting requests are to be fulfilled when resources are available. The choices are:

1. **HIGH.** Fulfills the request as soon as resources are available.
2. **MEDIUM.** Fulfills the request after it has fulfilled all requests in the HIGH priority queue.

3. **LOW.** Fulfills the request after it has fulfilled all requests in the HIGH and MEDIUM priority queues.

4. **LOWEST.** Fulfills the request only after it has fulfilled all requests in higher-priority queues.

If priority is not configured, then the NetScaler appliance assigns the request to the LOWEST priority queue by default.

respondWith

Configures the NetScaler ADC to take the specified Responder action when the specified threshold is reached. Must be used with one of the following settings:

- **ACS:** Serves content from an alternate content service. Threshold: maxConn (maximum connections) or delay.

- **NS:** Serves a built-in response from the NetScaler ADC. Threshold: maxConn (maximum connections) or delay.

- **NO ACTION:** Serves no alternative content. Assigns connections to the LOWEST priority queue if the maxConn (maximum connections) or delay threshold is reached.

altContentSvcName

If `-responseWith ACS` is specified, the name of the alternative content service, usually an absolute URL to the web server that hosts the alternate content.

altContentPath

If `-responseWith ( ACS | NS )` is specified, the path to the alternative content.

polqDepth

Policy queue depth threshold value for the policy queue associated with this action. When the number of connections in the policy queue associated with this action increases to the specified number, subsequent requests are assigned to the LOWEST policy queue. Minimum value: 1 Maximum value: 4,294,967,294

priqDepth

Policy queue depth threshold value for the specified priority queue. If the number of requests in the specified queue on the virtual server to which the policy associated with the current action is bound increases to the specified number, subsequent requests are assigned to the LOWEST priority queue. Minimum value: 1 Maximum value: 4,294,967,294

maxConn

The maximum number of connections that can be open for requests that match the policy rule. Minimum value: 1 Maximum value: 4,294,967,294

delay

The delay threshold, in microseconds, for requests that match the policy rule. If a matching request has been delayed for longer than the threshold, the NetScaler appliance performs the specified action. If NO ACTION is specified, then the appliance assigns requests to the LOWEST priority queue. Minimum value: 1 Maximum value:

599999,999

dosTrigExpression

Adds an optional second-level check to trigger DoS actions.

dosAction

Action to take when the ADC determines that it or a protected server is under DoS attack. Possible values: SimpleResponse, HICResponse

To configure an AppQoE action by using the configuration utility

1. Navigate to App-Expert > AppQoE > Actions.
2. In the details pane, do one of the following:
   - To create a new action, click Add.
   - To modify an existing action, select the action, and then click Edit.
3. In the Create AppQoE Action or the Configure AppQoE Action screen, type or select values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring the AppQoE Action" as follows (asterisk indicates a required parameter):
   - Name—name
   - Action type—respondWith
   - Priority—priority
   - Policy Queue Depth—polqDepth
   - Queue Depth—priqDepth
   - DOS Action—dosAction
4. Click Create or OK.

AppQoE Parameters

In the AppQoE parameters, you configure the session life of an AppQoE session, the file name of the file containing the customized response, and the number of client connections that can be placed in a queue.

To configure the AppQoE parameter settings by using the command line

At the command prompt, type the following commands:

- set appqoe parameter [-sessionLife <secs>] [-avgwaitingclient <positive_integer>] [-MaxAltRespBandWidth <positive_integer>] [-dosAttackThresh <positive_integer>]
- show appqoe parameter

Parameters for configuring the AppQoE parameters

sessionLife

Number of seconds to wait after displaying alternate content before the ADC displays the same content again. Default value: 300 Maximum Minimum value: 1 Maximum value: 4,294,967,294

avgwaitingclient

The average number of client requests that can be in the service waiting queue. Default value: 1000000 Maximum value: 4,294,967,294

MaxAltRespBandWidth

The maximum bandwidth to consume when sending alternate responses. If the maximum is reached, the ADC quits sending the alternate content til bandwidth consumption drops. Default value: 100 Minimum value: 1 Maximum value: 4,294,967,294

dosAtckThrsh

The denial-of-service attack threshold. The number of connections that must be waiting in queues before the ADC responds with DoS protection measures. Default value: 2000 Minimum value: 0 Maximum value: 4,294,967,294

To configure the AppQoE parameter settings by using the configuration utility

1. Navigate to AppExpert > AppQoE.
2. In the details pane, click Configure AppQoE Parameters.
3. In the Configure AppQoE params screen, type or select values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring the AppQoE Parameters" as follows (asterisk indicates a required parameter):
   - Session Life (secs)—sessionLife
   - Average waiting client—avgwaitingclient
   - Alternate Response Bandwidth Limit(Mbps) —MaxAltRespBandWidth
   - DOS Attack Threshold —dosAttackThresh
4. Click OK.

AppQoE Policies

To implement AppQoE, you must configure at least one policy to tell your NetScaler ADC how to distinguish the connections to be queued in a specific queue.

To configure an AppQoE policy by using the command line

At the command prompt, type the following command:

add appqoe policy <name> -rule <expression> -action <string>

Example

The following example selects requests with a User-Agent header that contains "Android", and assigns them to the medium priority queue. These requests come from smartphones and tablets that run the Google Android operating system.

```
> add appqoe action appqoe-act-primd -priority MEDIUM
Done
> add appqoe policy appqoe-pol-primd -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"Android\")" -acti
Done
> sh appqoe policy appqoe-pol-primd
      Name: appqoe-pol-primd
      Rule: HTTP.REQ.HEADER("User-Agent").CONTAINS("Android")
      Action: appqoe-act-primd
      Hits: 0

Done
```

Parameters for configuring an AppQoE policy

name

A name for the AppQoE policy. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should chose a name that helps identify the type of action.

rule

A NetScaler expression that tells the appliance which connections it should handle. For complete information about policy expressions, see the *Citrix NetScaler Policy Configuration and Reference Guide* at http://support.citrix.com/article/CTX132362.

action

The AppQoE action to perform when a connection matches the policy.

To configure an AppQoE policy by using the configuration utility

1. Navigate to App-Expert > AppQoE > Policies.
2. In the details pane, do one of the following:
   - To create a new policy, click Add.
   - To modify an existing policy, select the policy, and then click Edit.
3. If you are creating a new policy, in the Create AppQoE Policy dialog, in the Name text box, type a name for your new policy.

   The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should chose a name that helps identify the purpose and effect of this policy.

   If you are modifying an existing policy, skip this step. You cannot change the name of an existing policy.
4. In the Action drop-down list, choose the AppQoE action to perform when the policy matches a connection. Click the plus (+) to open the Add AppQoE Action dialog and add a new action.
5. In the Rule text box, either enter the policy expression directly, or click New to create a policy expression. If you click New, perform the following steps:
   a. In the Create Expression dialog box, click Add.
   b. In the Add Expression dialog box, select a common expression from the Frequently Used Expressions drop-down list, or use the Construct Expression drop-down lists to create the expression that defines which traffic to filter.

      If you choose to create your own expression, you start by selecting the first term from the first drop-down list on the left side of the Construct Expression area. The choices in that list are:

      - HTTP: All traffic to port 80 and port 443.
      - SYS:
      - CLIENT:
      - SERVER:
      - ANALYTICS:
      - TEXT:

      The default choice is HTTP. After you make a choice in the first drop-down list (or accept the default), you can choose the next term in your expression from the drop-down list to the right of it. The terms in that list and other lists that follow change depending on your previous choices; the lists offer only terms that are valid choices. Continue to select terms until you have finished the expression.

Use the Help and Preview Expression areas for assistance when creating the expression. For a complete description of the available choices, see the *Citrix NetScaler Policy Configuration and Reference Guide* at http://support.citrix.com/article/CTX132362.

c. When you have created the expression that you want, click OK. The expression is added in the Expression text box.

6. Click Create. The expression appears in the Rule text box.

Entity Templates

An entity template is a collection of configuration information for an individual entity on a Citrix® NetScaler® appliance. It provides a specification and a set of defaults for a configurable NetScaler entity, such as a policy, virtual server, service, or action. By using a template that defines a set of defaults, you can quickly configure multiple entities that require a similar configuration while eliminating several configuration steps.

Entity templates are available only in the configuration utility. You use the NetScaler configuration utility to create, manage, and use any type of entity template. You can share entity templates with other administrators and manage local folders that contain the templates. You can also import entity templates from and export entity templates to your local computer.

Before creating a template, you should be familiar with the configuration of the entity.

Note: You use entity templates to configure individual entities. To configure multiple entities related to a particular Web application, you must use an application template. For more information, see "AppExpert Applications and Templates."

How Entity Templates Work

When you create a template for a NetScaler entity, you specify default values for the entity. You specify what values must be read-only, what values must not be displayed, and what values users can configure. You also configure the pages that compose the template import wizard. All the information and settings you provide are stored in the template file.

When a user imports the entity template to a NetScaler appliance, a wizard guides the user through the various pages that you configured for the template. The wizard displays the read-only parameter values and prompts the user to specify values for the configurable parameters. After the user follows the instructions in the wizard, the appliance creates the entity with the configured values.

For example, you can create an entity template for HTTP services that provides a text box for a service name and assigns preset values for the service protocol, timeouts, thresholds, and monitors. Later, when you use the template to create new HTTP services, a wizard prompts you for a service name and supplies the preset values that you would otherwise have configured manually.

The procedure for creating entity templates for load balancing virtual servers is different than the AppExpert procedure for creating other entity templates. For more information, see "Creating an Entity Template."

In addition, the procedure for using the template to create the load balancing virtual server entity is different. For more information, see "Creating an Entity from a Template."

Configuring an Entity Template

You can create or modify an entity template either from the AppExpert feature node or from the associated NetScaler feature node for the entity. For example, you can create a content switching virtual server entity template in either the AppExpert feature node or the content switching feature node in the configuration utility.

If you create a template that is not based on an existing entity, you can specify the following options and settings for the template:

- The default value of a parameter.
- Whether the default values are visible to users.
- Whether the default values can be changed by users.
- The number of pages in the entity import wizard, including the page names, text, and available parameters.
- The entities that must be bound to the entity for which the template is being created.

  For example, when you are creating a cache redirection virtual server template, you can specify the policies that you want to bind to the cache redirection virtual servers that you create from the template. However, only binding information is included in the template. The bound entities are not included. If the entity template is imported to another NetScaler appliance, the bound entities must exist on the appliance at import time for the binding to succeed. If none of the bound entities exist on the target appliance, the entity (for which the template was configured) is created without any bindings. If only a subset of the bound entities exist on the target appliance, they are bound to the entity that is created from the template.

When you create a template based on an existing entity, the configuration settings of the entity appear in the template. All bound entities are selected by default, but you can modify bindings as necessary. As in the case of a template that is not based on an existing entity, only binding information is included and not the entities. You can either save the template with the existing configuration settings or use the settings as a basis for creating a new configuration for a template.

The procedure for creating a load balancing virtual server is distinctly different from the procedure for creating other entity templates. For more information, see Creating an Entity Template.

Creating an Entity Template

You can create entity templates in either the AppExpert node or the NetScaler feature node that corresponds to the type of entity. For example, you can create a content switching virtual server template from the entity templates tab of the AppExpert feature's Templates node or in the Content Switching node. You can also specify the parameters that you want the template to store, and specify whether you want the template import wizard to prompt the user for certain parameter values.

However, when creating load balancing virtual servers, you do not have the option of specifying parameter values that you want stored in the template. You create a load balancing virtual server template by selecting an existing load balancing virtual server and configuring any variables that you might want to create in existing parameters and bound policies. The variables can be assigned values when you create a load balancing virtual server from the template. The template stores load balancing parameters such as the virtual server's IP address and port number, bound policies, actions, and variable definitions. A deployment file is also created, automatically, from the load balancing configuration. The deployment file stores deployment-specific information, such as information about bound services, service groups, and the name-value pairs of variables. If the bound entities that are included in the template are already configured on the NetScaler appliance to which the template is imported, duplicates are created, with names that are generated automatically in a particular format. The duplicate entities are based on the parameter information stored in the entity template.

When you create a load balancing virtual server template from the AppExpert node, the template is always saved to the `/nsconfig/nstemplates/entities/lb vserver/` folder. If you want to save the template to a different folder, create the template from the Virtual Servers pane in the Load Balancing node. The deployment file is created with the name with which you save the template file, but with the string `_deployment` appended to the name. The deployment file is saved to the `/nsconfig/nstemplates/entities/lb vserver/deployment_files/` folder. For more information about deployment files for load balancing virtual server templates, see "Understanding Load Balancing Entity Templates and Deployment Files."

Note: You can use either of the first two procedures for creating any template, except for a load balancing virtual server template. For creating a load balancing virtual server template, use the third or fourth procedure.

To create an entity template by using the AppExpert feature node

1. Navigate to AppExpert > Templates.
2. In the details pane, on the Entity Templates tab, do one of the following:
   - To create a new template, click Add. In the Select the Template Type dialog box, select the template type, and then click OK.
   - To create a duplicate of an existing entity template, in the details pane, select the entity template, and then click Add.
3. In the Create...Template dialog box, follow the instructions to create a template.

   If you are creating a duplicate of an existing entity template, in the Create...Template dialog box, on the Specify Template Name page, you must change the name of the entity template.
4. Click Finish, and then click Exit.

To create an entity template by using its corresponding feature node

1. In the navigation pane of the NetScaler configuration utility, select the feature (for example, Content Switching), and then select the entity (for example, Virtual Servers), for which you want to create the entity template.
2. At the top of the details pane, click Entity Templates, and then click Create Template.
3. In the Create...Template dialog box, follow the instructions to create a template.
4. Click Finish, and then click Exit.

To create a load balancing virtual server template from the AppExpert node

1. Navigate to AppExpert > Templates.
2. In the details pane, on the LB Templates tab, click Add.
3. In the Select Load Balancing Virtual Server dialog box, select the load balancing virtual server whose configuration you want to save to a template file, and then click OK.
4. In the Create Template dialog box, provide the following information:
   - Name. The name of the template.

     Note: The Folder field shows the location to which the template will be saved. You cannot modify the path that is displayed.
   - Configure Variables. Configure variables for the load balancing template. For more information, see "Configuring Variables in Load Balancing Virtual Server Templates."
   - Introduction Description. A description of the virtual server for which you are creating a template.
   - Summary Description. A summary of the configuration or additional instructions for other administrators, such as a description of any additional steps that need to be followed after the entity is successfully created.
   - Author. The creator of the template.
   - Major. An optional major version number of your choice, to be specified if you want to maintain versions of your template.
   - Minor. An optional minor version number of your choice, to be specified if you want to maintain minor versions of your template.

     You can maintain versions by incrementing one or both of the version numbers each time you maintain the template. The Entity Template Wizard concatenates and displays the major and minor version numbers during import. For example, if the major version number is 1 and the minor version is 1, the Entity Template Wizard displays a version number of 1.1.
5. Click OK.

To create a load balancing virtual server template from the Load Balancing Virtual Servers pane

1. Navigate to Load Balancing > Virtual Servers.
2. In the details pane, select the virtual server on which to base the template,, and then click Create Template. You might have to click the scroll arrow at the bottom right of the pane to bring the Create Template button into view.
3. In the Create Template dialog box, provide the following information:
   - Name. The name of the template.
   - Folder. The location to which the template will be saved.

     Note: If you want to save the template to the appliance, you can save it only to the `/nsconfig/nstemplates/entities/lb vserver/` directory (the path displayed by default in Folder. If you want to save the template file to a folder on your computer, click the down-arrow on the Browse button, click Local, and then select a folder.
   - Configure Variables. Configure variables for the load balancing template. For more information, see "Configuring Variables in Load Balancing Virtual Server Templates."
   - Introduction Description. A description of the virtual server for which you are creating a template.
   - Summary Description. A summary of the configuration or additional instructions for other administrators, such as a description of any additional steps that need to be followed after the entity is successfully created.
   - Author. The creator of the template.
   - Major. An optional major version number of your choice, to be specified if you want to maintain versions of your template.
   - Minor. An optional minor version number of your choice, to be specified if you want to maintain minor versions of your template.

     You can maintain versions by incrementing one or both of the version numbers each time you maintain the template. The Entity Template Wizard concatenates and displays the major and minor version numbers during import. For example, if the major version number is 1 and the minor version is 1, the Entity Template Wizard displays a version number of 1.1.
4. Click OK.

Configuring Variables in Load Balancing Virtual Server Templates

Load balancing virtual server templates support the declaration of variables in the configured load balancing parameters and in bound policies and actions. The ability to declare variables enables you to replace preconfigured values with values that suit the environment into which you are importing the template. The Entity Template Wizard, which appears when you import a template, includes a Specify Variable Values page on which you can specify appropriate values for the variables that are configured for the entity template. This wizard page appears only when you import a template that is configured with existing variables.

As an example, consider the following expression configured for a policy that is bound to a load balancing virtual server for which you are creating a template. The expression evaluates the value of the Accept-Language header in an HTTP request.

```
HTTP.REQ.HEADER("Accept-Language").CONTAINS("en-us")
```

If you want the value of the header to be configurable at import time, you can specify the string `en-us` as a variable. When importing the template, you can specify a new value for the variable on the Specify Variable Values page.

After you create a variable, you can do the following:

- Assign additional strings to an existing variable. After you create a variable for a string, you can select and assign other parts of the same or different expression to the variable. The strings you assign to a variable need not be the same. At import time, all the strings that are assigned to the variable are replaced with the value that you provide.
- View the string or strings that are assigned to the variable.
- View a list of all the entities and parameters that use the variable.

To configure variables in a load balancing virtual server template

1. Navigate to Load Balancing > Virtual Servers.
2. In the details pane, right-click the virtual server that you want to export to a template file, and then click Create Template.
3. In the Create Template dialog box, modify the default template file name if required, specify the location where you want to save the template, and then click Configure Variables.
4. In the Configure Variables dialog box, click the tab that lists the entity for which you want to configure a variable, select the entity, and then click Configure Variables.
5. In the Variables for <Entity Type>: <Entity Name> dialog box, click the  button next to the parameter value or expression in which you want to create a variable.
6. In the Variables for <Field Name> dialog box, do the following:

   - To create a variable, in the text box that displays the configured expression or value, select the string that you want to be configurable at import time, and then click Add. In the Create Variable dialog box, specify a name and a description for the variable, and then click Create.

     The name of the variable, its value, and the description you provided appear in the Available Variables listing in the dialog box. The name you provide will be the name of the associated field in the template import wizard, and the description will appear as alt text when the user positions the mouse pointer over the field.

   - To modify a variable, in the Available Variables list, click the variable, and then click Open. In the Create Variable dialog box, modify the value and the description, and then click OK.

     The new value that you specify will not replace the text selected in the text box that displays the configured expression or value. However, when you import the template, the new value will be displayed as the default value for the variable in the template import wizard.

   - To view all the strings that are assigned to a given variable, in the Available Variables listing, click the name of the variable. The strings that are assigned to the variable are highlighted.

   - To view a list of all the parameters, expressions, and actions in which the variable is used, in the Available Variables listing, click the variable whose references you want to view, and then click Show References.

   - To assign a string to an existing variable, in the text box that displays the expression you configured, select the string you want to assign to an existing variable, right-click the selection, click Use existing Variable, and then click the name of the variable to which you want to assign the string.

     If a variable has multiple strings assigned to it, when you specify a new value for the variable during import, all strings assigned to the variable are replaced with the

new value.

7. Click Close.

Modifying an Entity Template

You can modify only the parameters, bindings, and pages configured for a template. The name and location of the template specified when the template was created cannot be changed. The NetScaler appliance does not provide you with the option of modifying a load balancing virtual server template.

To modify an entity template by using the AppExpert feature node

1. Navigate to AppExpert > Templates.
2. In the details pane, on the Entity Templates tab, select the template you want to change, and then click Open.
3. In the Modify...Template dialog box, follow the instructions to modify a template.
4. Click Finish, and then click Exit.

To modify an entity template by using its corresponding feature node

1. In the navigation pane, select the feature (for example, Content Switching), and then select the entity (for example, Virtual Servers) for which you want to modify the entity template.
2. At the top of the details pane, click Entity Templates, and then click Manage Template.
3. In the Manage <feature entity name> Entity Templates dialog box, select the template that you want to modify, and then click Modify.
4. In the Modify <template name> Template dialog box, follow the instructions to modify a template.
5. Click Finish, and then click Exit.
6. Click Close.

Deleting an Entity Template

Deleting an entity template does not affect any objects that have been created by using the template. You can delete a load balancing virtual server template only from the AppExpert feature node.

To delete an entity template by using the AppExpert feature node

1. Navigate to AppExpert > Templates.
2. In the details pane, on the Entity Templates tab, click the template you want to delete, and then click Remove.

To delete an entity template by using its corresponding feature node

1. In the navigation pane, select the feature (for example, Content Switching) and then select the entity (for example, Virtual Servers), for which you want to delete the entity template.
2. At the top of the details pane, click Entity Templates, and then click Manage Template.
3. In the Manage...Entity Templates dialog box, select the template that you want to delete, and then click Delete.

Creating an Entity from a Template

You can create an entity from an entity template either from the AppExpert feature node in the NetScaler configuration utility or from the NetScaler feature node that corresponds to the type of entity that you want to create. For example, you can create a content switching virtual server from a template with either the AppExpert feature node or the content switching feature node in the configuration utility.

The procedure for creating a load balancing virtual server from a template is different than the AppExpert procedure for creating other entities from templates.

After you create an instance of an entity using an entity template, you can configure it in the same way that you would any other object of that type, such as by using the configuration utility or the command line.

To create an entity from a template by using the AppExpert feature node

1. Navigate to AppExpert > Templates.
2. In the details pane, do one of the following:
   a. To create any entity other than a load balancing virtual server from a template, on the Entity Templates tab, click the template that you want to use, and then click Use Template.
   b. To create a load balancing virtual server from a template, on the LB Templates tab, click the template that you want to use, and then click Use Template.
3. In the <Entity Template Name> wizard, follow the instructions to create the entity on the NetScaler.
4. Click Finish, and then click Exit.

To create an entity from a template by using its corresponding feature node

1. In the navigation pane, expand a feature node (for example, Content Switching), and then click an entity subnode (for example, Virtual Servers).
2. At the top of the details pane, click Entity Templates, and then click Use Template.
3. Click the name of the template that you want to use.
4. In the Use <template name> Template wizard, follow the instructions to create the entity.

   Only templates that match the current context are displayed. For example, in the details pane for content switching virtual servers, only entity templates for content switching virtual servers appear, if configured.
5. Click Finish, and then click Exit.

To create a load balancing virtual server by using a load balancing virtual server template

1. Navigate to Load Balancing > Virtual Servers.
2. In the details pane, click Use Template.
3. In the Entity Template Wizard, follow the instructions to create a load balancing virtual server on the NetScaler.

   Only templates that match the current context are displayed. For example, when you click Browse (Appliance), only entity templates for load balancing virtual servers appear, if configured.
4. Click Finish, and then click Exit.

   Note: The Entity Template Wizard includes a Specify Variable Values page on which you can specify new values for variables. For more information about configuring variables in load balancing virtual server templates, see "Configuring Variables in Load Balancing Virtual Server Templates."

Managing Entity Template Folders

You can organize only load balancing virtual server template folders.

To organize load balancing virtual server template folders

1. Navigate to AppExpert > Templates > LB Templates.
2. In the Manage LB Templates dialog box, do one of the following:
   - To change the name of a folder, select the folder and click Rename.

     You can also click the folder that you want to rename, and then press F2. You cannot rename the top-level default folder.
   - To remove the folder, select the folder and click Delete.

     You can also click the folder that you want to remove, and then press the Delete key. You cannot remove the top-level default folder.
3. Click Close.

Uploading and Downloading Entity Templates

You can import the entity templates that are stored on your local computer. You can also download entity templates from the NetScaler appliance to your local computer and then import them to other NetScaler appliances.

Note: You cannot upload or download load balancing virtual server templates.

To upload an entity template to the NetScaler appliance

1. In the navigation pane of the NetScaler configuration utility, expand a feature node (for example, Content Switching), and then click a subnode (for example, Virtual Servers) for which you want to upload an entity template.
2. At the top of the details pane, click Entity Templates, and then click Manage Template.
3. In the Manage...Entity Templates dialog box, click the top-level folder, and then click Upload.
4. In the Upload Entity Template dialog box, navigate to the template file that you want to upload, and then click Select.
5. Click Close.

To download an entity template from the NetScaler appliance

1. In the navigation pane of the NetScaler configuration utility, expand a feature node (for example, Content Switching), and then click a subnode (for example, Virtual Servers) for which you want to upload an entity template.
2. At the top of the details pane, click Entity Templates, and then click Manage Template.
3. In the Manage...Entity Templates dialog box, click the template that you want to download, and then click Download.
4. In the Download Entity Template dialog box, navigate to the location at which you want to save the template on your local computer, enter a file name, and then click Save.
5. Click Close.

Understanding Load Balancing Entity Templates and Deployment Files

Load balancing entity templates are created in the same way that NetScaler application templates are created. When you export a load balancing virtual server to a template file, the following two files are automatically created:

- **Load balancing virtual server template file.** Contains XML elements that store the values of the parameters that are configured for the load balancing virtual server. The file also contains XML elements for storing information about bound policies.
- **Deployment file.** Contains XML elements that store deployment-specific information such as services, service groups, and configured variables.

In the template and deployment files, each unit of configuration information is encapsulated in a specific XML element that is meant for that unit type. For example, the load balancing method parameter, `lbMethod`, is encapsulated within the `<lbmethod>` and `</lbmethod>` tags.

Note: After you export a load balancing virtual server, you can add elements, remove elements, and modify existing elements before importing the configuration information to a NetScaler appliance.

Example of a Load Balancing Virtual Server Template

Following is an example of a template file that was created from a load balancing virtual server called "Lbvip":

```
<?xml version="1.0" encoding="UTF-8" ?>
 <template>
  <template_info>
   <entity_name>Lbvip</entity_name>
   <version_major>10</version_major>
   <version_minor>0</version_minor>
   <build_number>40.406</build_number>
  </template_info>
  <entitytemplate>
   <lbvserver_list>
    <lbvserver>
     <name>Lbvip</name>
     <servicetype>HTTP</servicetype>
     <ipv46>0.0.0.0</ipv46>
     <ipmask>*</ipmask>
     <port>0</port>
     <range>1</range>
     <persistencetype>NONE</persistencetype>
     <timeout>2</timeout>
```

```
        <persistencebackup>NONE</persistencebackup>
        <backuppersistencetimeout>2</backuppersistencetimeout>
        <lbmethod>LEASTCONNECTION</lbmethod>
        <persistmask>255.255.255.255</persistmask>
        <v6persistmasklen>128</v6persistmasklen>
        <pq>OFF</pq>
        <sc>OFF</sc>
        <m>IP</m>
        <datalength>0</datalength>
        <dataoffset>0</dataoffset>
        <sessionless>DISABLED</sessionless>
        <state>ENABLED</state>
        <connfailover>DISABLED</connfailover>
        <clttimeout>180</clttimeout>
        <somethod>NONE</somethod>
        <sopersistence>DISABLED</sopersistence>
        <sopersistencetimeout>2</sopersistencetimeout>
        <redirectportrewrite>DISABLED</redirectportrewrite>
        <downstateflush>DISABLED</downstateflush>
        <gt2gb>DISABLED</gt2gb>
        <ipmapping>0.0.0.0</ipmapping>
        <disableprimaryondown>DISABLED</disableprimaryondown>
        <insertvserveripport>OFF</insertvserveripport>
        <authentication>OFF</authentication>
        <authn401>OFF</authn401>
        <push>DISABLED</push>
        <pushlabel>none</pushlabel>
        <l2conn>OFF</l2conn>
        <appflowlog>DISABLED</appflowlog>
        <icmpvsrresponse>PASSIVE</icmpvsrresponse>
        <lbvserver_cmppolicy_binding_list>
          <lbvserver_cmppolicy_binding>
            <name>Lbvip</name>
            <policyname>NOPOLICY-COMPRESSION</policyname>
            <priority>100</priority>
            <gotopriorityexpression>END</gotopriorityexpression>
            <bindpoint>REQUEST</bindpoint>
          </lbvserver_cmppolicy_binding>
        </lbvserver_cmppolicy_binding_list>
      </lbvserver>
    </lbvserver_list>
  </entitytemplate>
</template>
```

Example of a Deployment File

Following is the deployment file associated with the virtual server in the preceding example:

```
<?xml version="1.0" encoding="UTF-8" ?>
  <template_deployment>
```

```
    <template_info>
      <entity_name>Lbvip</entity_name>
      <version_major>10</version_major>
      <version_minor>0</version_minor>
      <build_number>40.406</build_number>
    </template_info>
    <service_list>
      <service>
      <ip>1.2.3.4</ip>
      <port>80</port>
      <servicetype>HTTP</servicetype>
      </service>
    </service_list>
    <servicegroup_list>
      <servicegroup>
        <name>svcgrp</name>
        <servicetype>HTTP</servicetype>
        <servicegroup_servicegroupmember_binding_list>
          <servicegroup_servicegroupmember_binding>
            <ip>1.2.3.90</ip>
            <port>80</port>
          </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.8.0</ip>
          <port>80</port>
        </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.8.1</ip>
          <port>80</port>
        </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.9.0</ip>
          <port>80</port>
        </servicegroup_servicegroupmember_binding>
      </servicegroup_servicegroupmember_binding_list>
    </servicegroup>
  </servicegroup_list>
</template_deployment>
```

HTTP Callouts

For certain types of requests, or when certain criteria are met during policy evaluation, you might want to stall policy evaluation briefly, retrieve information from a server, and then perform a specific action that depends on the information that is retrieved. At other times, when you receive certain types of requests, you might want to update a database or the content hosted on a Web server. HTTP callouts enable you to perform all these tasks.

An HTTP callout is an HTTP request that the NetScaler appliance generates and sends to an external application when certain criteria are met during policy evaluation. The information that is retrieved from the server can be analyzed by default syntax policy expressions, and an appropriate action can be performed. You can configure HTTP callouts for HTTP content switching, TCP content switching, rewrite, responder, and for the token-based method of load balancing.

Before you configure an HTTP callout, you must set up an application on the server to which the callout will be sent. The application, which is called the *HTTP callout agent* , must be configured to respond to the HTTP callout request with the required information. The HTTP callout agent can also be a Web server that serves the data for which the NetScaler appliance sends the callout. You must make sure that the format of the response to an HTTP callout does not change from one invocation to another.

After you set up the HTTP callout agent, you configure the HTTP callout on the NetScaler appliance. Finally, to invoke the callout, you include the callout in a default syntax policy in the appropriate NetScaler feature and then bind the policy to the bind point at which you want the policy to be evaluated.

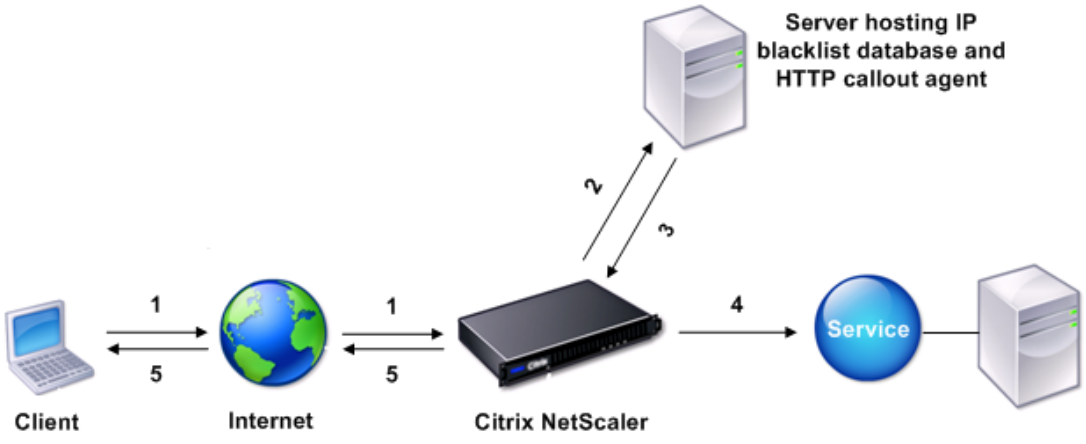
After you have configured the HTTP callout, you must verify the configuration to make sure that the callout is working correctly.

How an HTTP Callout Works

When the NetScaler appliance receives a client request, the appliance evaluates the request against the policies bound to various bind points. During this evaluation, if the appliance encounters the HTTP callout expression, SYS.HTTP_CALLOUT(<name>), it stalls policy evaluation briefly and sends a request to the HTTP callout agent by using the parameters configured for the specified HTTP callout. Upon receiving the response, the appliance inspects the specified portion of the response, and then either performs an action or evaluates the next policy, depending on whether the evaluation of the response from the HTTP callout agent evaluates to TRUE or FALSE, respectively. For example, if the HTTP callout is included in a responder policy, if the evaluation of the response evaluates to TRUE, the appliance performs the action associated with the responder policy.

If the HTTP callout configuration is incorrect or incomplete, or if the callout invokes itself recursively, the appliance raises an UNDEF condition, and updates the undefined hits counter.

The following figure illustrates the working of an HTTP callout that is invoked from a globally bound responder policy. The HTTP callout is configured to include the IP address of the client that is associated with an incoming request. When the NetScaler appliance receives a request from a client, the appliance generates the callout request and sends it to the callout server, which hosts a database of blacklisted IP addresses and an HTTP callout agent that checks whether the client's IP address is listed in the database. The HTTP callout agent receives the callout request, checks whether the client's IP address is listed, and sends a response that the NetScaler appliance evaluates. If the response indicates that the client's IP address is not blacklisted, the appliance forwards the response to the configured service. If the client's IP address is blacklisted, the appliance resets the client connection



1: Client request
2: HTTP callout request to check whether the client is blacklisted
3: Response from HTTP callout agent
4: Request forwarded to service if 3 indicates a safe IP address
5: Connection RESET if 3 indicates a bad IP address

Figure 1. HTTP Callout Entity Model

Notes on the Format of HTTP Requests and Responses

The NetScaler appliance does not check for the validity of the HTTP callout request. Therefore, before you configure HTTP callouts, you must know the format of an HTTP request. You must also know the format of an HTTP response, because configuring an HTTP callout involves configuring expressions that evaluate the response from the HTTP callout agent.

Format of an HTTP Request

An HTTP request contains a series of lines that each end with a carriage return and a line feed, represented as either <CR><LF> or \r\n.

The first line of a request (the *message line*) contains the HTTP method and target. For example, a message line for a GET request contains the keyword GET and a string that represents the object that is to be fetched, as shown in the following example:

GET /mysite/mydirectory/index.html HTTP/1.1\r\n

The rest of the request contains HTTP headers, including a required Host header and, if applicable, a message body.

The request ends with a bank line (an extra <CR><LF> or \r\n).

Following is an example of a request:

```
Get /mysite/index.html HTTP/1.1\r\n
Host: 10.101.101.10\r\n
Accept: */*\r\n
\r\n
```

Format of an HTTP Response

An HTTP response contains a status message, response HTTP headers, and the requested object or, if the requested object cannot be served, an error message.

Following is an example of a response:

HTTP/1.1 200 OK\r\n
Content-Length: 55\r\n
Content-Type: text/html\r\n
Last-Modified: Wed, 12 Aug 1998 15:03:50 GMT\r\n
Accept-Ranges: bytes\r\n
ETag: “04f97692cbd1:377”\r\n
Date: Thu, 19 Jun 2008 19:29:07 GMT\r\n
\r\n
<55-character response>

Configuring an HTTP Callout

When configuring an HTTP callout, you specify the destination and format of the request, the expected format of the response, and, finally, the portion of the response that you want to analyze.

For the destination, you either specify the IP address and port of the HTTP callout agent or engage a load balancing, content switching, or cache redirection virtual server to manage the HTTP callout requests. In the first case, the HTTP callout requests will be sent directly to the HTTP callout agent. In the second case, the HTTP callout requests will be sent to the virtual IP address (VIP) of the specified virtual server. The virtual server will then process the request in the same way as it processes a client request. For example, if you expect a large number of callouts to be generated, you can configure instances of the HTTP callout agent on multiple servers, bind these instances (as services) to a load balancing virtual server, and then specify the load balancing virtual server in the HTTP callout configuration. The load balancing virtual server then balances the load on those configured instances as determined by the load balancing algorithm.

For the format of the HTTP callout request, you can specify the individual attributes of the HTTP callout request (an attribute-based HTTP callout), or you can specify the entire HTTP callout request as a default syntax expression (an expression-based HTTP callout).

Note: The appliance does not check for the validity of the request. You must make sure that the request is a valid request. An incorrect or incomplete HTTP callout configuration results in a runtime UNDEF condition that is not associated with an action. The UNDEF condition merely updates the Undefined Hits counter, which enables you to troubleshoot an incorrectly configured HTTP callout. However, the appliance parses the HTTP callout request to enable you to configure certain NetScaler features for the callout. This can lead to an HTTP callout invoking itself. For information about callout recursion and how you can avoid it, see "Avoiding HTTP Callout Recursion."

Finally, regardless of whether you use HTTP request attributes or an expression to define the format of the HTTP callout request, you must specify the format of the response from the HTTP callout agent and the portion of the response that you want to evaluate. The response can be a Boolean value, a number, or text. The portion of the response that you want to evaluate is specified by an expression. For example, if you specify that the response contains text, you can use `HTTP.RES.BODY(<unit>)` to specify that the appliance must evaluate only the first <unit> bytes of the response from the callout agent.

At the command line, you first create an HTTP callout by using the add command. When you add a callout, all parameters are set to a default value of NONE, except the HTTP method, which is set to a default value of GET. You then configure the callout's parameters by using the set command. The set command is used to configure both types of callouts (attribute-based and expression-based). The difference lies in the parameters that are used for configuring the two types of callouts. Accordingly, the command-line instructions that follow include a set command for configuring an attribute-based callout and a set command for configuring an expression-based callout. In the configuration utility, all of these configuration tasks are performed in a single dialog box.

Note: Before you put an HTTP callout into a policy, you can modify all configured parameters except the return type. Once an HTTP callout is in a policy, you cannot completely modify an expression that is configured in the callout. For example, you

cannot change `HTTP.REQ.HEADER("myval")` to `CLIENT.IP.SRC`. However, you can modify the operators and arguments that are passed to the expression. For example, you can change `HTTP.REQ.HEADER("myVal1")` to `HTTP.REQ.HEADER("myVal2")`, or `HTTP.REQ.HEADER("myVal")` to `HTTP.REQ.HEADER("myVal").AFTER_STR(<string>)`. If the set command fails, create a new HTTP callout.

HTTP callout configuration involves configuring default syntax expressions. For more information about configuring default syntax expressions, see "Configuring Default Syntax Expressions: Getting Started."

To configure an HTTP callout by using the command line interface

At the command prompt, do the following:

1. Create a HTTP callout.

   add policy httpCallout <name>

   Example

   > add policy httpCallout mycallout

2. Configure the details of the HTTP callout.

   - To configure an attribute-based HTTP callout, type:

     set policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-port <port|*>] [-vServer <string>] [-returnType <returnType>] [-httpMethod (GET | POST)] [-hostExpr <string>] [-urlStemExpr <string>] [-headers <name(value)> ...] [-parameters <name(value)> ...] [-resultExpr <string>]

     Example

     > set policy httpCallout mycallout -vserver lbv1 -returnType num -httpMethod GET -hostExpr 'http.re
     -urlStemExpr "http.req.url" -parameters Name("My Name") -headers Name("MyHeader")
     -resultExpr "http.res.body(10000).length"

   - To configure an expression-based HTTP callout, type:

     set policy httpCallout <name> [-vServer <string>] [-returnType <returnType>] [-httpMethod (GET | POST)] [-fullReqExpr <string>] [-resultExpr <string>]

     Example

     > set policy httpCallout mycallout1 -vserver lbv1 -returnType num -httpMethod GET
     -fullReqExpr q{"GET " + http.req.url + "HTTP/" + http.req.version.major + "." + http.req.version.mino
     "r\nHost:10.101.10.10\r\nAccept: */*\r\n\r\n"}

3. Verify the configurations of the HTTP callout.

   show policy httpCallout <name>

To configure an HTTP callout by using the configuration utility

- Navigate to AppExpert > HTTP Callouts.
- In the details pane, do one of the following:
  - To create an HTTP callout, click Add.
  - To modify an existing HTTP callout, select the HTTP callout, and then click Open.
- In the Create HTTP Callout dialog box or Configure HTTP Callout dialog box, configure the parameters of the HTTP callout. For a description of the parameter, hover the mouse cursor over the check box.
- Click Create or OK.

Verifying the Configuration

For an HTTP callout to work correctly, all the HTTP callout parameters and the entities associated with the callout must be configured correctly. While the NetScaler appliance does not check the validity of the HTTP callout parameters, it indicates the state of the bound entities, namely the server or virtual server to which the HTTP callout is sent. The following table lists the icons and describes the conditions under which the icons are displayed.

Table 1. Icons That Indicate the States of Entities Bound to an HTTP Callout

Icon	Indicates that
	The state of the server that hosts the HTTP callout agent, or the load balancing, content switching, or cache redirection virtual server to which the HTTP callout is sent is UP.
	The state of the server that hosts the HTTP callout agent, or the load balancing, content switching, or cache redirection virtual server to which the HTTP callout is sent is OUT OF SERVICE.
	The state of the server that hosts the HTTP callout agent, or the load balancing, content switching, or cache redirection virtual server to which the HTTP callout is sent is DOWN.

For an HTTP callout to function correctly, the icon must be green at all times. If the icon is not green, check the state of the callout server or virtual server to which the HTTP callout is sent. If the HTTP callout is not working as expected even though the icon is green, check the parameters configured for the callout.

You can also verify the configuration by sending test requests that match the policy from which the HTTP callout is invoked, checking the hits counter for the policy and the HTTP callout, and verifying the responses that the NetScaler appliance sends to the client.

Note: An HTTP callout can sometimes invoke itself recursively a second time. If this happens, the hits counter is incremented by two counts for each callout that is generated by the appliance. For the hits counter to display the correct value, you must configure the HTTP callout in such a way that it does not invoke itself a second time. For more information about how you can avoid HTTP callout recursion, see "Avoiding HTTP Callout Recursion."

To view the hits counter for an HTTP callout

1. Navigate to AppExpert > HTTP Callouts.
2. In the details pane, click the HTTP callout for which you want to view the hits counter, and then view the hits in the Details area.

Invoking an HTTP Callout

After you configure an HTTP callout, you invoke the callout by including the `SYS.HTTP_CALLOUT(<name>)` expression in a default syntax policy rule. In this expression, <name> is the name of the HTTP callout that you want to invoke.

You can use default syntax expression operators with the callout expression to process the response and then perform an appropriate action. The return type of the response from the HTTP callout agent determines the set of operators that you can use on the response. If the part of the response that you want to analyze is text, you can use a text operator to analyze the response. For example, you can use the `CONTAINS(<string>)` operator to check whether the specified portion of the response contains a particular string, as in the following example:

SYS.HTTP_CALLOUT(mycallout).contains("Good IP address")

If you use the preceding expression in a responder policy, you can configure an appropriate responder action.

Similarly, if the part of the response that you want to evaluate is a number, you can use a numeric operator such as GT(int). If the response contains a Boolean value, you can use a Boolean operator.

Note: An HTTP callout can invoke itself recursively. HTTP callout recursion can be avoided by combining the HTTP callout expression with a default syntax expression that prevents recursion. For information about how you can avoid HTTP callout recursion, see "Avoiding HTTP Callout Recursion."

You can also cascade HTTP callouts by configuring policies that each invoke a callout after evaluating previously generated callouts. In this scenario, after one policy invokes a callout, when the NetScaler appliance is parsing the callout before sending the callout to the callout server, a second set of policies can evaluate the callout and invoke additional callouts, which can in turn be evaluated by a third set of policies, and so on. Such an implementation is described in the following example.

First, you could configure an HTTP callout called myCallout1, and then configure a responder policy, Pol1, to invoke myCallout1. Then, you could configure a second HTTP callout, myCallout2, and a responder policy, Pol2. You configure Pol2 to evaluate myCallout1 and invoke myCallout2. You bind both responder policies globally.

To avoid HTTP callout recursion, myCallout1 is configured with a unique custom HTTP header called "Request1." Pol1 is configured to avoid HTTP callout recursion by using the default syntax expression,

HTTP.REQ.HEADER(\"Request1\").EQ(\"Callout Request\").NOT.

Pol2 uses the same default syntax expression, but excludes the .NOT operator so that the policy evaluates myCallout1 when the NetScaler appliance is parsing it. Note that myCallout2 identifies its own unique header called "Request2," and Pol2 includes a default syntax expression to prevent myCallout2 from invoking itself recursively.
Example

```
> add policy httpCallout myCallout1

Done

> set policy httpCallout myCallout1 -IPAddress 10.102.3.95 -port 80 -returnType TEXT -hostExpr
 "\"10.102.3.95\"" -urlStemExpr "\"/cgi-bin/check_clnt_from_database.pl\"" -headers Request1
("Callout Request") -parameters cip(CLIENT.IP.SRC) -resultExpr "HTTP.RES.BODY(100)"

Done

> add responder policy Pol1 "HTTP.REQ.HEADER(\"Request1\").EQ(\"Callout Request\").NOT &&
SYS.HTTP_CALLOUT(myCallout1).CONTAINS(\"IP Matched\")" RESET

Done

> bind responder global Pol1 100 END -type OVERRIDE

Done

> add policy httpCallout myCallout2

Done

> set policy httpCallout myCallout2 -IPAddress 10.102.3.96 -port 80 -returnType TEXT -hostExpr
"\"10.102.3.96\"" -urlStemExpr "\"/cgi-bin/check_clnt_location_from_database.pl\"" -headers Request2
("Callout Request") -parameters cip(CLIENT.IP.SRC) -resultExpr "HTTP.RES.BODY(200)"

 Done

> add responder policy Pol2 "HTTP.REQ.HEADER(\"Request2\").EQ(\"Callout Request\").NOT &&
 HTTP.REQ.HEADER(\"Request1\").EQ(\"Callout Request\") && SYS.HTTP_CALLOUT(myCallout2).CONTAINS
(\"APAC\")" RESET

 Done

> bind responder global Pol2 110 END -type OVERRIDE

Done
```

Avoiding HTTP Callout Recursion

Even though the NetScaler appliance does not check for the validity of the HTTP callout request, it parses the request once before it sends the request to the HTTP callout agent. This parsing allows the appliance to treat the callout request as any other incoming request, which in turn allows you to configure several useful NetScaler features (such as integrated caching, SureConnect, and Priority Queuing) to work on the callout request.

However, during this parsing, the HTTP callout request can hit the same policy and therefore invoke itself recursively. The appliance detects the recursive invocation and raises an undefined (UNDEF) condition. However, the recursive invocation results in the policy and HTTP callout hit counters being incremented by two counts each instead of one count each.

To prevent a callout from invoking itself, you must identify at least one unique characteristic of the HTTP callout request, and then exclude all requests with this characteristic from being processed by the policy rule that invokes the callout. You can do so by including another default syntax expression in the policy rule. The expression must precede the `SYS.HTTP_CALLOUT(<name>)` expression so that it is evaluated before the callout expression is evaluated. For example:

<Expression that prevents callout recursion> && SYS.HTTP_CALLOUT(<name>)

When you configure a policy rule in this way, when the appliance generates the request and parses it, the compound rule evaluates to FALSE, the callout is not generated a second time, and the hit counters are incremented correctly.

One way by which you can assign a unique characteristic to an HTTP callout request is to include a unique custom HTTP header when you configure the callout. Following is an example of an HTTP callout called "myCallout." The callout generates an HTTP request that checks whether a client's IP address is present in a database of blacklisted IP addresses. The callout includes a custom header called "Request," which is set to the value "Callout Request." A globally bound responder policy, "Pol1," invokes the HTTP callout but excludes all requests whose Request header is set to this value, thus preventing a second invocation of myCallout. The expression that prevents a second invocation is `HTTP.REQ.HEADER(\"Request\").EQ(\"Callout Request\").NOT`.

Example

```
> add policy httpCallout myCallout
 Done

> set policy httpCallout myCallout -IPAddress 10.102.3.95 -port 80 -returnType TEXT -hostExpr "\"10.102.3.95
Done

> add responder policy Pol1 "HTTP.REQ.HEADER(\"Request\").EQ(\"Callout Request\").NOT && SYS.HTTP_CALL
Done

> bind responder global Pol1 100 END -type OVERRIDE
Done
```

Note: You can also configure an expression to check whether the URL of the request includes the URL stem expression that is configured for the HTTP callout. If you want to implement this scenario, make sure that the HTTP callout agent is dedicated to respond only to HTTP callouts and not to other client requests directed through the appliance. If the HTTP callout agent is an application or Web server that serves other client requests, such an expression will prevent the appliance from processing those client requests. Instead, use a unique custom header as described earlier.

Deployment Scenarios for HTTP Callouts

These topics demonstrate the configuration of HTTP callouts to perform various useful tasks. In all cases, the NetScaler appliance performs a callout to an external server where a callout agent is configured to respond to the request from the NetScaler appliance on the basis of data that is present on the external server. The callout agent is a program, for example, a CGI script, that is deployed in a container (for example, Apache Tomcat).

Note that the examples should be used only as a guideline when you want to create scripts that work in your deployment. The IP addresses and other entities used in these deployment scenarios should be modified to suit your environment.

Filtering Clients by Using an IP Blacklist

HTTP callouts can be used to block requests from clients that are blacklisted by the administrator. The list of clients can be a publicly known blacklist, a blacklist that you maintain for you organization, or a combination of both.

The NetScaler appliance checks the IP address of the client against the pre-configured blacklist and blocks the transaction if the IP address has been blacklisted. If the IP address is not in the list, the appliance processes the transaction.

To implement this configuration, you must perform the following tasks:

1. Enable responder on the NetScaler appliance.
2. Create an HTTP callout on the NetScaler appliance and configure it with details about the external server and other required parameters.
3. Configure a responder policy to analyze the response to the HTTP callout, and then bind the policy globally.
4. Create an HTTP callout agent on the remote server.

Enabling Responder

You must enable responder before you can use it.

To enable responder by using the configuration utility

1. Make sure that you have installed the responder license.
2. In the navigation pane, right-click Responder, and then click Enable Responder feature.

Creating an HTTP Callout on the NetScaler Appliance

Create an HTTP callout, HTTP-Callout-1, with the parameter settings shown in the following table. For more information about creating an HTTP callout, see "Configuring an HTTP Callout."

Table 1. Parameters and Values for HTTP-Callout-1

Parameter	Value
Name	HTTP-Callout-1
Server to receive callout request	
IP Address	10.103.9.95
Port	80
Request to send to the server	
Method	GET
Host Expression	10.102.3.95
URL Stem Expression	"/cgi-bin/check_clnt_from_database.pl"
Headers	
Name	Request
Value-expression	Callout Request
Parameters	
Name	Cip
Value-expression	CLIENT.IP.SRC
Server Response	
Return Type	TEXT
Expression to extract data from the response	HTTP.RES.BODY(100)

Configuring a Responder Policy and Binding it Globally

After you configure the HTTP callout, verify the callout configuration, and then configure a responder policy to invoke the callout. While you can create a responder policy in the Policies sub-node and then bind it globally by using the Responder Policy Manager, this demonstration uses the Responder Policy Manager to create the responder policy and bind the policy globally.

To create a responder policy and bind it globally by using the configuration utility

1. In the navigation pane, expand Responder.
2. In the details pane, under Policy Manager, click Policy Manager.
3. In the Responder Policy Manager dialog box, click Override Global.
4. Click Insert Policy, and then, under Policy Name, click New Policy.
5. In the Create Responder Policy dialog box, do the following:
    a. In Name, type Policy-Responder-1.
    b. In Action, select RESET.
    c. In Undefined-Result Action, select Global undefined-result action.
    d. In Expression, type the following default syntax expression:

        "HTTP.REQ.HEADER(\"Request\").EQ(\"Callout Request\").NOT && SYS.HTTP_CALLOUT(HTTP-Callout-1

    e. Click Create, and then click Close.
6. Click Apply Changes, and then click Close.

Creating an HTTP Callout Agent on the Remote Server

You must now create an HTTP callout agent on the remote callout server that will receive callout requests from the NetScaler appliance and respond appropriately. The HTTP callout agent is a script that is different for each deployment and must be written with the server specifications in mind, such as the type of database and the scripting language supported.

Following is a sample callout agent that verifies whether the given IP address is part of an IP blacklist. The agent has been written in the Perl scripting language and uses a MYSQL database.

The following CGI script checks for a given IP address on the callout server.

```
#!/usr/bin/perl -w
print "Content-type: text/html\n\n";
	use DBI();
	use CGI qw(:standard);
#Take the Client IP address from the request query
	my $ip_to_check = param('cip');
# Where a MYSQL database is running
	my $dsn = 'DBI:mysql:BAD_CLIENT:localhost';
# Database username to connect with
	my $db_user_name = ‘dbuser’;
# Database password to connect with
	my $db_password = 'dbpassword';
	my ($id, $password);
# Connecting to the database
	my $dbh = DBI->connect($dsn, $db_user_name, $db_password);
	my $sth = $dbh->prepare(qq{ select * from bad_clnt });
	$sth->execute();
	while (my ($ip_in_database) = $sth->fetchrow_array()) {
	chomp($ip_in_database);
# Check for IP match
	if ($ip_in_database eq $ip_to_check) {
	    print "\n IP Matched\n";
                                        $sth->finish();
                                    exit;
	     }
      }
      print "\n IP Failed\n";
      $sth->finish();
      exit;
```

ESI Support for Fetching and Updating Content Dynamically

Edge Side Includes (ESI) is a markup language for edge-level dynamic Web content assembly. It helps in accelerating dynamic Web-based applications by defining a simple markup language to describe cacheable and non-cacheable Web page components that can be aggregated, assembled, and delivered at the network edge. By using HTTP callouts on the NetScaler appliance, you can read through the ESI constructs and aggregate or assemble content dynamically.

To implement this configuration, you must perform the following tasks:

1. Enable rewrite on the NetScaler appliance.
2. Create an HTTP callout on the appliance and configure it with details about the external server and other required parameters.
3. Configure a rewrite action to replace the ESI content with the callout response body.
4. Configure a rewrite policy to specify the conditions under which the action is performed, and then bind the rewrite policy globally.

Enabling Rewrite

Rewrite must be enabled before it is used on the NetScaler appliance. The following procedure describes the steps to enable the rewrite feature.

To enable rewrite by using the configuration utility

1. Make sure that you have installed the rewrite license.
2. In the navigation pane, right-click Rewrite, and then click Enable Rewrite feature.

Creating an HTTP Callout on the NetScaler Appliance

Create an HTTP callout, HTTP-Callout-2, with the parameter settings shown in the following table. For more information about creating an HTTP callout, see "Configuring an HTTP Callout."

Table 1. Parameters and Values for HTTP-Callout-2

Parameter	Value
Name	HTTP-Callout-2
Server to receive callout request	
IP Address	10.102.56.51
Port	80
Request to send to the server	
Method	GET
Host Expression	10.102.56.51:80
URL Stem Expression	"HTTP.RES.BODY(500).AFTER_STR(\"src=\").BEFORE_STR(\"/>\")"
Headers	
Name	Name
Value-expression	Callout
Server Response	
Return Type	TEXT
Expression to extract data from the response	HTTP.RES.BODY(100)

Configuring the Rewrite Action

Create a rewrite action, Action-Rewrite-1, to replace the ESI content with the callout response body. Use the parameter settings shown in the following table.

Table 1. Parameters and Values for Action-Rewrite-1

Parameter	Value
Name	Action-Rewrite-1
Type	Replace
Expression to choose target text reference	"HTTP.RES.BODY(500).AFTER_STR (\" <example>\").BEFORE_STR (\"</example>\")"
String expression for replacement text	"SYS.HTTP_CALLOUT(HTTP-Callout-2)"

To configure the rewrite action by using the configuration utility

1. Navigate to Rewrite > Actions.
2. In the details pane, click Add.
3. In the Create Rewrite Action dialog box, in Name, type Action-Rewrite-1.
4. In Type, select REPLACE.
5. In Expression to choose target text reference, type the following default syntax expression:

   "HTTP.RES.BODY(500).AFTER_STR(\"<example>\").BEFORE_STR(\"</example>\")"
6. In the String expression for replacement text, type the following string expression:

   "SYS.HTTP_CALLOUT(HTTP-Callout-2)"
7. Click Create, and then click Close.

Creating the Rewrite Policy and Binding it Globally

Create a rewrite policy, Policy-Rewrite-1, with the parameter settings shown in the following table. You can create a rewrite policy in the Policies subnode and then bind it globally by using the Rewrite Policy Manager. Alternatively, you can use the Rewrite Policy Manager to perform both these tasks simultaneously. This demonstration uses the Rewrite Policy Manager to perform both tasks.

Table 1. Parameters and Values for Policy-Rewrite-1

Parameter	Value
Name	Policy-Rewrite-1
Action	Action_Rewrite-1
Undefined Result Action	-Global undefined-result action-
Expression	"HTTP.REQ.HEADER(\"Name\").CONTAINS (\"Callout\").NOT"

To configure a rewrite policy and bind it globally by using the configuration utility

1. In the navigation pane, expand Rewrite.
2. In the details pane, under Policy Manager, click Rewrite Policy Manager.
3. In the Rewrite Policy Manager dialog box, click Override Global.
4. Click Insert Policy, and then, in the Policy Name column, click New Policy.
5. In the Create Rewrite Policy dialog box, do the following:
    a. In Name, type Policy-Rewrite-1.
    b. In Action, select Action-Rewrite-1.
    c. In Undefined-Result Action, select Global undefined-result action.
    d. In Expression, type the following default syntax expression:

        "HTTP.REQ.HEADER(\"Name\").CONTAINS(\"Callout\").NOT"

    e. Click Create, and then click Close.
6. Click Apply Changes, and then click Close.

Access Control and Authentication

In high security zones, it is mandatory to externally authenticate the user before a resource is accessed by clients. On the NetScaler appliance, you can use HTTP callouts to externally authenticate the user by evaluating the credentials supplied. In this example, the assumption is that the client is sending the user name and password through HTTP headers in the request. However, the same information could be fetched from the URL or the HTTP body.

To implement this configuration, you must perform the following tasks:

1. Enable the responder feature on the NetScaler appliance.
2. Create an HTTP callout on the appliance and configure it with details about the external server and other required parameters.
3. Configure a responder policy to analyze the response, and then bind the policy globally.
4. Create a callout agent on the remote server.

Enabling Responder

The responder feature must be enabled before it is used on the NetScaler appliance.

To enable responder by using the configuration utility

1. Make sure that the responder license is installed.
2. In the navigation pane, right-click Responder, and then click Enable Responder feature.

Creating an HTTP Callout on the NetScaler Appliance

Create an HTTP callout, HTTP-Callout-3, with the parameter settings shown in the following table. For more information about creating an HTTP callout, see "Configuring an HTTP Callout."

Table 1. Parameters and Values for HTTP-Callout-3

Parameter	Value
Name	HTTP-Callout-3
Server to receive callout request	
IP Address	10.103.9.95
Port	80
Request to send to the server	
Method	GET
Host Expression	10.102.3.95
URL Stem Expression	“/cgi-bin/authenticate.pl”
Headers	
Name	Request
Value-expression	Callout Request
Parameters	
Name	Username
Value-expression	HTTP.REQ.HEADER("Username").VALUE(0)
Name	Password
Value-expression	HTTP.REQ.HEADER("Password").VALUE(0)
Server Response	
Return Type	TEXT
Expression to extract data from the response	HTTP.RES.BODY(100)

Creating a Responder Policy to Analyze the Response

Create a responder policy, Policy-Responder-3, that will check the response from the callout server and RESET the connection if the source IP address has been blacklisted. Create the policy with the parameters settings shown in the following table. While you can create a responder policy in the Policies subnode and then bind it globally by using the Responder Policy Manager, this demonstration uses the Responder Policy Manager to create the responder policy and bind the policy globally.

Table 1. Parameters and Values for Policy-Responder-3

Parameter	Value
Name	Policy-Responder-3
Action	RESET
Undefined-Result-Action	-Global undefined-result action-
Expression	"HTTP.REQ.HEADER(\"Request\").EQ(\"Callout Request\").NOT && SYS.HTTP_CALLOUT(HTTP-Callout-3).CONTAINS(\"Authentication Failed\")"

To create a responder policy and bind it globally by using the configuration utility

1. In the navigation pane, expand Responder.
2. In the details pane, under Policy Manager, click Responder Policy Manager.
3. In the Responder Policy Manger dialog box, click Override Global.
4. Click Insert Policy, and then, in the Policy Name column, click New Policy.
5. In the Create Responder Policy dialog box, do the following:
    a. In Name, type Policy-Responder-3.
    b. In Action, select RESET.
    c. In Undefined-Result Action , select Global undefined-result action.
    d. In the Expression text box, type:

        "HTTP.REQ.HEADER(\"Request\").EQ(\"Callout Request\").NOT && SYS.HTTP_CALLOUT(HTTP-Callo

    e. Click Create, and then click Close.
6. Click Apply Changes, and then click Close.

Creating an HTTP Callout Agent on the Remote Server

You now need to create an HTTP callout agent on the remote callout server. The HTTP callout agent receives callout requests from the NetScaler appliance and responds appropriately. The callout agent is a script that is different for each deployment and must be written with server specifications in mind, such as the type of database and the scripting language supported.

Following is sample callout agent pseudo-code that verifies whether the supplied user name and password are valid. The agent can be implemented in any programming language of your choice. The pseudo-code is to be used only as a guideline for developing the callout agent. You can build additional functionality into the program.

To verify the supplied user name and password by using pseudo-code

1. Accept the user name and password supplied in the request and format them appropriately.
2. Connect to the database that contains all the valid user names and passwords.
3. Check the supplied credentials against your database.
4. Format the response as required by the HTTP callout.
5. Send the response to the NetScaler appliance.

OWA-Based Spam Filtering

Spam filtering is the ability to dynamically block emails that are not from a known or trusted source or that have inappropriate content. Spam filtering requires an associated business logic that indicates that a particular kind of message is spam. When the NetScaler appliance processes Outlook Web Access (OWA) messages based on the HTTP protocol, HTTP callouts can be used to filter spam.

You can use HTTP callouts to extract any portion of the incoming message and check with an external callout server that has been configured with rules that are meant for determining whether a message is legitimate or spam. In case of spam email, for security reasons, the NetScaler appliance does not notify the sender that the email is marked as spam.

The following example conducts a very basic check for various listed keywords in the email subject. These checks can be more complex in a production environment.

To implement this configuration, you must perform the following tasks:

1. Enable the responder feature on the NetScaler appliance.
2. Create an HTTP callout on the NetScaler appliance and configure it with details about the external server and other required parameters.
3. Create a responder policy to analyze the response, and then bind the policy globally.
4. Create a callout agent on the remote server.

Enabling Responder

The responder feature must be enabled before it can be used on the NetScaler appliance.

To enable responder by using the configuration utility

1. Make sure that the responder license is installed.
2. In the navigation pane, right-click Responder, and then click Enable Responder feature.

Creating an HTTP Callout on the NetScaler Appliance

Create an HTTP callout, HTTP-Callout-4, with the parameter settings shown in the following table. For more information about creating an HTTP callout, see "Configuring an HTTP Callout."

Table 1. Parameters and Values for HTTP-Callout-4

Parameter	Value
Name	HTTP-Callout-4
Server to receive callout request	
IP Address	10.103.56.51
Port	80
Request to send to the server	
Method	POST
Host Expression	fffffff
URL Stem Expression	"/cgi-bin/Callout/spam_filter.pl"
Headers	
Name	Request
Value-expression	Callout Request
Parameters	
Name	Subject
Value-expression	("\"" + HTTP.REQ.BODY(1000).AFTER_STR("urn:schemas:httpmail:subject=").BEFORE_STR("\n").TO_LOWER + "\"")
Server Response	
Return Type	BOOL
Expression to extract data from the response	HTTP.RES.BODY(100) .CONTAINS(\"Matched\")

Creating a Responder Action

Create a responder action, Action-Responder-4. Create the action with the parameter settings shown in the following table.

Table 1. Parameters and Values for Action-Responder-4

Parameter	Value
Name	Action-Responder-4
Type	Respond with
Target	"\"HTTP/1.1 200 OK\r\nServer: Microsoft-IIS/6.0\r\nX-Powered-By: ASP.NET\r\nContent-Length: 0\r\nMS-WebStorage: 6.5.6944\r\nCache-Control: no-cache\r\n\r\n\""

To create a responder action by using the configuration utility

1. Navigate to Responder > Actions.
2. In the details pane, click Add.
3. In the Create Responder Action dialog box, in Name, type Action-Responder-4.
4. In Type, click Respond with.
5. In Target, type:

   "\"HTTP/1.1 200 OK\r\nServer: Microsoft-IIS/6.0\r\nX-Powered-By: ASP.NET\r\nContent-Length: 0\r\nMS-W
6. Click Create, and then click Close.

Creating a Responder Policy to Invoke the HTTP Callout

Create a responder policy, Policy-Responder-4, that will check the request body and, if the body contains the word "*subject*," invoke the HTTP callout to verify the email. Create the policy with the parameter settings shown in the following table. While you can create a responder policy in the Policies subnode and then bind it globally by using the Responder Policy Manager, this demonstration uses the Responder Policy Manager to create the responder policy and bind it globally.

Table 1. Parameters and Values for Policy-Responder-4

Parameter	Value
Name	Policy-Responder-4
Action	Action-Responder-4
Undefined-Result-Action	-Global undefined-result action-
Expression	"HTTP.REQ.BODY(1000).CONTAINS(\"urn:schemas:httpmail:subject\") && SYS.HTTP_CALLOUT(HTTP-Callout-4)"

To create a responder policy by using the configuration utility

1. In the navigation pane, expand Responder.
2. In the details pane, under Policy Manager, click Responder policy manager.
3. In the Responder Policy Manger dialog box, click Override Global.
4. Click Insert Policy, and then, in the Policy Name column, click New Policy.
5. In the Create Responder Policy dialog box, do the following:
    a. In Name, type Policy-Responder-4.
    b. In Action, click Action-Responder-4.
    c. In Undefined-Result Action, click Global undefined-result action.
    d. In the Expression text box, type:

        "HTTP.REQ.BODY(1000).CONTAINS(\"urn:schemas:httpmail:subject\") && SYS.HTTP_CALLOUT(HTTP-C

    e. Click Create, and then click Close.
6. Click Apply Changes, and then click Close.

Creating an HTTP Callout Agent on the Remote Server

You will now need to create an HTTP callout agent on the remote callout server. The HTTP callout agent receives callout requests from the NetScaler appliance and responds accordingly. The callout agent is a script that is different for each deployment and must be written with server specifications in mind, such as the type of database and the scripting language supported.

The following pseudo-code provides instructions for creating a callout agent that checks a list of words that are generally understood to indicate spam mails. The agent can be implemented in any programming language of your choice. The pseudo-code is to be used only as a guideline for developing the callout agent. You can build additional functionality into the program.

To identify spam email by using pseudo-code

1. Accept the email subject provided by the NetScaler appliance.
2. Connect to the database that contains all the terms against which the email subject is checked.
3. Check the words in the email subject against the spam word list.
4. Format the response as required by the HTTP callout.
5. Send the response to the NetScaler appliance.

Dynamic Content Switching

This use case provides dynamic content switching by using an HTTP callout to get the name of the load balancing virtual server to which the request is forwarded.

1. Add a content switching virtual server.

   > add cs vserver cs_vserver1 HTTP 10.102.29.196 80

2. Create an HTTP callout.

   > add policy httpCallout http_callout1

3. Configure the HTTP callout to respond with the name of the load balancing virtual server from a request that contains the client IP address in the HTTP header "X-CLIENT-IP".

   > set policy httpCallout http_callout1 -IPAddress 10.217.14.23 -port 80 -returnType TEXT -hostExpr "\"ww

4. Configure the content switching action to retrieve the callout response.

   > add cs action cs_action1 -targetVserverExpr 'SYS.HTTP_CALLOUT(http_callout1)'

   Note: You must bind a load balancing virtual server to the content switching virtual server to account for:

   - The non-availability of the load balancing virtual server that the callout resolves to.
   - A UNDEF condition that results from the execution of the callout.

   > bind cs vserver cs_vserver1 -lbvserver default_lbvip

5. Configure the content switching policy.

   > add cs policy cs_policy1 -rule true -action cs_action1

6. Binding the content switching policy to the content switching virtual server.

   > bind cs vserver cs_vserver1 -policyName cs_policy1 -priority 10

Pattern Sets and Data Sets

Policy expressions for string matching operations on a large set of string patterns tend to become long and complex. Resources consumed by the evaluation of such complex expressions are significant in terms of processing cycles, memory, and configuration size. You can create simpler, less resource-intensive expressions by using pattern matching.

Depending on the type of patterns that you want to match, you can use one of the following features to implement pattern matching:

- A *pattern set* is an array of indexed patterns used for string matching during default syntax policy evaluation. Example of a pattern set: imagetypes {svg, bmp, png, gif, tiff, jpg}.
- A *data set* is a specialized form of pattern set. It is an array of patterns of types number (integer), IPv4 address, or IPv6 address.

In many cases, you can use either pattern sets or data sets. However, in cases where you want specific matches for numerical data or IPv4 and IPv6 addresses, you must use data sets.

Note: Pattern sets and data sets can be used only in default syntax policies.

To use pattern sets or data sets, first create the pattern set or data set and bind patterns to it. Then, when you configure a policy for comparing a string in a packet, use an appropriate operator and pass the name of the pattern set or data set as an argument.

How String Matching works with Pattern Sets and Data Sets

A pattern set or data set contains a set of patterns, and each pattern is assigned a unique index. When a policy is applied to a packet, an expression identifies a string to be evaluated, and the operator compares the string to the patterns defined in the pattern set or data set until a match is found or all patterns have been compared. Then, depending on its function, the operator returns either a boolean value that indicates whether or not a matching pattern was found or the index of the pattern that matches the string.

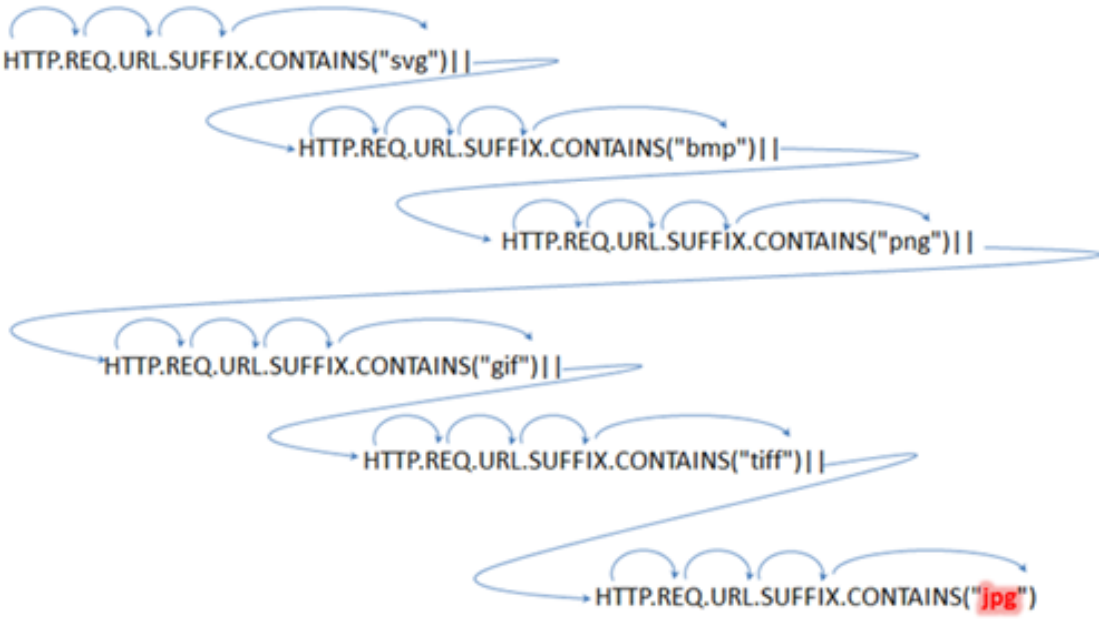
Note: This topic explains the working of a pattern set. Data sets work the same way. The only difference between pattern sets and data sets is the type of patterns defined in the set.

Consider the following use case to understand how patterns can be used for string matching.

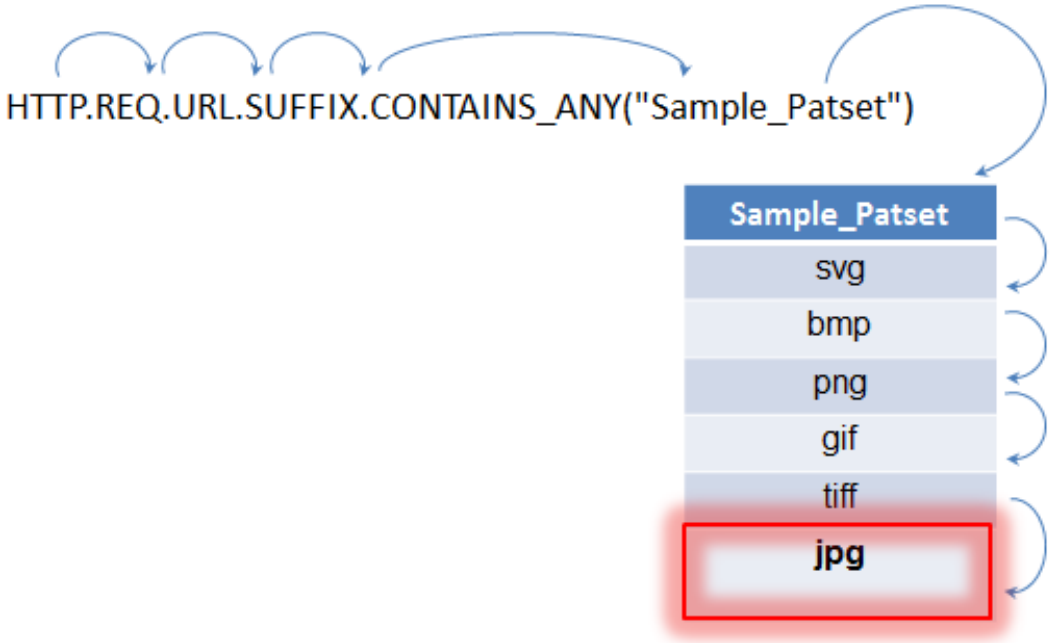
You want to determine whether the URL suffix (target text) contains any of the image file extensions. Without using pattern sets, you would have to define a complex expression, as follows:

```
HTTP.REQ.URL.SUFFIX.CONTAINS("svg") || HTTP.REQ.URL.SUFFIX.CONTAINS("bmp") || HTTP.REQ.URL.SUFFIX
HTTP.REQ.URL.SUFFIX.CONTAINS("gif") || HTTP.REQ.URL.SUFFIX.CONTAINS("tiff") || HTTP.REQ.URL.SUFFIX.
```

If the URL has a suffix of "jpg," with the above compound expression, the NetScaler appliance has to iterate through the entire compound expression sequentially, from one sub expression to the next, to determine that the request refers to a jpg image. The following figure shows the steps in the process.



When a compound expression includes hundreds of sub expressions, the above process is resource intensive. A better alternative is an expression that invokes a pattern set, as shown in the following figure.



During policy evaluation as shown above, the operator (CONTAINS_ANY) compares the string identified in the request with the patterns defined in the pattern set until a match is found. With the `Sample_Patset` expression, the multiple iterations through six sub expressions are reduced to just one.

By eliminating the need to configure compound expressions that perform string matching with multiple OR operations, pattern sets or data sets simplify configuration and accelerate processing of requests and responses.

Configuring a Pattern Set

To configure a pattern set, you must specify the strings that are to serve as patterns. You can manually assign a unique index value to each of these patterns, or you can allow the index values to be assigned automatically.

Note: Pattern sets are case sensitive (unless you specify the expression to ignore case). Therefore, the string pattern "product1," for example, is not the same as the string pattern "Product1."

Points to remember about index values

- You cannot bind the same index value to more than one pattern.
- An automatically assigned index value is one number larger than the highest index value of the existing patterns within the pattern set. For example, if the highest index value of existing patterns in a pattern set is 104, the next automatically assigned index value will be 105.
- If you do not specify an index for the first pattern, index value 1 is automatically assigned to that pattern.
- Index values are not regenerated automatically if one or more patterns are deleted or modified. For example, if the set contains five patterns, with indexes from 1 through 5, and if the pattern with an index of 3 is deleted, the other index values in the pattern set are not automatically regenerated to produce values from 1 through 4.
- The maximum index value that can be assigned to a pattern is 4294967290. If that value is already assigned to a pattern in the set, you must manually assign index values to any newly added patterns. An unused index value that is lower than a currently used value cannot be assigned automatically.

To configure a pattern set by using the command line interface

At the command prompt, do the following:

1. Create a pattern set.

   add policy patset <name>

   Example:

   > add policy patset samplepatset

2. Bind patterns to the pattern set.

   bind policy patset <name> <string> [-index <positive_integer>]

Example:

> bind policy patset samplepatset product1 -index 1

Note: Repeat this step for all the patterns you want to bind to the pattern set.

3. Verify the configuration.

   show policy patset <name>

To configure a pattern set by using the configuration utility

1. Navigate to AppExpert > Pattern Sets.
2. In the details pane, click Add to open the Create Pattern Set dialog box.
3. Specify a name for the pattern set in the Name text box.
4. Under Specify Pattern, type the first pattern and, optionally, specify values for the following parameters:
   - Treat back slash as escape character—Select this check box to specify that any backslash characters that you might include in the pattern are to be treated as escape characters.
   - Index—A user assigned index value, from 1 through 4294967290.
5. Verify that you have entered the correct characters, and then click Add.
6. Repeat steps 4 and 5 to add additional patterns, and then click Create.

Configuring a Data Set

To configure a data set, you must specify the strings that are to serve as patterns, and assign a type (number, IPv4 address, or IPv6 address) to each pattern. You can manually assign a unique index value to each of these patterns, or you can allow the index values to be assigned automatically.

Note: Data sets are case sensitive (unless you specify the expression to ignore case). Therefore, the string pattern "product1," for example, is not the same as the string pattern "Product1."

The rules applied for index values of data sets are the same as those applied for pattern sets. For information about index values, see "Configuring a Pattern Set."

To configure a data set by using the command line interface

At the command prompt, do the following:

1. Create a data set.

   add policy dataset <name> <type>

   Example:

   > add policy dataset sampledataset ipv4

2. Bind patterns to the data set.

   bind policy dataset <name> <value> [-index <positive_integer>]

   Example:

   > bind policy dataset sampledataset 10.102.29.1 -index 1

   Note: Repeat this step for all the patterns you want to bind to the data set.

3. Verify the configuration.

   show policy dataset <name>

To configure a data set by using the configuration utility

Navigate to AppExpert > Data Sets, click Add and specify the relevant details.

Using Pattern Sets and Data Sets

Default syntax policy expressions that take pattern sets or data sets as an argument can be used to perform string matching operations.

The usage is as follows:

<text>.<operator>("<name>")

where,

- `<text>` is the expression that identifies a string in a packet. Example: `HTTP.REQ.HEADER("Host")`.
- `<operator>` is one of the operators described in the following table.

  Table 1. Operators for pattern sets and data sets

Operator	Description
`<text>.CONTAINS_ANY(<name>)`	Returns true if the target text contains one or more of the patterns defined in the specified pattern set or data set.
`<text>.SUBSTR_ANY(<name>)`	Returns the first string that matches any pattern defined in the specified pattern set or data set.
`<text>.BEFORE_STR_ANY(<name>)`	Returns the text that is present before the first occurrence of any of the patterns defined in the specified pattern set or data set.
`<text>.AFTER_STR_ANY(<name>)`	Returns the text that is present after the first occurrence of any of the patterns defined in the specified pattern set or data set.
`<text>.EQUALS_ANY (<name>)`	Returns true if the target text exactly matches any of the patterns defined in the specified pattern set or data set.
`<text>.ENDSWITH_ANY(<name>)`	Returns true if the target text ends with any of the patterns that are defined in the specified pattern set or data set.
`<text>.STARTSWITH_ANY(<name>)`	Returns true if the target text starts with any of the patterns that are defined in the specified pattern set or data set.

`<text>.STARTSWITH_INDEX(<name>)`	Evaluates whether the target text starts with any of the patterns that are defined in the specified pattern set or data set. If a match is found, the index of the matching pattern is returned. Otherwise, 0 is returned.
`<text>.ENDSWITH_INDEX(<name>)`	Evaluates whether the target text ends with any of the patterns that are defined in the specified pattern set or data set. If a match is found, the index of the matching pattern is returned. Otherwise, 0 is returned.
`<text>.CONTAINS_INDEX(<name>)`	Evaluates whether the target text contains any of the patterns that are defined in the specified pattern set or data set. If a match is found, the index of the matching pattern is returned. Otherwise, 0 is returned.
`<text>.EQUALS_INDEX(<name>)`	Evaluates whether the target text exactly matches any of the patterns that are defined in the specified pattern set or data set. If an exact match is found, the index of the pattern is returned. Otherwise, 0 is returned.

- `<name>` is the name of the pattern set or data set

For sample usage, see "Sample Usage."

Sample Usage

To understand the usage of pattern sets in expressions, consider the example of a pattern set named "imagetypes."

Table 1. Pattern set "imagetypes"

Patterns	Index value
svg	1
bmp	2
png	3
gif	4
tiff	5
jpg	6

Example 1: Determine whether the suffix of an HTTP request is one of the file extensions defined in the "imagetypes" pattern set.

- **Expression.** `HTTP.REQ.URL.SUFFIX.EQUALS_ANY("imagetypes")`
- **Sample URL.** http://www.example.com/homepageicon.jpg
- **Result.** TRUE

Example 2: Determine whether the suffix of an HTTP request is one of the file extensions defined in the "imagetypes" pattern set, and return the index of that pattern.

- **Expression.** `HTTP.REQ.URL.SUFFIX.EQUALS_INDEX("imagetypes")`
- **Sample URL.** http://www.example.com/mylogo.gif
- **Result.** 4 (The index value of the pattern "gif".)

Example 3: Use the index value of a pattern to determine whether the URL suffix is within a specified index-value range.

- **Expression.** `HTTP.REQ.URL.SUFFIX.EQUALS_INDEX("imagetypes").GE(3) && HTTP.REQ.URL.SUFFIX.EQUALS_INDEX("imagetypes").LE(5)`
- **Sample URL.** http://www.example.com/mylogo.gif
- **Result.** TRUE (The index value of gif file types is 4.)

Example 4: Implement one set of policies for file extensions bmp, jpg, and png, and a different set of policies for gif, tiff, and svg files.

An expression that returns the index of a matched pattern can be used to define traffic subsets for a web application. The following two expressions could be used in content switching policies for a content switching virtual server:

- `HTTP.REQ.URL.SUFFIX.EQUALS_INDEX("imagetypes").LE(3)`
- `HTTP.REQ.URL.SUFFIX.EQUALS_INDEX("imagetypes").GE(4)`

Policies and Expressions

The following topics provide the conceptual and reference information that you require for configuring advanced policies on the Citrix® NetScaler® appliance.

Introduction to Policies and Expressions	Describes the purpose of expressions, policies, and actions, and how different NetScaler applications make use of them.
Configuring Advanced Policies	Describes the structure of advanced policies and how to configure them individually and as policy banks.
Configuring Advanced Expressions: Getting Started	Describes expression syntax and semantics, and briefly introduces how to configure expressions and policies.
Advanced Expressions: Evaluating Text	Describes expressions that you configure when you want to operate on text (for example, the body of an HTTP POST request or the contents of a user certificate).
Advanced Expressions: Working with Dates, Times, and Numbers	Describes expressions that you configure when you want to operate on any type of numeric data (for example, the length of a URL, a client's IP address, or the date and time that an HTTP request was sent).
Advanced Expressions: Parsing HTTP, TCP, and UDP Data	Describes expressions for parsing IP and IPv6 addresses, MAC addresses, and data that is specific to HTTP and TCP traffic.
Advanced Expressions: Parsing SSL Certificates	Describes how to configure expressions for SSL traffic and client certificates, for example, how to retrieve the expiration date of a certificate or the certificate issuer.
Advanced Expressions: IP and MAC Addresses, Throughput, VLAN IDs	Describes expressions that you can use to work with any other client- or server-related data not discussed in other chapters.
Typecasting Data	Describes expressions for transforming data of one type to another.
Regular Expressions	Describes how to pass regular expressions as arguments to operators in advanced expressions.
Configuring Classic Policies and Expressions	Provides details on how to configure the simpler policies and expressions known as classic policies and classic expressions.

Expressions Reference	A reference for classic and advanced expression arguments.
Summary Examples of Advanced Expressions and Policies	Examples of classic and advanced expressions and policies, in both quick reference and tutorial format, that you can customize for your own use.
Tutorial Examples of Advanced Policies for Rewrite	Examples of advanced policies for use in the Rewrite feature.
Tutorial Examples of Classic Policies	Examples of classic policies for NetScaler features such as application firewall and SSL.
Migration of Apache mod_rewrite Rules to Advanced Policies	Examples of functions that were written using the Apache HTTP Server mod_rewrite engine, with examples of these functions after translation into Rewrite and Responder policies on the NetScaler.

Introduction to Policies and Expressions

For many NetScaler features, policies control how a feature evaluates data, which ultimately determines what the feature does with the data. A policy uses a logical expression, also called a rule, to evaluate requests, responses, or other data, and applies one or more actions determined by the outcome of the evaluation. Alternatively, a policy can apply a profile, which defines a complex action.

Some NetScaler features use default syntax policies, which provide greater capabilities than do the older, classic, policies. If you migrated to a newer release of the NetScaler software and have configured classic policies for features that now use default syntax policies, you might have to manually migrate policies to the default syntax.

Classic and Default Syntax Policies

Classic policies evaluate basic characteristics of traffic and other data. For example, classic policies can identify whether an HTTP request or response contains a particular type of header or URL.

Default syntax policies can perform the same type of evaluations as classic policies. In addition, default syntax policies enable you to analyze more data (for example, the body of an HTTP request) and to configure more operations in the policy rule (for example, transforming data in the body of a request into an HTTP header).

In addition to assigning a policy an action or profile, you bind the policy to a particular point in the processing associated with the NetScaler features. The bind point is one factor that determines when the policy will be evaluated.

Benefits of Using Default Syntax Policies

Default syntax policies use a powerful expression language that is built on a class-object model, and they offer several options that enhance your ability to configure the behavior of various NetScaler features. With default syntax policies, you can do the following:

- Perform fine-grained analyses of network traffic from layers 2 through 7.
- Evaluate any part of the header or body of an HTTP or HTTPS request or response.
- Bind policies to the multiple bind points that the default syntax policy infrastructure supports at the default, override, and virtual server levels.
- Use goto expressions to transfer control to other policies and bind points, as determined by the result of expression evaluation.
- Use special tools such as pattern sets, policy labels, rate limit identifiers, and HTTP callouts, which enable you to configure policies effectively for complex use cases.

Additionally, the configuration utility extends robust graphical user interface support for default syntax policies and expressions and enables users who have limited knowledge of networking protocols to configure policies quickly and easily. The configuration utility also includes a policy evaluation feature for default syntax policies. You can use this feature to evaluate a default syntax policy and test its behavior before you commit it, thus reducing the risk of configuration errors.

Basic Components of a Classic or Default Syntax Policy

Following are a few characteristics of both classic and default syntax policies:

Name.

Each policy has a unique name.

Rule.

The rule is a logical expression that enables the NetScaler feature to evaluate a piece of traffic or another object.

For example, a rule can enable the NetScaler to determine whether an HTTP request originated from a particular IP address, or whether a Cache-Control header in an HTTP request has the value “No-Cache.”

Default syntax policies can use all of the expressions that are available in a classic policy, with the exception of classic expressions for the SSL VPN client. In addition, default syntax policies enable you to configure more complex expressions.

Bindings.

To ensure that the NetScaler can invoke a policy when it is needed, you associate the policy, or bind it, to one or more bind points.

You can bind a policy globally or to a virtual server. For more information, see "About Policy Bindings."

An associated action.

An action is a separate entity from a policy. Policy evaluation ultimately results in the NetScaler performing an action.

For example, a policy in the integrated cache can identify HTTP requests for .gif or .jpeg files. An action that you associate with this policy determines that the responses to these types of requests are served from the cache.

For some features, you configure actions as part of a more complex set of instructions known as a profile. For more information, see "Order of Evaluation Based on Traffic Flow."

How Different NetScaler Features Use Policies

The NetScaler supports a variety of features that rely on policies for operation. The following table summarizes how the NetScaler features use policies.

Table 1. NetScaler Feature, Policy Type, and Policy Usage

Feature Name	Policy Type	How You Use Policies in the Feature
System	Classic	For the Authentication function, policies contain authentication schemes for different authentication methods. For example, you can configure LDAP and certificate-based authentication schemes. You also configure policies in the Auditing function.
DNS	Default	To determine how to perform DNS resolution for requests.

SSL	Classic and Default	To determine when to apply an encryption function and add certificate information to clear text. To provide end-to-end security, after a message is decrypted, the SSL feature re-encrypts clear text and uses SSL to communicate with Web servers.
Compression	Classic and Default	To determine what type of traffic is compressed.
Integrated Caching	Default	To determine whether HTTP responses are cacheable.
Responder	Default	To configure the behavior of the Responder function.
Protection Features	Classic	To configure the behavior of the Filter, SureConnect, and Priority Queuing functions.
Content Switching	Classic and Default	To determine what server or group of servers is responsible for serving responses, based on characteristics of an incoming request. Request characteristics include device type, language, cookies, HTTP method, content type, and associated cache server.

AAA - Traffic Management	Classic Exceptions: · Traffic policies support only default syntax policies · Authorization policies support both classic and default syntax policies.	To check for client-side security before users log in and establish a session. Traffic policies, which determine whether single sign-on (SSO) is required, use only the default syntax. Authorization policies authorize users and groups that access intranet resources through the appliance.
Cache Redirection	Classic	To determine whether responses are served from a cache or from an origin server.

Rewrite	Default	To identify HTTP data that you want to modify before serving. The policies provide rules for modifying the data. For example, you can modify HTTP data to redirect a request to a new home page, or a new server, or a selected server based on the address of the incoming request, or you can modify the data to mask server information in a response for security purposes. The URL Transformer function identifies URLs in HTTP transactions and text files for the purpose of evaluating whether a URL should be transformed.
Application Firewall	Classic and Default	To identify characteristics of traffic and data that should or should not be admitted through the firewall.
Access Gateway, Clientless Access function	Default	To define rewrite rules for general Web access using the Access Gateway.
Access Gateway	Classic	To determine how the Access Gateway performs authentication, authorization, auditing, and other functions.

About Actions and Profiles

Policies do not themselves take action on data. Policies provide read-only logic for evaluating traffic. To enable a feature to perform an operation based on a policy evaluation, you configure actions or profiles and associate them with policies.

Note: Actions and profiles are specific to particular features. For information about assigning actions and profiles to features, see the documentation for the individual features.

About Actions

Actions are steps that the NetScaler takes, depending on the evaluation of the expression in the policy. For example, if an expression in a policy matches a particular source IP address in a request, the action that is associated with this policy determines whether the connection is permitted.

The types of actions that the NetScaler can take are feature specific. For example, in Rewrite, actions can replace text in a request, change the destination URL for a request, and so on. In Integrated Caching, actions determine whether HTTP responses are served from the cache or an origin server.

In some NetScaler features actions are predefined, and in others they are configurable. In some cases, (for example, Rewrite), you configure the actions using the same types of expressions that you use to configure the associated policy rule.

About Profiles

Some NetScaler features enable you to associate profiles, or both actions and profiles, with a policy. A profile is a collection of settings that enable the feature to perform a complex function. For example, in the application firewall, a profile for XML data can perform multiple screening operations, such as examining the data for illegal XML syntax or evidence of SQL injection.

Use of Actions and Profiles in Particular Features

The following table summarizes the use of actions and profiles in different NetScaler features. The table is not exhaustive. For more information about specific uses of actions and profiles for a feature, see the documentation for the feature.

Table 1. Use of Actions and Profiles in Different NetScaler Features

ure	Use of an Action	Use of a Profile

cation all	Synonymous with a profile	All application firewall features use profiles to defin behaviors, including pattern-based learning. You add these profiles to policies.
ss way	The following features of the Access Gateway use actions: · **Pre-Authentication.** Uses Allow and Deny actions. You add these actions to a profile. · **Authorization.** Uses Allow and Deny actions. You add these actions to a policy. · **TCP Compression.** Uses various actions. You add these actions to a policy.	The following features use a profile: · Pre-Authentication · Session · Traffic · Clientless Access After configuring the profiles, you add them to polic
ite	You configure URL rewrite actions and add them to a policy.	Not used.
rated ing	You configure caching and invalidation actions within a policy	Not used.
Traffic gement	You select an authentication type, set an authorization action of ALLOW or DENY, or set auditing to SYSLOG or NSLOG.	You can configure session profiles with a default tim authorization action.
ction ures	You configure actions within policies for the following functions: · Filter · Compression · Responder · SureConnect	Not used.
	You configure actions within SSL policies	Not used.
m	The action is implied. For the Authentication function, it is either Allow or Deny. For Auditing, it is Auditing On or Auditing Off.	Not used.
	The action is implied. It is either Drop Packets or the location of a DNS server.	Not used.
ffload	The action is implied. It is based on a policy that you associate with an SSL virtual server or a service.	Not used.
pression	Determine the type of compression to apply to the data	Not used.
ent hing	The action is implied. If a request matches the policy, the request is directed to the virtual server associated with the policy.	Not used.
e ection	The action is implied. If a request matches the policy, the request is directed to the origin server.	Not used.

About Policy Bindings

A policy is associated with, or bound to, an entity that enables the policy to be invoked. For example, you can bind a policy to request-time evaluation that applies to all virtual servers. A collection of policies that are bound to a particular bind point constitutes a policy bank.

Following is an overview of different types of bind points for a policy:

Request time global.

A policy can be available to all components in a feature at request time.

Response time global.

A policy can be available to all components in a feature at response time.

Request time, virtual server-specific.

A policy can be bound to request-time processing for a particular virtual server. For example, you can bind a request-time policy to a cache redirection virtual server to ensure that particular requests are forwarded to a load balancing virtual server for the cache, and other requests are sent to a load balancing virtual server for the origin.

Response time, virtual server-specific.

A policy can also be bound to response-time processing for a particular virtual server.

User-defined policy label.

For default syntax policies, you can configure custom groupings of policies (policy banks) by defining a policy label and collecting a set of related policies under the policy label.

Other bind points.

The availability of additional bind points depends on type of policy (classic or default syntax), and specifics of the relevant NetScaler feature. For example, classic policies that you configure for the Access Gateway have user and group bind points.

For additional information about default syntax policy bindings, see "Binding Policies That Use the Default Syntax" and Configuring a Policy Bank for a Virtual Server. For additional information about classic policy bindings, see "Configuring a Classic Policy."

About Evaluation Order of Policies

For classic policies, policy groups and policies within a group are evaluated in a particular order, depending on the following:

- The bind point for the policy, for example, whether the policy is bound to request-time processing for a virtual server or global response-time processing. For example, at request time, the NetScaler evaluates all request-time classic policies before evaluating any virtual server-specific policies.

- The priority level for the policy. For each point in the evaluation process, a priority level that is assigned to a policy determines the order of evaluation relative to other policies that share the same bind point. For example, when the NetScaler evaluates a bank of request-time, virtual server-specific policies, it starts with the policy that is assigned to the lowest priority value. In classic policies, priority levels must be unique across all bind points.

For default syntax policies, as with classic policies, the NetScaler selects a grouping, or bank, of policies at a particular point in overall processing. Following is the order of evaluation of the basic groupings, or banks, of default syntax policies:

1. Request-time global override
2. Request-time, virtual server-specific (one bind point per virtual server)
3. Request-time global default
4. Response-time global override
5. Response-time virtual server-specific
6. Response-time global default

However, within any of the preceding banks of policies, the order of evaluation is more flexible than in classic policies. Within a policy bank, you can point to the next policy to be evaluated regardless of the priority level, and you can invoke policy banks that belong to other bind points and user-defined policy banks.

Order of Evaluation Based on Traffic Flow

As traffic flows through the NetScaler and is processed by various features, each feature performs policy evaluation. Whenever a policy matches the traffic, the NetScaler stores the action and continues processing until the data is about to leave the NetScaler. At that point, the NetScaler typically applies all matching actions. Integrated Caching, which only applies a final Cache or NoCache action, is an exception.

Some policies affect the outcome of other policies. Following are examples:

- If a response is served from the integrated cache, some other NetScaler features do not process the response or the request that initiated it.
- If the Content Filtering feature prevents a response from being served, no subsequent features evaluate the response.

If the application firewall rejects an incoming request, no other features can process it.

Classic and Default Syntax Expressions

One of the most fundamental components of a policy is its rule. A policy rule is a logical expression that enables the policy to analyze traffic. Most of the policy's functionality is derived from its expression.

An expression matches characteristics of traffic or other data with one or more parameters and values. For example, an expression can enable the NetScaler to accomplish the following:

- Determine whether a request contains a certificate.
- Determine the IP address of a client that sent a TCP request.
- Identify the data that an HTTP request contains (for example, a popular spreadsheet or word processing application).
- Calculate the length of an HTTP request.

About Classic Expressions

Classic expressions enable you to evaluate basic characteristics of data. They have a structured syntax that performs string matching and other operations.

Following are a few simple examples of classic expressions:

- An HTTP response contains a particular type of Cache Control header.

```
res.http.header Cache-Control contains public
```

- An HTTP response contains image data.

```
res.http.header Content-Type contains image/
```

- An SSL request contains a certificate.

```
req.ssl.client.cert exists
```

About Default Syntax Expressions

Any feature that uses default syntax policies also uses default syntax expressions. For information about which features use default syntax policies, see the table "NetScaler Feature, Policy Type, and Policy Usage."

Default syntax expressions have a few other uses. In addition to configuring default syntax expressions in policy rules, you configure default syntax expressions in the following situations:

Integrated Caching:

You use default syntax expressions to configure a selector for a content group in the integrated cache.

Load Balancing:

You use default syntax expressions to configure token extraction for a load balancing virtual server that uses the TOKEN method for load balancing.

Rewrite:

You use default syntax expressions to configure rewrite actions.

Rate-based policies:

You use default syntax expressions to configure limit selectors when configuring a policy to control the rate of traffic to various servers.

Following are a few simple examples of default syntax expressions:

- An HTTP request URL contains no more than 500 characters.

```
http.req.url.length <= 500
```

- An HTTP request contains a cookie that has fewer than 500 characters.

```
http.req.cookie.length < 500
```

- An HTTP request URL contains a particular text string.

```
http.req.url.contains(".html")
```

Converting Classic Expressions to the Newer Default Expression Syntax

You can convert a classic expression to the default expression syntax by using the nspepi conversion tool. You can also use the tool to convert all the classic expressions in the NetScaler configuration to the default syntax (with the exception of NetScaler entities that currently support only classic expressions).

The conversion tool does not convert policies configured for the following features, because the features currently support only classic policies:

- Authentication, Pre-authentication
- SSL
- Cache redirection
- VPN (session, traffic, and tunnel traffic)
- Content filtering (The responder feature not only provides you with functionality that is equivalent to that provided by the content filtering feature but also surpasses the content filtering feature in the use cases that it supports. Additionally, responder supports the more powerful default syntax for policy expressions.)

The following NetScaler features support both classic and default syntax expressions and, therefore, support the conversion of classic expressions to default syntax expressions:

- Application firewall policies
- Authorization policies
- Named expressions
- Compression policies
- Content switching policies
- User-defined, rule-based tokens/persistency (the –rule parameter value that is specified for a load balancing virtual server)

About the Conversion Process

When parsing a NetScaler configuration file, the conversion tool performs the following actions:

1. In commands that create classic named expressions, the conversion tool replaces the names of the classic expressions with default syntax expressions.

2. In commands that support only the classic syntax, if classic named expressions are used, the conversion tool replaces the names of the classic expressions with the actual classic expressions they represent. This action ensures that the names of expressions in classic-only features do not reference the default syntax expressions created from Step 1.

3. In commands associated with entities that support both the classic syntax and the default syntax, the conversion tool replaces all classic expressions in commands with default syntax expressions.

Example

Consider the following sample configuration commands:

```
add policy expression ne_c1 "METHOD == GET"
add policy expression ne_c2 "ne_c1 || URL == /*.htm "
add filter policy pol1 -rule "ne_c2" -reqAction YES
add cmp policy pol2 -rule "REQ.HTTP.HEADER Accept CONTAINS \'text/html\'" -resAction COMPRESS
add cmp policy pol3 -rule "ne_c1 || ne_c2" -resAction GZIP
```

In the commands that create the classic named expressions `ne_c1` and `ne_c2`, the tool replaces the names of the expressions with actual default syntax expressions. This action, which corresponds to Step 1 described earlier, results in the following commands:

```
add policy expression ne_c1 "HTTP.REQ.METHOD.EQ(\"GET\")"

add policy expression ne_c2 "HTTP.REQ.URL.SUFFIX.EQ(\"htm\")"
```

The filter policy command supports only the classic syntax. Therefore, the conversion tool replaces the classic named expression `ne_c1` with the actual classic expression it represents. Note that the tool replaces `ne_c1` in the expression for `ne_c2`, and then replaces `ne_c2` in the filter policy with the classic expression. This action, which corresponds to Step 2 described earlier, results in the following command:

```
add filter policy pol1 -rule "METHOD == GET || URL == /*.htm"
-reqAction YES
```

The compression feature supports both classic and default syntax expressions. Therefore, in the command that creates the compression policy `pol2`, the conversion tool replaces the expression with a default syntax expression. This action, which corresponds to Step 3 described earlier, results in the following command:

```
add cmp policy pol2 -rule
"HTTP.REQ.HEADER(\"Accept\").AFTER_STR(\"text/html\").LENGTH.GT(0)"
-resAction COMPRESS
```

The command that creates the compression policy `pol3` is unaffected by the conversion process because, after the conversion process is complete, `ne_c1` and `ne_c2` reference the default syntax expressions that result from Step 1.

Client security messages are not supported in the newer default policy format and, therefore, are lost. The `SYS.EVAL_CLASSIC_EXPR` function is replaced with a default policy expression. The following entities support the `SYS.EVAL_CLASSIC_EXPR` function:

- DNS policies
- Rate limit selectors
- Cache selectors
- Cache policies
- Content switching policies
- Rewrite policies
- URL transformation policies
- Responder policies
- Application firewall policies
- Authorization policies
- Compression policies
- CVPN access policies

After performing the conversion, the tool saves the changes in a new configuration file. The new configuration file is created in the directory in which the input file exists. The name of the new configuration file is the same as the name of the input configuration file except for the string `new_` used as a prefix. Conversion warnings are reported in a warning line at the end of the screen output. Additionally, a warning file is created in the directory in which the input configuration file resides. For more information about the warning file and the types of warnings that are reported, see "Conversion Warnings."

Converting Expressions

You can use the `nspepi` tool to convert a single classic expression to the default syntax. The `nspepi` tool must be run from the shell prompt on the NetScaler appliance.

To convert a classic expression to the default syntax by using the command line interface

At the shell prompt, type:

`nspepi -e` `"<classic expression>"`

Example

```
root@NS# nspepi -e "REQ.HTTP.URL == /*.htm"
 "HTTP.REQ.URL.REGEX_MATCH(re#/(.*)\.htm#)"
```

Parameters for converting a classic expression to a default syntax expression

e

Specifies that the input is a single classic expression. This option is mutually exclusive with the `-f` option, which specifies that the input is a NetScaler configuration file.

classic expression

The classic expression that you want to convert to the default syntax.

Converting a NetScaler Configuration File

You can use the `nspepi` tool to convert all the classic expressions in a NetScaler configuration file to the default syntax (except for those commands that do not support the default syntax). The `nspepi` tool must be run from the shell prompt on the NetScaler appliance.

To convert all the classic expressions in a NetScaler configuration file to the default syntax by using the command line interface

At the shell prompt, type:

`nspepi -f` `"<ns config file>" -v`

Example

```
root@NS# nspepi -f ns.conf
OUTPUT: New configuration file created: new_ns.conf
OUTPUT: New warning file created: warn_ns.conf
WARNINGS: Total number of warnings due to bind commands: 18
WARNINGS: Line numbers which has bind command issues: 305, 306, 706, 707, 708, 709, 710, 711, 712, 713,
714, 715, 767, 768, 774, 775, 776, 777
root@NS#
```

Parameters for converting the classic expressions in a NetScaler configuration file to the default syntax

f

Specifies that the input is a NetScaler configuration file. This option is mutually exclusive with the `-e` option, which specifies that the input is a single classic expression.

ns config file

The full path to the NetScaler configuration file. If the NetScaler configuration file is in the present working directory, the name of the NetScaler configuration file is sufficient.

v

The verbose option. If this option is specified, the output of the conversion tool is printed to the screen. The configuration file and the warning file are created even if this option is used.

Conversion Warnings

When classic expressions that are included in CLI commands are upgraded to the default syntax, the number of characters in the expression might exceed the 1499-character limit. The commands that include expressions longer than 1499 characters fail when the configuration is being applied. You must manually update these commands.

In addition, multiple classic policies can be bound to a given bind point with priority 0 or with equal priority, but the default syntax policy infrastructure does not support a priority value of 0 or policies with the same priority at a given bind point. These commands fail when the configuration is being applied. The commands must be updated manually with the correct priority values.

The line numbers of lines that threw a warning during conversion are listed at the end of the output in a warning line. In addition, a warning file is created in the same directory as the one in which the old and new configuration files reside. The name of the warning file is the same as the name of the input configuration file except that the string `warn_` is added as a prefix.

About Migration from Classic to Default Syntax Policies and Expressions

The NetScaler supports either classic or default syntax policies within a feature. You cannot have both types in the same feature. Over the past few releases, some NetScaler features have migrated from using classic policies and expressions to default syntax policies and expressions. If a feature of interest to you has changed to the default syntax format, you may have to manually migrate the older information. Following are guidelines for deciding if you need to migrate your policies:

- If you configured classic policies in a version of the Integrated Caching feature prior to release 9.0 and then upgrade to version 9.0 or later, there is no impact. All legacy policies are migrated to the default syntax policy format.
- For other features, you need to manually migrate classic policies and expressions to the default syntax if the feature has migrated to the default syntax.

Before You Proceed

Before configuring expressions and policies, be sure you understand the relevant NetScaler feature and the structure of your data, as follows:

- Read the documentation on the relevant feature.
- Look at the data stream for the type of data that you want to configure.

You may want to run a trace on the type of traffic or content that you want to configure. This will give you an idea of the parameters and values, and operations on these parameters and values, that you need to specify in an expression.

Configuring Default Syntax Policies

You can create default syntax policies for various NetScaler features, including DNS, Rewrite, Responder, and Integrated Caching, and the clientless access function in the Access Gateway. Policies control the behavior of these features.

When you create a policy, you assign it a name, a rule (an expression), feature-specific attributes, and an action that is taken when data matches the policy. After creating the policy, you determine when it is invoked by binding it globally or to either request-time or response-time processing for a virtual server.

Policies that share the same bind point are known as a *policy bank*. For example, all policies that are bound to a virtual server constitute the policy bank for the virtual server. When binding the policy, you assign it a priority level to specify when it is invoked relative to other policies in the bank. In addition to assigning a priority level, you can configure an arbitrary evaluation order for policies in a bank by specifying Goto expressions.

In addition to policy banks that are associated with a built-in bind point or a virtual server, you can configure *policy labels*. A policy label is a policy bank that is identified by an arbitrary name. You invoke a policy label, and the policies in it, from a global or virtual-server-specific policy bank. A policy label or a virtual-server policy bank can be invoked from multiple policy banks.

For some features, you can use the policy manager to configure and bind policies.

Rules for Names in Identifiers Used in Policies

The names of identifiers in the named expression, HTTP callout, pattern set, and rate limiting features must begin with an ASCII alphabet or an underscore (_). The remaining characters can be ASCII alphanumeric characters or underscores (_).

The names of these identifiers must not begin with the following reserved words:

- The words `ALT`, `TRUE`, or `FALSE` or the `Q` or `S` one-character identifier.
- The special-syntax indicator `RE` (for regular expressions) or `XP` (for XPath expressions).
- Expression prefixes, which currently are the following:
  - `CLIENT`
  - `EXTEND`
  - `HTTP`
  - `SERVER`
  - `SYS`
  - `TARGET`
  - `TEXT`
  - `URL`
  - `MYSQL`
  - `MSSQL`

Additionally, the names of these identifiers cannot be the same as the names of enumeration constants used in the policy infrastructure. For example, the name of an identifier cannot be `IGNORECASE`, `YEAR`, or `LATIN2_CZECH_CS` (a MySQL character set).

Note: The NetScaler appliance performs a case-insensitive comparison of identifiers with these words and enumeration constants. For example, names of the identifiers cannot begin with `TRUE`, `True`, or `true`.

Creating or Modifying a Policy

All policies have some common elements. Creating a policy consists, at minimum, of naming the policy and configuring a rule. The policy configuration tools for the various features have areas of overlap, but also differences. For the details of configuring a policy for a particular feature, including associating an action with the policy, see the documentation for the feature.

To create a policy, begin by determining the purpose of the policy. For example, you may want to define a policy that identifies HTTP requests for image files, or client requests that contain an SSL certificate. In addition to knowing the type of information that you want the policy to work with, you need to know the format of the data that the policy is analyzing.

Next, determine whether the policy is globally applicable, or if it pertains to a particular virtual server. Also consider the effect that the order in which your policies are evaluated (which will be determined by how you bind the policies) will have on the policy that you are about to configure.

To create a policy by using the command line interface

At the command prompt, type the following commands to create a policy and verify the configuration:

- `add responder|dns|cs|rewrite|cache policy <policyName> -rule <expression> [<feature-specific information>]`
- show rewrite policy <name>

Example 1:

```
add rewrite policy "pol_remove-ae" true "act_remove-ae"
 Done
> show rewrite policy pol_remove-ae
        Name: pol_remove-ae
        Rule: true
        RewriteAction: act_remove-ae
        UndefAction: Use Global
        Hits: 0
        Undef Hits: 0
        Bound to: GLOBAL RES_OVERRIDE
        Priority: 90
        GotoPriorityExpression: END
 Done
>
```

Example 2:

```
add cache policy BranchReportsCachePolicy -rule q{http.req.url.query.value("actionoverride").contains("
Done
   show cache policy BranchReportsCachePolicy
      Name: BranchReportsCachePolicy
      Rule: http.req.url.query.value("actionoverride").contains("branchReports")
      CacheAction: CACHE
      Stored in group: DEFAULT
      UndefAction: Use Global
      Hits: 0
      Undef Hits: 0
 Done
```

Note: At the command line, quote marks within a policy rule (the expression) must be escaped or delimited with the q delimiter. For more information, see "Configuring Default Syntax Expressions in a Policy."

Parameters for creating or modifying a policy

policyName

A unique name for the policy. (Cannot be changed for an existing policy.)

Note that in the Content Switching feature, the name cannot start with app_ because this is a reserved name. Policies with this name are not displayed in the configuration utility.

expression

A logical expression. See "Configuring Default Syntax Expressions: Getting Started."

feature-specific information

Varies by feature. Includes a built-in or user-defined action that you associate with the policy. See the documentation for the feature to which the policy applies.

To create or modify a policy by using the configuration utility

1. In the navigation pane, expand the name of the feature for which you want to configure a policy, and then click Policies. For example, you can select Content Switching, Integrated Caching, DNS, Rewrite, or Responder.

2. In the details pane, click Add, or select an existing policy and click Open. A policy configuration dialog box appears.

3. Specify values for the following parameters. (An asterisk indicates a required parameter. For a term in parentheses, see the corresponding parameter in "Parameters for creating or modifying a policy.")

4. Click Create, and then click Close.

5. Click Save. A policy is added.

   Note: After you create a policy, you can view the policy's details by clicking the policy entry in the configuration pane. Details that are highlighted and underlined are links to the corresponding entity (for example, a named expression).

Policy Configuration Examples

These examples show how policies and their associated actions are entered at the command line interface. In the configuration utility, the expressions would appear in the Expression window of the feature-configuration dialog box for the integrated caching or rewrite feature.

Following is an example of creating a caching policy. Note that actions for caching policies are built in, so you do not need to configure them separately from the policy.

```
add cache policy BranchReportsCachePolicy -rule q{http.req.url.query.value("actionoverride").contains("bra
```

Following is an example of a Rewrite policy and action:

```
add rewrite action myAction1 INSERT_HTTP_HEADER "myHeader" "valueForMyHeader"
add rewrite policy myPolicy1 "http.req.url.contains(\"myURLstring\")" myAction1
```

Note: At the command line, quote marks within a policy rule (the expression) must be escaped or delimited with the q delimiter. For more information, see "Configuring Default Syntax Expressions in a Policy."

Binding Policies That Use the Default Syntax

After defining a policy, you indicate when the policy is to be invoked by binding the policy to a bind point and specifying a priority level. You can bind a policy to only one bind point. A bind point can be global, that is, it can apply to all virtual servers that you have configured. Or, a bind point can be specific to a particular virtual server, which can be either a load balancing or a content switching virtual server. Not all bind points are available for all features.

The order in which policies are evaluated determines the order in which they are applied, and features typically evaluate the various policy banks in a particular order. Sometimes, however, other features can affect the order of evaluation. Within a policy bank, the order of evaluation depends on the values of parameters configured in the policies. Most features apply all of the actions associated with policies whose evaluation results in a match with the data that is being processed. The integrated caching feature is an exception.

Feature-Specific Differences in Policy Bindings

You can bind policies to built-in, global bind points (or banks), to virtual servers, or to policy labels.

However, the NetScaler features differ in terms of the types of bindings that are available. The following table summarizes how you use policy bindings in various NetScaler features that use policies.

Table 1. Feature-Specific Bindings for Policies

Feature Name	Virtual Servers Configured in the Feature	Policies Configured in the Feature	Bind Points Configured for the Policies	Use of Po the Featu
DNS	none	DNS policies	Global	To deterr how to pe DNS resol requests.

Content Switching **Note:** This feature can support either or classic policies or policies that use the default syntax, but not both.	Content Switching (CS)	Content Switching policies	· Content switching or cache redirection virtual server · Policy label	To determ what serv group of s is respons serving responses on charac of an inco request. Request character include d type, lang cookies, H method, type, and associate server.
Integrated Caching	none	Caching policies	· Global override · Global default · Policy label · Load balancing, content switching, or SSL offload virtual server	To determ whether I responses stored in, served fro NetScaler appliance integrate
Responder	none	Responder policies	· Global override · Global default · Policy label · Load balancing, content switching, or SSL offload virtual server	To config behavior Responde function.

Rewrite	none	Rewrite policies	· Global override · Global default · Policy label · Load balancing, content switching, or SSL offload virtual server	To identif data that want to m before se The polic provide ru modifying data. For exam can modi data to re request t selected s based on address o incoming or to mas informati response security purposes.
URL Transform function in the Rewrite feature	none	Transformation policies	· Global override · Global default · Policy label	To identif in HTTP transacti text files purpose o evaluatin whether a should be altered.
Access Gateway (clientless VPN functions only)	VPN server	Clientless Access policies	· VPN Global · VPN server	To determ how the A Gateway performs authentic authoriza auditing, other fun and to de rewrite ru general W access us Access Ga

Bind Points and Order of Evaluation

For a policy to take effect, you must ensure that the policy is invoked at some point during processing. To do so, you associate the policy with a bind point. The collection of policies that is bound to a bind point is known as a policy bank.

Following are the bind points that the NetScaler evaluates, listed in the typical order of evaluation within a policy bank

1. **Request-time override.** When a request flows through a feature, the NetScaler first evaluates request-time override policies for the feature.

2. **Request-time Load Balancing virtual server.** If policy evaluation cannot be completed after all the request-time override policies have been evaluated, the NetScaler processes request-time policies for load balancing virtual servers.

3. **Request-time Content Switching virtual server.** If policy evaluation cannot be completed after all the request-time policies for load balancing virtual servers have been evaluated, the NetScaler processes request-time policies for content switching virtual servers.

4. **Request-time default.** If policy evaluation cannot be completed after all request-time, virtual server-specific policies have been evaluated, the NetScaler processes request-time default policies.

5. **Response-time override.** At response time, the NetScaler starts with policies that are bound to the response-time override bind point.

6. **Response-time Load Balancing virtual server.** If policy evaluation cannot be completed after all response-time override policies have been evaluated, the NetScaler process the response-time policies for load balancing virtual servers.

7. **Response-time Content Switching virtual server.** If policy evaluation cannot be completed after all policies have been evaluated for load balancing virtual servers, the NetScaler process the response-time policies for content switching virtual servers.

8. **Response-time default.** If policy evaluation cannot be completed after all response-time, virtual-server-specific policies have been evaluated, the NetScaler processes response-time default policies.

Policy Evaluation across Features

In addition to attending to evaluation of policies within a feature, if you have bound policies to a content switching virtual server, note that these policies are evaluated before other policies. Binding a policy to a content switching vserver produces a different result in NetScaler versions 9.0.x and later than in 8.x versions. In NetScaler 9.0 and later versions, evaluation occurs as follows:

- Content switching policies are evaluated before other policies. If a content switching policy evaluates to TRUE, the target load balancing vserver is selected.

- If all content switching policies evaluate to FALSE, the default load balancing vserver under the content switching VIP is selected.

After a target load balancing vserver is selected by the content switching process, policies are evaluated in the following order:

1. Policies that are bound to the global override bind point.

2. Policies that are bound to the default load balancing vserver.

3. Policies that are bound to the target content switching vserver.

4. Policies that are bound to the global default bind point.

To be sure that the policies are evaluated in the intended order, follow these guidelines:

- Make sure that the default load balancing vserver is not directly reachable from the outside; for example, the vserver IP address can be 0.0.0.0.
- To prevent exposing internal data on the load balancing default vserver, configure a policy to respond with a “503 Service Unavailable” status and bind it to the default load balancing vserver.

Entries in a Policy Bank

Each entry in a policy bank has, at minimum, a policy and a priority level. You can also configure entries that change the priority-based evaluation order, and you can configure entries that invoke external policy banks.

The following table summarizes each entry in a policy bank.

Table 2. Format of Each Entry in a Policy Bank

Policy Name	Priority	Goto Expression	Invocation Type	Policy Bank to Be Invoked
The policy name, or a “dummy” policy named NOPOLICY. The NOPOLICY entry controls evaluation flow without processing a rule.	An integer.	Optional. Identifies the next policy in the bank to evaluate, or ends any further evaluation	Optional. Indicates that an external policy bank will be invoked. This field restricts the choices to a global policy label or a virtual server.	Optional. Used with Invocation Type. This is the label for a policy bank or a virtual server name. The NetScaler returns to the current bank after processing the external bank.

If the policy evaluates to TRUE, the NetScaler stores the action that is associated with the policy. If the policy evaluates to FALSE, the NetScaler evaluates the next policy. If the policy is neither TRUE nor FALSE, the NetScaler uses the associated Undef (undefined) action.

Evaluation Order within a Policy Bank

Within a policy bank, the evaluation order depends on the following items:

A priority.

The most minimal amount of information about evaluation order is a numeric priority level. The lower the number, the higher the priority.

A Goto expression.

If supplied, the Goto expression indicates the next policy to be evaluated, typically within the same policy bank.. Goto expressions can only proceed forward in a bank. To prevent looping, a policy bank configuration is not valid if a Goto statement points backwards in the bank.

Invocation of other policy banks.

Any entry can invoke an external policy bank. The NetScaler provides a built-in entity named NOPOLICY that does not have a rule. You can add a NOPOLICY entry in a policy bank when you want to invoke another policy bank, but do not want to process any other rules prior to the invocation. You can have multiple NOPOLICY entries in multiple policy banks.

Values for a Goto expression are as follows:

NEXT.

This keyword selects the policy with the next higher priority level in the current policy bank.

An integer.

If you supply an integer, it must match the priority level of another policy in the current policy bank.

END.

This keyword stops evaluation after processing the current policy, and no additional policies in this bank are processed.

Blank.

If the Goto expression is empty, it is the same as specifying END.

A numeric expression.

This is a default syntax expression that resolves to a priority number for another policy in the current bank.

USE_INVOCATION_RESULT.

This phrase can be used only if you are invoking an external policy bank. Entering this phrase causes the NetScaler to perform one of the following actions:

- If the final Goto in the invoked policy bank has a value of END or is empty, the invocation result is END, and evaluation stops.
- If the final Goto expression in the invoked policy bank is anything other than END, the NetScaler performs a NEXT.

The following table illustrates a policy bank that uses Goto statements and policy bank invocations.

Table 3. Example of a Policy Bank That Uses Gotos and External Bank Invocations

Policy Name	Priority	Goto	Invocation	Policy Bank to Be Invoked
ClientCertificatePolicy (rule: does the request contain a client certificate?)	100	300	None	None
SubnetPolicy (rule: is the client from a private subnet?)	200	NEXT	None	None
NOPOLICY	300	USE INVOCATION RESULT	Request vserver	My_Request_VServer
NOPOLICY	350	USE INVOCATION RESULT	Policy Label	My_Policy_Label
WorkingHoursPolicy (rule: is it working hours?)	400	END	None	None

How Policy Evaluation Ends

Evaluation of a policy bank ends when one of the following takes place:

- A policy evaluates to TRUE and its Goto statement value is END.

  No further policies or policy banks in this feature are evaluated.

- An external policy bank is invoked, its evaluation returns an END, and the Goto statement uses a value of USE_INVOCATION_RESULT or END.

  Evaluation continues with the next policy bank for this feature. For example, if the current bank is the request-time override bank, the NetScaler next evaluates request-time policy banks for the virtual servers.

- The NetScaler has walked through all the policy banks in this feature, but has not encountered an END.

  If this is the last entry to be evaluated in this policy bank, the NetScaler proceeds to the next feature.

How Features Use Actions after Policy Evaluation

After evaluating all relevant policies for a particular data point (for example, an HTTP request), the NetScaler stores all the actions that are associated with any policy that matched the data.

For most features, all the actions from matching policies are applied to a traffic packet as it leaves the NetScaler. The Integrated Caching feature only applies one action: CACHE or NOCACHE. This action is associated with the policy with the lowest priority value in the “highest priority” policy bank (for example, request-time override policies are applied before virtual server-specific policies).

Binding a Policy Globally

The following binding procedures are typical. However, refer to the documentation for the feature of interest to you for complete instructions.

To bind an Integrated Caching policy globally by using the command line interface

At the command prompt, type the following commands to bind an Integrated Caching policy and verify the configuration:

- bind cache global <policy> -priority <positiveInteger> [-type REQ_OVERRIDE | REQ_DEFAULT | RES_OVERRIDE | RES_DEFAULT]
- show cache global

  Example

  ```
  bind cache global _nonPostReq -priority 100 -type req_default
  Done
  > show cache global
  1)      Global bindpoint: REQ_DEFAULT
         Number of bound policies: 2

  2)      Global bindpoint: RES_DEFAULT
         Number of bound policies: 1
  Done
  ```

  The type argument is optional to maintain backward compatibility. If you omit the type, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression.

To bind a Rewrite policy globally by using the command line interface

At the command prompt, type the following commands to bind a Rewrite policy and verify the configuration:

- bind rewrite global <policyName> <priority> [-type REQ_OVERRIDE | REQ_DEFAULT | RES_OVERRIDE | RES_DEFAULT]
- show rewrite global

  Example

```
bind rewrite global pol_remove-pdf 100
 Done
> show rewrite global
1)      Global bindpoint: REQ_DEFAULT
        Number of bound policies: 1

2)      Global bindpoint: REQ_OVERRIDE
        Number of bound policies: 1

 Done
```

The type argument is optional for globally bound policies, to maintain backward compatibility. If you omit the type, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression.

To bind a compression policy globally by using the command line interface

At the command prompt, type the following commands to bind a compression policy and verify the configuration:

- bind cmp global <policyName> -priority <positiveInteger> [-type REQ_OVERRIDE | REQ_DEFAULT | RES_OVERRIDE | RES_DEFAULT]
- show cmp global

Example

```
> bind cmp global cmp_pol_1 -priority 100
 Done
> show cmp policy cmp_pol_1
        Name: cmp_pol_1
        Rule: HTTP.REQ.URL.SUFFIX.EQ("BMP")
        Response Action: COMPRESS
        Hits: 0

        Policy is bound to following entities
        1) GLOBAL REQ_DEFAULT
        Priority: 100
        GotoPriorityExpression: END
 Done
>
```

To bind a Responder policy globally by using the command line interface

At the command prompt, type the following commands to bind a Responder policy and verify the configuration:

- bind responder global <policyName> <priority> [-type OVERRIDE | DEFAULT]
- show responder global

Example

```
bind responder global pol404Error1 200
Done
> show responder global
1)      Global bindpoint: REQ_DEFAULT
        Number of bound policies: 1

Done
```

To bind a DNS policy globally by using the command line interface

At the command prompt, type the following commands to bind a DNS policy and verify the configuration:

- bind dns global <policyName> <priority>
- show dns global

Example

```
> bind dns global pol_ddos_drop1 150
Done
> show dns global
Policy name : pol_ddos_drop
        Priority : 100
        Goto expression : END
Policy name : pol_ddos_drop1
        Priority : 150
Done
>
```

To bind an Integrated Caching, Responder, Rewrite, or Compression policy globally by using the configuration utility

1. In the navigation pane, click the name of the feature for which you want to bind the policy.
2. In the details pane, click <Feature Name> policy manager.
3. In the Policy Manager dialog box, select the bind point to which you want to bind the policy (for example, for Integrated Caching, Rewrite, or Compression, you could select Request and Default Global). The Responder does not differentiate between request-time and response-time policies.
4. Click Insert Policy and, from the Policy Name pop-up menu, select the policy name. A priority is assigned automatically to the policy, but you can click the cell in the Priority column and drag it anywhere within the dialog box if you want the policy to be evaluated after other policies in this bank. The priority is automatically reset. Note that priority values within a policy bank must be unique.
5. Click Apply Changes.
6. Click Close. A message in the status bar indicates that the policy is bound successfully.

To bind a DNS policy globally by using the configuration utility

1. In the navigation pane, expand DNS, and then click Policies.
2. In the details pane, click Global Bindings.
3. In the global bindings dialog box, click Insert Policy, and select the policy that you want to bind globally.
4. Click in the Priority field and enter the priority level.
5. Click OK. A message in the status bar indicates that the policy is bound successfully.

Binding a Policy to a Virtual Server

A globally bound policy applies to all load balancing and content switching virtual servers.

Note that when binding a policy to a virtual server, you must identify it as a request-time or a response-time policy.

To bind a policy to a load balancing or content switching virtual server by using the command line interface

At the command prompt, type the following commands to bind a policy to a load balancing or content switching virtual server and verify the configuration:

- `bind lb|cs vserver <virtualServerName> -policyName <policyName> -priority <positiveInteger> -type REQUEST|RESPONSE`
- show lb vserver <name>

Example

```
> bind lb vserver lbvip -policyName ns_cmp_msapp -priority 50
 Done
> show lb vserver lbvip
        lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
        State: DOWN
        Last state change was at Wed Jul 15 05:54:24 2009 (+226 ms)
        Time since last state change: 28 days, 01:57:26.350
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1)      Policy : ns_cmp_msapp Priority:50
2)      Policy : cf-pol Priority:1      Inherited
 Done
```

To bind a policy to an SSL offload virtual server by using the command line interface

At the command prompt, type the following commands to bind a policy to an SSL offload virtual server and verify the configuration:

bind ssl vserver <vServerName>@ -policyName <policyName> -priority <positiveInteger>

To bind a policy to a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, Content Switching, SSL Offload, AAA-Application Traffic, or Access Gateway, and then click Virtual Servers.
2. In the details pane, double-click the virtual server to which you want to bind the policy, and then click Open.
3. On the Policies tab, click the icon for the type of policy that you want to bind (the choices are feature-specific), and then click the name of the policy. Note that for some features, you can bind both classic policies and policies that use the default syntax to the virtual server.
4. If you are binding a policy to a Content Switching virtual server, in the Target field select a load balancing virtual server to which traffic that matches the policy is sent.
5. Click OK. A message in the status bar indicates that the policy is bound successfully.

Displaying Policy Bindings

You can display policy bindings to verify that they are correct.

To display policy bindings by using the command line interface

At the command prompt, type the following commands to display policy bindings and verify the configuration:

show rewrite policy <name>

Example

```
> show rewrite policy pol_remove-pdf
        Name: pol_remove-pdf
        Rule: http.req.url.contains(".pdf")
        RewriteAction: act_remove-ae
        UndefAction: Use Global
        Hits: 0
        Undef Hits: 0
        Bound to: GLOBAL REQ_DEFAULT
        Priority: 100
        GotoPriorityExpression: END
 Done
>
```

To display global policy bindings for Integrated Caching, Rewrite, or Responder by using the configuration utility

1. In the navigation pane, expand the feature that contains the policy that you want to view, and then click Policies.
2. In the details pane, click the policy. Bound policies have a check mark next to them.
3. At the bottom of the page, under Details, next to Bound to, view the entity to which the policy is bound.

To display global policy bindings for DNS or Clientless Access in the Access Gateway by using the configuration utility

1. In the navigation pane, expand DNS, and then click Policies.
2. In the details pane, click Global Bindings.

To display global policy bindings for Content Switching by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Policies.
2. In detailed pane, select policy.
3. In the details pane, click Show Bindings.

Unbinding a Policy

If you want to re-assign a policy or delete it, you must first remove its binding.

To unbind an integrated caching, rewrite, or compression default syntax policy globally by using the command line interface

At the command prompt, type the following commands to unbind an integrated caching, rewrite, or compression default syntax policy globally and verify the configuration:

- `unbind cache|rewrite|cmp global <policyName> [-type req_override|req_default|res_override|res_default] [-priority <positiveInteger>]`
- `show cache|rewrite|cmp global`

Example

```
> unbind cache global_nonPostReq
 Done
> show cache global
1)      Global bindpoint: REQ_DEFAULT
       Number of bound policies: 1

2)      Global bindpoint: RES_DEFAULT
       Number of bound policies: 1

 Done
```

The priority is required only for the “dummy” policy named NOPOLICY.

To unbind a responder policy globally by using the command line interface

At the command prompt, type the following commands to unbind a responder policy globally and verify the configuration:

- unbind responder global `<policyName>` [-type override|default] [-priority <positiveInteger>]
- `show responder global`

Example

```
> unbind responder global pol404Error
 Done
> show responder global
1)      Global bindpoint: REQ_DEFAULT
        Number of bound policies: 1

 Done
```

The priority is required only for the “dummy” policy named NOPOLICY.

To unbind a DNS policy globally by using the command line interface

At the command prompt, type the following commands to unbind a DNS policy globally and verify the configuration:

- unbind responder global <policyName>
- unbind responder global

Example

```
 unbind dns global dfgdfg
 Done
 show dns global
Policy name : dfgdfggfhg
        Priority : 100
        Goto expression : END
 Done
```

To unbind a default syntax policy from a virtual server by using the command line interface

At the command prompt, type the following commands to unbind a default syntax policy from a virtual server and verify the configuration:

- unbind cs vserver <name> -policyName <policyName> [-priority <positiveInteger>] [-type REQUEST|RESPONSE]
- show lb vserver <name>

Example

```
 unbind cs vserver vs-cont-switch  -policyName pol1
 Done
> show cs vserver vs-cont-switch
        vs-cont-switch (10.102.29.10:80) - HTTP Type: CONTENT
        State: UP
        Last state change was at Wed Aug 19 08:56:55 2009 (+18 ms)
        Time since last state change: 0 days, 02:47:55.750
```

```
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        State Update: DISABLED
        Default:        Content Precedence: RULE
        Vserver IP and Port insertion: OFF
        Case Sensitivity: ON
        Push: DISABLED  Push VServer:
        Push Label Rule: none
 Done
```

The priority is required only for the “dummy” policy named NOPOLICY.

To unbind an integrated caching, responder, rewrite, or compression default syntax policy globally by using the configuration utility

1. In the navigation pane, click the feature with the policy that you want to unbind (for example, Integrated Caching).
2. In the details pane, click <Feature Name> policy manager.
3. In the Policy Manager dialog box, select the bind point with the policy that you want to unbind, for example, Default Global.
4. Click the policy name that you want to unbind, and then click Unbind Policy.
5. Click Apply Changes.
6. Click Close. A message in the status bar indicates that the policy is unbound successfully.

To unbind a DNS policy globally by using the configuration utility

1. In the navigation pane, expand DNS, and then click Policies.
2. In the details pane, click Global Bindings.
3. In the Global Bindings dialog box, select policy and click unbind policy.
4. Click OK. A message in the status bar indicates that the policy is unbinded successfully.

To unbind a default syntax policy from a load balancing or content switching virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing or Content Switching, and then click Virtual Servers.
2. In the details pane, double-click the virtual server from which you want to unbind the policy.
3. On the Policies tab, in the Active column, clear the check box next to the policy that you want to unbind.
4. Click OK. A message in the status bar indicates that the policy is unbinded successfully.

Creating Policy Labels

In addition to the built-in bind points where you set up policy banks, you can also configure user-defined policy labels and associate policies with them.

Within a policy label, you bind policies and specify the order of evaluation of each policy relative to others in the bank of policies for the policy label. The NetScaler also permits you to define an arbitrary evaluation order as follows:

- You can use “goto” expressions to point to the next entry in the bank to be evaluated after the current one.
- You can use an entry in a policy bank to invoke another bank.

Creating Policy Labels

Each feature determines the type of policy that you can bind to a policy label, the type of load balancing virtual server that you can bind the label to, and the type of content switching virtual server from which the label can be invoked. For example, a TCP policy label can only be bound to a TCP load balancing virtual server. You cannot bind HTTP policies to a policy label of this type. And you can invoke a TCP policy label only from a TCP content switching virtual server.

After configuring a new policy label, you can invoke it from one or more banks for the built-in bind points.

To create a caching policy label by using the command line interface

At the command prompt, type the following commands to create a Caching policy label and verify the configuration:

- add cache policylabel <labelName> -evaluates req|res
- show cache policylabel<labelName>

Example

```
> add cache policylabel lbl-cache-pol -evaluates req
 Done

> show cache policylabel lbl-cache-pol
        Label Name: lbl-cache-pol
        Evaluates: REQ
        Number of bound policies: 0
        Number of times invoked: 0
 Done
>
```

To create a Content Switching policy label by using the command line interface

At the command prompt, type the following commands to create a Content Switching policy label and verify the configuration:

- add cs policylabel <labelName> http|tcp|rtsp|ssl
- show cs policylabel <labelName>

Example

```
> add cs policylabel lbl-cs-pol http
 Done
> show cs policylabel lbl-cs-pol
        Label Name: lbl-cs-pol
        Label Type: HTTP
        Number of bound policies: 0
        Number of times invoked: 0
 Done
```

To create a Rewrite policy label by using the command line interface

At the command prompt, type the following commands to create a Rewrite policy label and verify the configuration:

- add rewrite policylabel <labelName> http_req|http_res|url|text|clientless_vpn_req|clientless_vpn_res
- show rewrite policylabel <labelName>

Example

```
> add rewrite policylabel lbl-rewrt-pol http_req
 Done

> show rewrite policylabel lbl-rewrt-pol
        Label Name: lbl-rewrt-pol
        Transform Name: http_req
        Number of bound policies: 0
        Number of times invoked: 0
 Done
```

To create a Responder policy label by using the command line interface

At the command prompt, type the following commands to create a Responder policy label and verify the configuration:

- add responder policylabel <labelName>
- show responder policylabel <labelName>

Example

```
> add responder policylabel lbl-respndr-pol
 Done

> show responder policylabel lbl-respndr-pol
```

```
    Label Name: lbl-respndr-pol
    Number of bound policies: 0
    Number of times invoked: 0
Done
```

Note: Invoke this policy label from a policy bank. For more information, see "Binding a Policy to a Policy Label."

To create a policy label by using the configuration utility

1. In the navigation pane, expand the feature for which you want to create a policy label, and then click Policy Labels. The choices are Integrated Caching, Rewrite, Content Switching, or Responder.
2. In the details pane, click Add.
3. In the Name box, enter a unique name for this policy label.
4. Enter feature-specific information for the policy label. For example, for Integrated Caching, in the Evaluates drop-down menu, you would select REQ if you want this policy label to contain request-time policies, or select RES if you want this policy label to contain response-time policies. For Rewrite, you would select a Transform name.
5. Click Create.
6. Configure one of the built-in policy banks to invoke this policy label. For more information, see "Binding a Policy to a Policy Label." A message in the status bar indicates that the policy label is created successfully.

Binding a Policy to a Policy Label

As with policy banks that are bound to the built-in bind points, each entry in a policy label is a policy that is bound to the policy label. As with policies that are bound globally or to a vserver, each policy that is bound to the policy label can also invoke a policy bank or a policy label that is evaluated after the current entry has been processed. The following table summarizes the entries in a policy label.

Name

The name of a policy, or, to invoke another policy bank without evaluating a policy, the "dummy" policy name NOPOLICY.

You can specify NOPOLICY more than once in a policy bank, but you can specify a named policy only once.

Priority

An integer. This setting can work with the Goto expression.

Goto Expression

Determines the next policy to evaluate in this bank. You can provide one of the following values:

NEXT:

Go to the policy with the next higher priority.

END:

Stop evaluation.

USE_INVOCATION_RESULT:

Applicable if this entry invokes another policy bank. If the final Goto in the invoked bank has a value of END, evaluation stops. If the final Goto is anything other than END, the current policy bank performs a NEXT.

Positive number:

The priority number of the next policy to be evaluated.

Numeric expression:

An expression that produces the priority number of the next policy to be evaluated.

The Goto can only proceed forward in a policy bank.

If you omit the Goto expression, it is the same as specifying END.

Invocation Type

Designates a policy bank type. The value can be one of the following:

Request Vserver:

Invokes request-time policies that are associated with a virtual server.

Response Vserver:

Invokes response-time policies that are associated with a virtual server.

Policy label:

Invokes another policy bank, as identified by the policy label for the bank.

Invocation Name

The name of a virtual server or a policy label, depending on the value that you specified for the Invocation Type.

Configuring a Policy Label or Virtual Server Policy Bank

After you have created policies, and created policy banks by binding the policies, you can perform additional configuration of polices within a label or policy bank. For example, before you configure invocation of an external policy bank, you might want to wait until you have configured that policy bank.

Configuring a Policy Label

A policy label consists of a set of policies and invocations of other policy labels and virtual server-specific policy banks. An Invoke parameter enables you to invoke a policy label or a virtual server-specific policy bank from any other policy bank. A special-purpose NoPolicy entry enables you to invoke an external bank without processing an expression (a rule). The NoPolicy entry is a “dummy” policy that does not contain a rule.

For configuring policy labels from the NetScaler command line, note the following elaborations of the command syntax:

- gotoPriorityExpression is configured as described in "Entries in a Policy Bank."
- The type argument is required. This is unlike binding a conventional policy, where this argument is optional.
- You can invoke the bank of policies that are bound to a virtual server by using the same method as you use for invoking a policy label.

To configure a policy label by using the command line interface

At the command prompt, type the following commands to configure a policy label and verify the configuration:

- `bind cache|rewrite|responder policylabel <policylabelName> -policyName <policyName> -priority <priority> [-gotoPriorityExpression <gotopriorityExpression>] [-invoke reqvserver|resvserver|policylabel <policyLabelName>|<vserverName>]`
- `show cache|rewrite|responder policylabel <policylabelName>`

Example

```
bind cache policylabel _reqBuiltinDefaults -policyName  _nonGetReq -priority 100
Done
show cache policylabel _reqBuiltinDefaults
        Label Name: _reqBuiltinDefaults
        Evaluates: REQ
        Number of bound policies: 3
        Number of times invoked: 0
1)      Policy Name: _nonGetReq
        Priority: 100
        GotoPriorityExpression: END
2)      Policy Name: _advancedConditionalReq
        Priority: 200
        GotoPriorityExpression: END
```

```
3)     Policy Name: _personalizedReq
       Priority: 300
       GotoPriorityExpression: END
Done
```

To invoke a policy label from a Rewrite policy bank with a NOPOLICY entry by using the command line interface

At the command prompt, type the following commands to invoke a policy label from a Rewrite policy bank with a NOPOLICY entry and verify the configuration:

- bind rewrite global <policyName> <priority> <gotoPriorityExpression> -type REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT -invoke reqvserver|resvserver|policylabel <policyLabelName>|<vserverName>
- `show rewrite global`

  Example

```
> bind rewrite global NOPOLICY 100 -type REQ_DEFAULT -invoke policylabel lbl-rewrt-pol
Done
> show rewrite global
1)     Global bindpoint: REQ_DEFAULT
       Number of bound policies: 1

2)     Global bindpoint: REQ_OVERRIDE
       Number of bound policies: 1
Done
```

To invoke a policy label from an Integrated Caching policy bank by using the command line interface

At the command prompt, type the following commands to invoke a policy label from an Integrated Caching policy bank and verify the configuration:

- `bind cache global NOPOLICY -priority <priority> -gotoPriorityExpression <gotopriorityExpression> -type REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT -invoke reqvserver|resvserver|policylabel <policyLabelName>|<vserverName>`
- `show cache global`

  Example

```
bind cache global NOPOLICY -priority 100 -gotoPriorityExpression END -type REQ_DEFAULT -invoke polic
Done
> show cache global
```

1) Global bindpoint: REQ_DEFAULT
Number of bound policies: 2

2) Global bindpoint: RES_DEFAULT
Number of bound policies: 1

Done

To invoke a policy label from a Responder policy bank by using the command line interface

At the command prompt, type the following commands to invoke a policy label from a Responder policy bank and verify the configuration:

- `bind responder global NOPOLICY <priority> <gotoprioritыExpression> -type OVERRIDE|DEFAULT -invoke vserver|policylabel <policyLabelName>|<vserverName>`
- `show responder global`

Example

> bind responder global NOPOLICY 100 NEXT -type DEFAULT -invoke policylabel lbl-respndr-pol
Done
> show responder global
1) Global bindpoint: REQ_DEFAULT
Number of bound policies: 2

Done

To configure a policy label by using the configuration utility

1. In the navigation pane, expand the feature for which you want to configure a policy label, and then click Policy Labels. The choices are Integrated Caching, Rewrite, or Responder.

2. In the details pane, double-click the label that you want to configure.

3. If you are adding a new policy to this policy label, click Insert Policy, and in the Policy Name field, select New Policy. For more information about adding a policy, see "Creating or Modifying a Policy." Note that if you are invoking a policy bank, and do not want a rule to be evaluated prior to the invocation, click Insert Policy, and in the Policy Name field select NOPOLICY.

4. For each entry in this policy label, configure the following:

   Policy Name:

   This is already determined by the Policy Name, new policy, or NOPOLICY entry that you inserted in this bank.

   Priority:

   A numeric value that determines either an absolute order of evaluation within the bank, or is used in conjunction with a Goto expression.

   Expression:

   The policy rule. Policy expressions are described in detail in the following chapters. For an introduction, see "Configuring Default Syntax Expressions: Getting Started."

   Action:

   The action to be taken if this policy evaluates to TRUE.

   Goto Expression:

   Optional. Used to augment the Priority level to determine the next policy or policy bank to evaluate. For more information on possible values for a Goto expression, see the table "Entries in a Policy Bank."

   Invoke:

   Optional. Invokes another policy bank.

5. Click Ok. A message in the status bar indicates that the policy label is configured successfully.

Configuring a Policy Bank for a Virtual Server

You can configure a bank of policies for a virtual server. The policy bank can contain individual policies, and each entry in the policy bank can optionally invoke a policy label or a bank of policies that you configured for another virtual server. If you invoke a policy label or policy bank, you can do so without triggering an expression (a rule) by selecting a NOPOLICY “dummy” entry instead of a policy name.

To add policies to a virtual server policy bank by using the command line interface

At the command prompt, type the following commands to add policies to a virtual server policy bank and verify the configuration:

- `bind lb|cs vserver <virtualServerName> <serviceType> [-policyName <policyName>] [-priority <positiveInteger>] [-gotoPriorityExpression <expression>] [-type REQUEST|RESPONSE]`
- `show lb|cs vserver <virtualServerName>`

Example

```
add lb vserver vs-cont-sw TCP
Done
show lb vserver vs-cont-sw
      vs-cont-sw (0.0.0.0:0) - TCP    Type: ADDRESS
      State: DOWN
      Last state change was at Wed Aug 19 10:04:02 2009 (+279 ms)
      Time since last state change: 0 days, 00:02:14.420
      Effective State: DOWN
      Client Idle Timeout: 9000 sec
      Down state flush: ENABLED
      Disable Primary Vserver On Down : DISABLED
      No. of Bound Services :  0 (Total)      0 (Active)
      Configured Method: LEASTCONNECTION
      Mode: IP
      Persistence: NONE
      Connection Failover: DISABLED
Done
```

To invoke a policy label from a virtual server policy bank with a NOPOLICY entry by using the command line interface

At the command prompt, type the following commands to invoke a policy label from a virtual server policy bank with a NOPOLICY entry and verify the configuration:

- `bind lb|cs vserver <virtualServerName> -policyName NOPOLICY_REWRITE|NOPOLICY_CACHE|NOPOLICY_RESPONDER -priority <integer> -type REQUEST|RESPONSE -gotoPriorityExpression <gotopriorityExpression> -invoke reqVserver|resVserver|policyLabel <vserverName>|<labelName>`

- `show lb vserver`

  Example

  > bind lb vserver vs-cont-sw -policyname NOPOLICY-REWRITE -priority 200 -type REQUEST -gotoPriorityEx
  Done

To configure a virtual server policy bank by using the configuration utility

1. In the left navigation pane, expand Load Balancing, Content Switching, SSL Offload, AAA - Application Traffic, or Access Gateway, as appropriate, and then click Virtual Servers.

2. In the details pane, select the virtual server that you want to configure, and then click Open.

3. In the Configure Virtual Server dialog box click the Policies tab.

4. To create a new policy in this bank, click the icon for the type of policy or policy label that you want to add to the virtual server's bank of policies, click Insert Policy. Note that if you want to invoke a policy label without evaluating a policy rule, select the NOPOLICY "dummy" policy.

5. To configure an existing entry in this policy bank, enter the following:

   Priority:

   A numeric value that determines either an absolute order of evaluation within the bank or is used in conjunction with a Goto expression.

   Expression:

   The policy rule. Policy expressions are described in detail in the following chapters. For an introduction, see "Configuring Default Syntax Expressions: Getting Started."

   Action: on:

   The action to be taken if this policy evaluates to TRUE.

   Goto Expression:

   Optional. Determines the next policy or policy bank to evaluate. For more information on possible values for a Goto expression, see "Entries in a Policy Bank."

   Invoke:

   Optional. To invoke another policy bank, select the name of the policy label or virtual server policy bank that you want to invoke.

6. When you are done, click OK. A message in the status bar indicates that the policy is configured successfully.

Invoking or Removing a Policy Label or Virtual Server Policy Bank

Unlike a policy, which can only be bound once, you can use a policy label or a virtual server's policy bank any number of times by invoking it. Invocation can be performed from two places:

- From the binding for a named policy in a policy bank.
- From the binding for a NOPOLICY "dummy" entry in a policy bank.

Typically, the policy label must be of the same type as the policy from which it is invoked. For example, you would invoke a responder policy label from a responder policy.

Note: When binding or unbinding a global NOPOLICY entry in a policy bank at the command line, you specify a priority to distinguish one NOPOLICY entry from another.

To invoke a rewrite or integrated caching policy label by using the command line interface

At the command prompt, type the one of the following commands to invoke a rewrite or integrated caching policy label and verify the configuration:

- bind cache global <policy> -priority <positive_integer> [**-gotoPriorityExpression** <expression>] **-type REQ_OVERRIDE**|**REQ_DEFAULT**|**RES_OVERRIDE**|**RES_DEFAULT**] **-invoke reqvserver**|**resvserver**|**policylabel** <label_name>
- bind rewrite global<policy> -priority <positive_integer> [**-gotoPriorityExpression** <expression>] **-type REQ_OVERRIDE**|**REQ_DEFAULT**|**RES_OVERRIDE**|**RES_DEFAULT**] **-invoke reqvserver**|**resvserver**|**policylabel** <label_name>
- show cache global|show rewrite global

  Example

  > bind cache global _nonPostReq2 -priority 100 -type req_override -invoke policylabel lbl-cache-pol
  Done
  > show cache global
  1) Global bindpoint: REQ_DEFAULT
  Number of bound policies: 2

  2) Global bindpoint: RES_DEFAULT
  Number of bound policies: 1

  3) Global bindpoint: REQ_OVERRIDE

```
        Number of bound policies: 1

    Done
```

To invoke a responder policy label by using the command line interface

At the command prompt, type the following commands to invoke a responder policy label and verify the configuration:

- **bind responder global** <policy_Name> <priority_as_positive_integer> [<gotoPriorityExpression>] **-type REQ_OVERRIDE|REQ_DEFAULT|OVERRIDE|DEFAULT -invoke vserver|policylabel** <label_name>

- **show responder global**

  Example

```
> bind responder global pol404Error1 300 -invoke policylabel lbl-respndr-pol
 Done
> show responder global
1)      Global bindpoint: REQ_DEFAULT
        Number of bound policies: 2

 Done
>
```

To invoke a Virtual Server Policy Bank by using the command line interface

At the command prompt, type the following commands to invoke a Virtual Server Policy Bank and verify the configuration:

- **bind lb vserver** <vserver_name> **-policyName** <policy_Name> **-priority** <positive_integer> [**-gotoPriorityExpression** <expression>] **-type REQUEST|RESPONSE -invoke reqvserver|resvserver|policylabel** <policy_Label_Name>

- **bind lb vserver** <vserver_name>

  Example

```
> bind lb vserver lbvip -policyName ns_cmp_msapp -priority 100
 Done

> show lb vserver lbvip
        lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
        State: DOWN
```

```
        Last state change was at Wed Jul 15 05:54:24 2009 (+166 ms)
        Time since last state change: 28 days, 06:37:49.250
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1)      CSPolicy: pol-cont-sw   CSVserver: vs-cont-sw   Priority: 100   Hits: 0

1)      Policy : pol-ssl Priority:0
2)      Policy : ns_cmp_msapp Priority:100
3)      Policy : cf-pol Priority:1      Inherited
 Done
>
```

To remove a rewrite or integrated caching policy label by using the command line interface

At the command prompt, type one of the following commands to remove a rewrite or integrated caching policy label and verify the configuration:

- unbind rewrite global <policyName> -priority <positiveInteger> -type **REQ_OVERRIDE**|**REQ_DEFAULT**|**RES_OVERRIDE**|**RES_DEFAULT**
- unbind cache global <policyName> -priority <positiveInteger> -type **REQ_OVERRIDE**|**REQ_DEFAULT**|**RES_OVERRIDE**|**RES_DEFAULT**
- show rewrite global|show cache global

  Example

```
> unbind rewrite global NOPOLICY -priority 100 -type REQ_OVERRIDE
 Done
> show rewrite global
1)      Global bindpoint: REQ_DEFAULT
        Number of bound policies: 1

 Done
```

To remove a responder policy label by using the command line interface

At the command prompt, type the following commands to remove a responder policy label and verify the configuration:

- unbind responder global <policyName> -priority <positiveInteger> **-type OVERRIDE|DEFAULT**
- **show responder global**

Example

```
> unbind responder global NOPOLICY -priority 100 -type REQ_DEFAULT
 Done
> show responder global
1)      Global bindpoint: REQ_DEFAULT
        Number of bound policies: 1

 Done
```

To remove a Virtual Server policy label by using the command line interface

At the command prompt, type one of the following commands to remove a Virtual Server policy label and verify the configuration:

- unbind lb vserver <virtualServerName> -policyName **NOPOLICY-REWRITE|NOPOLICY-RESPONDER|NOPOLICY-CACHE -type REQUEST|RESPONSE -priority** <positiveInteger>
- unbind cs vserver <virtualServerName> -policyName **NOPOLICY-REWRITE|NOPOLICY-RESPONDER|NOPOLICY-CACHE -type REQUEST|RESPONSE -priority** <positiveInteger>
- show lb vserver|show cs vserver

Example

```
> unbind lb vserver lbvip -policyName ns_cmp_msapp -priority 200
 Done
> show lb vserver lbvip
        lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
        State: DOWN
        Last state change was at Wed Jul 15 05:54:24 2009 (+161 ms)
        Time since last state change: 28 days, 06:47:54.600
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
```

```
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

    1)      CSPolicy: pol-cont-sw   CSVserver: vs-cont-sw   Priority: 100   Hits: 0

    1)      Policy : pol-ssl Priority:0
    2)      Policy : cf-pol Priority:1      Inherited
     Done
```

To invoke a policy label or virtual server policy bank by using the configuration utility

1. Bind a policy, as described in "Binding a Policy Globally", "Binding a Policy to a Virtual Server", or "Binding a Policy to a Policy Label." Alternatively, you can enter a NOPOLICY “dummy” entry instead of a policy name. You do this if you do not want to evaluate a policy before evaluating the policy bank.

2. In the Invoke field, select the name of the policy label or virtual server policy bank that you want to evaluate if traffic matches the bound policy. A message in the status bar indicates that the policy label or virtual server policy bank is invoked successfully.

To remove a policy label invocation by using the configuration utility

1. Open the policy and clear the Invoke field. Unbinding the policy also removes the invocation of the label. A message in the status bar indicates that the policy label is removed successfully.

Configuring and Binding Policies with the Policy Manager

Some applications provide a specialized Policy Manager in the NetScaler configuration utility to simplify configuring policy banks. It also lets you find and delete policies and actions that are not being used.

The Policy Manager is currently available for the Rewrite, Integrated Caching, Responder, and Compression features.

The following are keyboard equivalents for the procedures in this section:

- For editing a cell in the Policy Manager, you can tab to the cell and click F2 or press the SPACE bar on the keyboard.
- To select an entry in a drop-down menu, you can tab to the entry, press the space bar to view the drop-down menu, use the UP and DOWN ARROW keys to navigate to the entry that you want, and press the space bar again to select the entry.
- To cancel a selection in a drop-down menu, press the Escape key.
- To insert a policy, tab to the row above the insertion point and press Control + Insert, or click Insert Policy.
- To remove a policy, tab to the row that contains the policy and press Delete.

Note: Note that when you delete the policy, the NetScaler searches the Goto Expression values of other policies in the bank. If any of these Goto Expression values match the priority level of the deleted policy, they are removed.

To configure policy bindings by using the Policy Manager

1. In the navigation pane, click the feature for which you want to configure policies. The choices are Responder, Integrated Caching, Rewrite or Compression.

2. In the details pane, click Policy Manager.

3. If you are configuring classic policy bindings for compression, in the Compression Policy Manager dialog box, click **Switch to Classic Syntax**. The dialog box switches to the classic syntax view and displays the Switch to Default Syntax button. At any time before you complete configuring policy bindings, if you want to configure bindings for policies that use the default syntax, click the Switch to Default Syntax button.

4. For features other than Responder, to specify the bind point, click Request or Response, and then click one of the request-time or response-time bind points. The options are Override Global, LB Virtual Server, CS Virtual Server, Default Global, or Policy Label. If you are configuring the Responder, the Request and Response flow types are not available.

5. To bind a policy to this bind point, click Insert Policy, and select a previously configured policy, a NOPOLICY label, or the New policy option. Depending on the option that you select, you have the following choices:

   - **New policy:** Create the policy as described in "Creating or Modifying a Policy," and then configure the priority level, GoTo expression, and policy invocation as described in the table, "Format of Each Entry in a Policy Bank."

   - **Existing policy**, **NOPOLICY**, or **NOPOLICY<feature name>**: Configure the priority level, GoTo expression, and policy invocation as described in the table, "Format of Each Entry in a Policy Bank." The **NOPOLICY** or **NOPOLICY<feature name>** options are available only for policies that use default syntax expressions.
6. Repeat the preceding steps to add entries to this policy bank.

7. To modify the priority level for an entry, you can do any of the following:

   - Double-click the Priority field for an entry and edit the value.

   - Click and drag a policy to another row in the table.

   - Click Regenerate Priorities.

   In all three cases, priority levels of all other policies are modified as needed to accommodate the new value. Goto Expressions with integer values are also updated automatically. For example, if you change a priority value of 10 to 100, all policies with a Goto Expression value of 10 are updated to the value 100.

8. To change the policy, action, or policy bank invocation for an row in the table, click the down arrow to the right of the entry and do one of the following:

   - To change the policy, select another policy name or select New Policy and follow the steps in "Creating or Modifying a Policy."

   - To change the Goto Expression, select Next, End, USE_INVOCATION_RESULT, or select more and enter an expression whose result returns the priority level of

another entry in this policy bank.

- To modify an invocation, select an existing policy bank, or click New Policy Label and follow the steps in "Binding a Policy to a Policy Label."

9. To unbind a policy or a policy label invocation from this bank, click any field in the row that contains the policy or policy label, and then click Unbind Policy.

10. When you are done, click Apply Changes. A message in the status bar indicates that the policy is bound successfully.

To remove unused policies by using the Policy Manager

1. In the navigation pane, click the feature for which you want to configure the policy bank. The choices are Responder, Integrated Caching, or Rewrite.

2. In the details pane, click <Feature Name> policy manager.

3. In the <Feature Name> Policy Manager dialog box, click Cleanup Configuration.

4. In the Cleanup Configuration dialog box, select the items that you want to delete, and then click Remove.

5. In the Remove dialog box, click Yes.

6. Click Close. A message in the status bar indicates that the policy is removed successfully.

Configuring Default Syntax Expressions: Getting Started

Default syntax policies evaluate data on the basis of information that you supply in default syntax expressions. A default syntax expression analyzes data elements (for example, HTTP headers, source IP addresses, the NetScaler system time, and POST body data). In addition to configuring a default syntax expression in a policy, in some NetScaler features you configure default syntax expressions outside of the context of a policy.

To create a default syntax expression, you select a prefix that identifies a piece of data that you want to analyze, and then you specify an operation to perform on the data. For example, an operation can match a piece of data with a text string that you specify, or it can transform a text string into an HTTP header. Other operations match a returned string with a set of strings or a string pattern. You configure compound expressions by specifying Boolean and arithmetic operators, and by using parentheses to control the order of evaluation.

Default syntax expressions can also contain classic expressions. You can assign a name to a frequently used expression to avoid having to build the expression repeatedly.

Expression Characteristics

Policies and a few other entities include rules that the NetScaler uses to evaluate a packet in the traffic flowing through it, to extract data from the NetScaler system itself, to send a request (a “callout”) to an external application, or to analyze another piece of data. A rule takes the form of a logical expression that is compared against traffic and ultimately returns values of TRUE or FALSE.

The elements of the rule can themselves return TRUE or FALSE, string, or numeric values.

Before configuring a default syntax expression, you need to understand the characteristics of the data that the policy or other entity is to evaluate. For example, when working with the Integrated Caching feature, a policy determines what data can be stored in the cache. With Integrated Caching, you need to know the URLs, headers, and other data in the HTTP requests and responses that the NetScaler receives. With this knowledge, you can configure policies that match the actual data and enable the NetScaler to manage caching for HTTP traffic. This information helps you determine the type of expression that you need to configure in the policy.

Basic Elements of a Default Syntax Expression

A default syntax expression consists of, at a minimum, a prefix (or a single element used in place of a prefix). Most expressions also specify an operation to be performed on the data that the prefix identifies. You format an expression of up to 1,499 characters as follows:

```
<prefix>.<operation> [<compound-operator> <prefix>.<operation>. . .]
```

where

<prefix>

is an anchor point for starting an expression.

The prefix is a period-delimited key that identifies a unit of data. For example, the following prefix examines HTTP requests for the presence of a header named Content-Type:

```
http.req.header("Content-Type")
```

Prefixes can also be used on their own to return the value of the object that the prefix identifies.

<operation>

identifies an evaluation that is to be performed on the data identified by the prefix.

For example, consider the following expression:

```
http.req.header("Content-Type").eq("text/html")
```

In this expression, the following is the operator component:

```
eq("text/html")
```

This operator causes the NetScaler to evaluate any HTTP requests that contain a Content-Type header, and in particular, to determine if the value of this header is equal to the string “text/html.” For more information, see "Operations."

<compound-operator>

is a Boolean or arithmetic operator that forms a compound expression from multiple prefix or prefix.operation elements.

For example, consider the following expression:

```
http.req.header("Content-Type").eq("text/html") &&
http.req.url.contains(".html")
```

Prefixes

An expression prefix represents a discrete piece of data. For example, an expression prefix can represent an HTTP URL, an HTTP Cookie header, or a string in the body of an HTTP POST request. An expression prefix can identify and return a wide variety of data types, including the following:

- A client IP address in a TCP/IP packet
- NetScaler system time
- An external callout over HTTP
- A TCP or UDP record type

In most cases, an expression prefix begins with one of the following keywords:

CLIENT:

Identifies a characteristic of the client that is either sending a request or receiving a response, as in the following examples:

- The prefix `client.ip.dst` designates the destination IP address in the request or response.
- The prefix `client.ip.src` designates the source IP address.

HTTP:

Identifies an element in an HTTP request or a response, as in the following examples:

- The prefix `http.req.body(integer)` designates the body of the HTTP request as a multiline text object, up to the character position designated in integer.
- The prefix `http.req.header("header_name")` designates an HTTP header, as specified in header_name.
- The prefix `http.req.url` designates an HTTP URL in URL-encoded format.

SERVER:

Identifies an element in the server that is either processing a request or sending a response.

SYS:

Identifies a characteristic of the NetScaler that is processing the traffic.

Note: Note that DNS policies support only SYS, CLIENT, and SERVER objects.

In addition, in the Access Gateway, the Clientless VPN function can use the following types of prefixes:

TEXT:

Identifies any text element in a request or a response.

TARGET:

Identifies the target of a connection.

URL:

Identifies an element in the URL portion of an HTTP request or response.

As a general rule of thumb, any expression prefix can be a self-contained expression. For example, the following prefix is a complete expression that returns the contents of the HTTP header specified in the string argument (enclosed in quotation marks):

```
http.res.header.("myheader")
```

Or you can combine prefixes with simple operations to determine TRUE and FALSE values. For example, the following returns a value of TRUE or FALSE:

```
http.res.header.("myheader").exists
```

You can also use complex operations on individual prefixes and multiple prefixes within an expression, as in the following example:

```
http.req.url.length + http.req.cookie.length <= 500
```

Which expression prefixes you can specify depends on the NetScaler feature. The following table describes the expression prefixes that are of interest on a per-feature basis

Table 1. Permitted Types of Expression Prefixes in Various NetScaler Features

Feature	Types of Expression Prefix Used in the Feature
DNS	`SYS, CLIENT, SERVER`
Responder in Protection Features	`HTTP, SYS, CLIENT`
Content Switching	`HTTP, SYS, CLIENT`
Rewrite	`HTTP, SYS, CLIENT, SERVER, URL, TEXT, TARGET, VPN`
Integrated Caching	`HTTP, SYS, CLIENT, SERVER`
Access Gateway, Clientless Access	`HTTP, SYS, CLIENT, SERVER, URL, TEXT, TARGET, VPN`

Note: For details on the permitted expression prefixes in a feature, see the documentation for that feature.

Single-Element Expressions

The simplest type of default syntax expression contains a single element. This element can be one of the following:

- `true`. A default syntax expression can consist simply of the value `true`. This type of expression always returns a value of TRUE. It is useful for chaining policy actions and triggering Goto expressions.
- `false`. A default syntax expression can consist simply of the value `false`. This type of expression always returns a value of FALSE.
- A prefix for a compound expression. For example, the prefix `HTTP.REQ.HOSTNAME` is a complete expression that returns a host name and `HTTP.REQ.URL` is a complete expression that returns a URL. The prefix could also be used in conjunction with operations and additional prefixes to form a compound expression.

Operations

In most expressions, you also specify an operation on the data that the prefix identifies. For example, suppose that you specify the following prefix:

```
http.req.url
```

This prefix extracts URLs in HTTP requests. This expression prefix does not require any operators to be used in an expression. However, when you configure an expression that processes HTTP request URLs, you can specify operations that analyze particular characteristics of the URL. Following are a few possibilities:

- Search for a particular host name in the URL.
- Search for a particular path in the URL.
- Evaluate the length of the URL.
- Search for a string in the URL that indicates a time stamp and convert it to GMT.

The following is an example of a prefix that identifies an HTTP header named Server and an operation that searches for the string IIS in the header value:

```
http.res.header("Server").contains("IIS")
```

Following is an example of a prefix that identifies host names and an operation that searches for the string “www.mycompany.com” as the value of the name:

```
http.req.hostname.eq("www.mycompany.com")
```

Basic Operations on Expression Prefixes

The following table describes a few of the basic operations that can be performed on expression prefixes.

Table 1. Basic Operations for Expressions

Operation	Determines Whether or Not
`CONTAINS(<string>)`	The object matches <string>. Following is an example: `http.req.header("Cache-Control").contains("no-cache")`
`EXISTS`	A particular item is present in an object. Following is an example: `http.res.header("MyHdr").exists`
`EQ(<text>)`	A particular non-numeric value is present in an object. Following is an example: `http.req.method.eq(post)`
`EQ(<integer>)`	A particular numeric value is present in an object. Following is an example: `client.ip.dst.eq(10.100.10.100)`
`LT(<integer>)`	An object's value is less than a particular value. Following is an example: `http.req.content_length.lt(5000)`
`GT(<integer>)`	An object's value is greater than a particular value. Following is an example: `http.req.content_length.gt(5)`

The following table summarizes a few of the available types of operations.

Table 2. Basic Types of Operations

Operation Type	Description

Text operations	Match individual strings and sets of strings with any portion of a target. The target can be an entire string, the start of a string, or any portion of text in between the start and the end of the string. For example, you can extract the string "XYZ" from "XYZSomeText". Or, you can compare an HTTP header value with an array of different strings. You can also transform text into another type of data. Following are examples: · Transform a string into an integer value · Create a list from the query strings in a URL · Transform a string into a time value
Numeric operations	Numeric operations include applying arithmetic operators, evaluating content length, the number of items in a list, dates, times, and IP addresses.

Compound Default Syntax Expressions

You can configure a default syntax expression that contains Boolean or arithmetic operators and multiple atomic operations. The following compound expression contains a boolean AND:

```
http.req.hostname.eq("mycompany.com") && http.req.method.eq(post)
```

The following expression adds the value of two targets, and compares the result to a third value:

```
http.req.url.length + http.req.cookie.length <= 500
```

A compound expression can contain any number of logical and arithmetic operators. The following expression evaluates the length of an HTTP request on the basis of its URL and cookie, evaluates text in the header, and performs a Boolean AND on these two results:

```
http.req.url.length + http.req.cookie.length <= 500 &&
http.req.header.contains("some text")
```

You can use parentheses to control the order of evaluation in a compound expression.

Booleans in Compound Expressions

You configure compound expressions with the following operators:

&&.

This operator is a logical AND. For the expression to evaluate to TRUE, all components that are joined by the And must evaluate to TRUE. Following is an example:

```
http.req.url.hostname.eq("myHost") &&
http.req.header("myHeader").exists
```

||.

This operator is a logical OR. If any component of the expression that is joined by the OR evaluates to TRUE, the entire expression is TRUE.

!.

Performs a logical NOT on the expression.

In some cases, the NetScaler configuration utility offers AND, NOT, and OR operators in the Add Expression dialog box. However, these are of limited use. Citrix recommends that you use the operators &&, ||, and ! to configure compound expressions that use Boolean logic.

Parentheses in Compound Expressions

You can use parentheses to control the order of evaluation of an expression. The following is an example:

```
http.req.url.contains("myCompany.com") ||
(http.req.url.hostname.eq("myHost") &&
http.req.header("myHeader").exists)
```

The following is another example:

```
(http.req.header("Content-Type").exists &&
http.req.header("Content-Type").eq("text/html")) ||
(http.req.header("Transfer-Encoding").exists ||
http.req.header("Content-Length").exists)
```

Compound Operations for Strings

The following table describes operators that you can use to configure compound operations on string data.

Table 1. String-Based Operations for Compound Default Syntax Expressions

All string operations	
Operations that produce a string value	
str + str	Concatenates the value of the expression on the left of the operator with the value on the right. Following is an example: `http.req.hostname + http.req.url.protocol`
str + num	Concatenates the value of the expression on the left of the operator with a numeric value on the right. Following is an example: `http.req.hostname + http.req.url.content_length`
num + str	Concatenates the numeric value of the expression on the left side of the operator with a string value on the right. Following is an example: `http.req.url.content_length + http.req.url.hostname`
str + ip	Concatenates the string value of the expression on the left side of the operator with an IP address value on the right. Following is an example: `http.req.hostname + 10.00.000.00`
ip + str	Concatenates the IP address value of the expression on the left of the operator with a string value on the right.Following is an example: `client.ip.dst + http.req.url.hostname`
str1 ALT str2	Uses the string1 or string2 value that is derived from the expression on either side of the operator, as long as neither of these expressions is a compound expressions. Following is an example: `http.req.hostname alt client.ip.src`
Operations on strings that produce a result of TRUE or FALSE	

str == str	Evaluates whether the strings on either side of the operator are the same. Following is an example:
	
	`http.req.header("myheader") ==`
	`http.res.header("myheader")`

str <= str	Evaluates whether the string on the left side of the operator is the same as the string on the right, or precedes it alphabetically.
str >= str	Evaluates whether the string on the left side of the operator is the same as the string on the right, or follows it alphabetically.

str < str	Evaluates whether the string on the left side of the operator precedes the string on the right alphabetically.
str > str	Evaluates whether the string on the left side of the operator follows the string on the right alphabetically.
str !!= str	Evaluates whether the strings on either side of the operator are different.
Logical operations on strings	

bool && bool	This operator is a logical AND. When evaluating the components of the compound expression, all components that are joined by the AND must evaluate to TRUE. Following is an example:
	
	`http.req.method.eq(GET) &&`
	`http.req.url.query.contains("viewReport && my_pagelabel")`

bool || bool	This operator is a logical OR. When evaluating the components of the compound expression, if any component of the expression that is joined by the OR evaluates to TRUE, the entire expression is TRUE. Following is an example:
	
	`http.req.url.contains(".js") ||`
	`http.res.header.("Content-Type").contains("javascript")`

!bool	`Performs a logical NOT on the expression.`

Compound Operations for Numbers

You can configure compound numeric expressions. For example, the following expression returns a numeric value that is the sum of an HTTP header length and a URL length:

```
http.req.header.length + http.req.url.length
```

The following tables describes operators that you can use to configure compound expressions for numeric data.

Table 1. Arithmetic Operations on Numbers

Operator	Description
num + num	Add the value of the expression on the left of the operator to the value of the expression on the right. Following is an example: `http.req.content_length + http.req.url.length`
num – num	Subtract the value of the expression on the right of the operator from the value of the expression on the left.
num * num	Multiply the value of the expression on the left of the operator with the value of the expression on the right. Following is an example: `client.interface.rxthroughput * 9`
num / num	Divide the value of the expression on the left of the operator by the value of the expression on the right.
num % num	Calculate the modulo, or the numeric remainder on a division of the value of the expression on the left of the operator by the value of the expression on the right. For example, the values "15 mod 4" equals 3, and "12 mod 4" equals 0.
~number	Returns a number after applying a bitwise logical negation of the number. The following example assumes that numeric.expression returns 12 (binary 1100): `~numeric.expression.` The result of applying the ~ operator is -11 (a binary 1110011, 32 bits total with all ones to the left). Note that all returned values of less than 32 bits before applying the operator implicitly have zeros to the left to make them 32 bits wide.

number ^ number	Compares two bit patterns of equal length and performs an XOR operation on each pair of corresponding bits in each number argument, returning 1 if the bits are different, and 0 if they are the same. Returns a number after applying a bitwise XOR to the integer argument and the current number value. If the values in the bitwise comparison are the same, the returned value is a 0. The following example assumes that numeric.expression1 returns 12 (binary 1100) and numeric.expression2 returns 10 (binary 1010): `numeric.expression1 ^ numeric.expression2` The result of applying the ^ operator to the entire expression is 6 (binary 0110). Note that all returned values of less than 32 bits before applying the operator implicitly have zeros to the left to make them 32 bits wide.
number | number	Returns a number after applying a bitwise OR to the number values. If either value in the bitwise comparison is a 1, the returned value is a 1. The following example assumes that numeric.expression1 returns 12 (binary 1100) and numeric.expression2 returns 10 (binary 1010): `numeric.expression1 | numeric.expression2` The result of applying the | operator to the entire expression is 14 (binary 1110). Note that all returned values of less than 32 bits before applying the operator implicitly have zeros to the left to make them 32 bits wide.
number & number	Compares two bit patterns of equal length and performs a bitwise AND operation on each pair of corresponding bits, returning 1 if both of the bits contains a value of 1, and 0 if either bits are 0. The following example assumes that numeric.expression1 returns 12 (binary 1100) and numeric.expression2 returns 10 (binary 1010): `numeric.expression1 & numeric.expression2` The whole expression evaluates to 8 (binary 1000). Note that all returned values of less than 32 bits before applying the operator implicitly have zeros to the left to make them 32 bits wide.

num << num	Returns a number after a bitwise left shift of the number value by the right-side number argument number of bits. Note that the number of bits shifted is integer modulo 32. The following example assumes that numeric.expression1 returns 12 (binary 1100) and numeric.expression2 returns 3: `numeric.expression1 << numeric.expression2` The result of applying the LSHIFT operator is 96 (a binary 1100000). Note that all returned values of less than 32 bits before applying the operator implicitly have zeros to the left to make them 32 bits wide.
num >> num	Returns a number after a bitwise right shift of the number value by the integer argument number of bits. Note that the number of bits shifted is integer modulo 32. The following example assumes that numeric.expression1 returns 12 (binary 1100) and numeric.expression2 returns 3: `numeric.expression1 >> numeric.expression2` The result of applying the RSHIFT operator is 1 (a binary 0001). Note that all returned values of less than 32 bits before applying the operator implicitly have zeros to the left to make them 32 bits wide.

Table 2. Numeric Operators That Produce a Result of TRUE or FALSE

Operator	Description
num == num	Determine if the value of the expression on the left of the operator is equal to the value of the expression on the right.
num != num	Determine if the value of the expression on the left of the operator is not equal to the value of the expression on the right.
num > num	Determine if the value of the expression on the left of the operator is greater than the value of the expression on the right.
num < num	Determine if the value of the expression on the left of the operator is less than the value of the expression on the right.
num >= num	Determine if the value of the expression on the left of the operator is greater than or equal to the value of the expression on the right.
num <= num	Determine if the value of the expression on the left of the operator is less than or equal to the value of the expression on the right

Functions for Data Types in the Policy Infrastructure

The NetScaler policy infrastructure supports the following numeric data types:

- Integer (32 bits)
- Unsigned long (64 bits)
- Double (64 bits)

Simple expressions can return all of these data types. Therefore, you can create compound expressions that use arithmetic operators and logical operators to evaluate or return values of these data types. Additionally, you can use all of these values in policy expressions. Literal constants of type unsigned long can be specified by appending the string `ul` to the number. Literal constants of type double contain a period (.), an exponent, or both.

Arithmetic Operators, Logical Operators, and Type Promotion

In compound expressions, the following standard arithmetic and logical operators can be used for the double and unsigned long data types:

- +, -, *, and /
- %, ~, ^, &, |, <<, and >> (do not apply to double)
- ==, !=, >, <, >=, and <=

All of these operators have the same meaning as in the C programming language.

In all cases of mixed operations between operands of type integer, unsigned long, and double, type promotion is performed so that the operation can be performed on operands of the same type. A type of lower precedence is automatically promoted to the type of the operand with the highest precedence involved in the operation. The order of precedence (higher to lower) is as follows:

- Double
- Unsigned long
- Integer

Therefore, an operation that returns a numeric result returns a result of the highest type involved in the operation.

For example, if the operands are of type integer and unsigned long, the integer operand is automatically converted to type unsigned long. This type conversion is performed even in simple expressions in which the type of data identified by the expression prefix does not match the type of data that is passed as the argument to the function. To illustrate such an example, in the operation `HTTP.REQ.CONTENT_LENGTH.DIV(3ul)`, the integer returned by the prefix `HTTP.REQ.CONTENT_LENGTH` is automatically converted to unsigned long (the type of the data passed as the argument to the `DIV()` function), and an unsigned long

division is performed. Similarly, the argument can be promoted in an expression. For example, `HTTP.REQ.HEADER("myHeader").TYPECAST_DOUBLE_AT.DIV(5)` promotes the integer `5` to type double and performs double-precision division.

The following table describes the arithmetic and Boolean functions that can be used with the integer, unsigned long, and double data types. For information about expressions for casting data of one type to data of another type, see "Typecasting Data."

Function	Description
`<prefix>.ADD(<integer>|<unsigned long>|<double>)`	Adds the argument to the value of the expression prefix and returns the result **Example:** `http.req.content_length.add(10)`
`<prefix>.SUB(<integer>|<unsigned long>|<double>)`	Subtracts the argument from the value of the prefix and returns the result. **Example:** `http.req.header.length.sub(10)`
`<prefix>.DIV(<integer>|<unsigned long>|<double>)`	Divides the value of the prefix by the argument and returns the quotient. **Example:** `http.req.content_length.div(2)`
`<prefix>.MUL(<integer>|<unsigned long>|<double>)`	Multiplies the value of the prefix by the argument and returns the product. **Example:** `http.req.content_length.mul(2)`
`<prefix>.BETWEEN(<lower_integer>, <higher_integer>|<lower_unsigned_long, higher_unsigned_long>|<lower_double>, <higher_double>)`	Returns a Boolean `TRUE` if the value of the prefix is greater than or equal to t value argument and less than or equal to the higher value argument. **Example:** `http.req.content_length.between(5, 500)`
`<prefix>.EQ(<integer>|<unsigned long>|<double>)`	Returns a Boolean `TRUE` if the value of the prefix is equal to the argument. **Example:** `http.req.content_length.eq(50)`
`<prefix>.NE(<integer>|<unsigned long>|<double>)`	Returns a Boolean `TRUE` if the value of the prefix is not equal to the argumen **Example:** `http.req.content_length.ne(50)`
`<prefix>.GE(<integer>|<unsigned long>|<double>)`	Returns a Boolean `TRUE` if the value of the prefix is greater than or equal to t argument. **Example:** `http.req.content_length.ge(500)`

<prefix>.GT(<integer>|<unsigned long>|<double>)	Returns a Boolean TRUE if the value of the prefix is greater than the argumen **Example:** http.req.content_length.gt(500)
<prefix>.LE(<integer>|<unsigned long>|<double>)	Returns a Boolean TRUE if the value of the prefix is less than or equal to the argument. **Example:** http.req.content_length.le(5)
<prefix>.LT(<integer>|<unsigned long>|<double>)	Returns a Boolean TRUE if the value of the prefix is less than the argument. **Example:** http.req.content_length.lt(5)
<prefix>.NEG	Returns the negative of the value of the prefix. This function cannot be used v prefix that returns data of type unsigned long. **Example:** http.req.content_length.neg If the content length is 30 characters, the NEG function in the above example value of ▫30.
<prefix>.BITAND(<integer>|<unsigned long>)	Returns the result of a bitwise AND operation performed on the binary equiva the argument and the value returned by the prefix. The bitwise AND operation operates on each pair of corresponding bits in the bit strings. The operation returns 1 only if both bits are equal to 1. If either bi if both bits are 0, the operation returns 0. If the binary equivalent of an opera contains fewer than 32 bits, the function implicitly adds leading zeros to make operand 32 bits wide before performing the operation. The BITAND function be used with the double data type. **Example:** http.req.header (\"test\").contains_index(\"patternset1\").bitand(4) In the above example, assume that the index returned by the CONTAINS_IND pattern set function is an integer value of 12. The BITAND function performs AND operation between the binary value of 12, which is 00000000000000000000000000001100 (32 bits wide) and the binary value of 4, 00000000000000000000000000001100 (32 bits wide). The resulting bit string th function returns is 00000000000000000000000000000100, whose decimal equiv 4. An ampersand (&) performs a similar function to BITAND but takes two expre operands rather than an expression (the prefix) and the argument.

<prefix>.BITNEG	Returns the value that results from a bitwise negation of the value of the pref data type of the value that is returned is the same as that of the value that wo otherwise be returned by the prefix. This function cannot be used with a prefi returns data of type double. If the binary equivalent of an operand contains fe 32 bits, the function implicitly adds leading zeros to make the operand 32 bits before performing the operation. **Example:** http.req.header(\"test\").contains_index(\"patternset1\").b In the above example, assume that the index returned by the CONTAINS_IND pattern set function is an integer value of 12, whose binary value is 00000000000000000000000000001100 (32 bits wide). The BITNEG function ret 11111111111111111111111111110011, which represents an integer value of - 1 A tilde (~) performs a similar function to that of BITNEG but takes another ex as an argument, instead of operating on an integer prefix expression.
<prefix>.BITOR(<integer>|<unsigned long>)	Returns the result of a bitwise OR operation performed on the value of the pr the argument. The function returns 1 if either or both bits in a corresponding set to 1. If both bits are 0, the function returns 0. The BITOR function cannot with the double data type. If the binary equivalent of an operand contains few 32 bits, the function implicitly adds leading zeros to make the operand 32 bits before performing the operation. **Example:** http.req.header (\"test\").contains_index(\"patternset1\").bitor(7) In the above example, assume that the index returned by the CONTAINS_IND pattern set function is an integer value of 9. The BITOR function performs a bi operation on the binary value of 9, which is 0000000000000000000000000000100 bits wide), and the binary value of 7, which is 0000000000000000000000000000000 bits wide). The function returns 00000000000000000000000000001111, which represents an integer value of 15. The pipe (|) performs a similar function to that of BITOR but takes two expre operands rather than an integer or unsigned long (the argument to the functio expression prefix.

<prefix>.BITXOR(<integer>|<unsigned long>)	Returns the result of a bitwise EXLUSIVE-OR (XOR) operation performed on t of the prefix and the value of the argument. If the values of a pair of correspo bits are the same, the function returns 0. If the bits do not have the same valu function returns 1. If the binary equivalent of an operand contains fewer than the function implicitly adds leading zeros to make the operand 32 bits wide be performing the operation. The BITXOR function cannot be used with the doub type. **Example:** `http.req.header (\"test\").contains_index(\"patternset1\").bitxor(8)` In the above example, assume that the index returned by the CONTAINS_IND pattern set function is an integer value of 15. The BITOR function performs a XOR operation on the binary value of 15, which is 00000000000000000000000000 (32 bits wide), and the binary value of 8, which is 00000000000000000000000000 (32 bits wide). The function returns 00000000000000000000000000000111, whi represents an integer value of 7. A caret (^) performs a similar function to that of BITXOR but takes two expre operands rather than an expression and an argument.
<prefix>.LSHIFT(<integer>|<unsigned long>)	Returns the result of a bitwise left shift operation on the value of the prefix. T number of shifts is <integer> modulo 32. Each leftward shift effectively mu the value of the prefix by 2. If the binary equivalent of an operand contains fe 32 bits, the function implicitly adds leading zeros to make the operand 32 bits before performing the operation. This function cannot be used with a prefix th returns data of type double. **Example:** `http.req.header (\"test\").contains_index(\"pat1\").lshift(` Assume that the index that is returned by the CONTAINS_INDEX operator is 1 left shift operator drops the two leftmost bits in the binary value of 10, which 00000000000000000000000000001010 (32 bits wide), and adds two zeros to the The result is 00000000000000000000000000101000, which represents a decima 40. A double less-than (<<) performs a similar function to that of LSHIFT but tak expressions as operands, instead of an expression and an argument.

`<prefix>.RSHIFT(<integer>|<unsigned long>)`	Returns the result of a bitwise right shift operation on the value of the prefix. number of shifts is `<integer>` modulo 32. Each rightward shift effectively di value of the prefix by 2. If the binary equivalent of an operand contains less th bits, the function implicitly adds leading zeros before performing the operatio make the operand 32 bits wide. This function cannot be used with a prefix tha data of type double. **Example:** `http.req.header (\"test\").contains_index(\"pat1\").Rshift(` Assume that the index that is returned by the `CONTAINS_INDEX` operator is 3 left shift operator drops the two rightmost bits in the binary value of 320, whi 00000000000000000000000101000000 (32 bits wide), and adds two zeros to the The result is 00000000000000000000000001010000, which represents an intege of 80. A double greater-than (>>) performs the same function as `RSHIFT` but takes t expressions as operands, instead of an expression and an argument.
`<prefix>.MOD(<integer>|<unsigned long>)`	Divides the value returned by the preceding function by its argument and retu remainder. The argument must be a non-zero value.

Specifying the Character Set in Expressions

The policy infrastructure on the Citrix® NetScaler® appliance supports the ASCII and UTF-8 character sets. The default character set is ASCII. If the traffic for which you are configuring an expression consists of only ASCII characters, you need not specify the character set in the expression. However, you must specify the character set in every simple expression that is meant for UTF-8 traffic. To specify the UTF-8 character set in a simple expression, you must include the `SET_CHAR_SET(<charset>)` function, with `<charset>` specified as UTF_8, as shown in the following examples:

```
HTTP.REQ.BODY(10).SET_CHAR_SET(UTF_8).CONTAINS("ß")

HTTP.RES.BODY(100).SET_CHAR_SET(UTF_8).BEFORE_STR("Bücher").AFTER_STR
("Wörterbuch")
```

In an expression, the `SET_CHAR_SET()` function must be introduced at the point in the expression after which data processing must be carried out in the specified character set. For example, in the expression `HTTP.REQ.BODY(1000).AFTER_REGEX(re/following example/).BEFORE_REGEX(re/In the preceding example/).CONTAINS_ANY("Greek_ alphabet")`, if the strings stored in the pattern set "Greek_alphabet" are in UTF-8, you must include the `SET_CHAR_SET(UTF_8)` function immediately before the `CONTAINS_ANY("<string>")` function, as follows:

```
HTTP.REQ.BODY(1000).AFTER_REGEX(re/following
example/).BEFORE_REGEX(re/In the preceding
example/).SET_CHAR_SET(UTF_8).CONTAINS_ANY("Greek_ alphabet")
```

The `SET_CHAR_SET()` function sets the character set for all further processing (that is, for all subsequent functions) in the expression unless it is overridden later in the expression by another `SET_CHAR_SET()` function that changes the character set. Therefore, if all the functions in a given simple expression are intended for UTF-8, you can include the `SET_CHAR_SET(UTF_8)` function immediately after functions that identify text (for example, the `HEADER("<name>")` or `BODY(<int>)` functions). In the second example that follows the first paragraph above, if the ASCII arguments passed to the `AFTER_REGEX()` and `BEFORE_REGEX()` functions are changed to UTF-8 strings, you can include the `SET_CHAR_SET(UTF_8)` function immediately after the `BODY(1000)` function, as follows:

```
HTTP.REQ.BODY(1000).SET_CHAR_SET(UTF_8).AFTER_REGEX(re/Bücher/).BEFOR
E_REGEX(re/Wörterbuch/).CONTAINS_ANY("Greek_alphabet")
```

The UTF-8 character set is a superset of the ASCII character set, so expressions configured for the ASCII character set continue to work as expected if you change the character set to UTF-8.

Compound Expressions with Different Character Sets

In a compound expression, if one subset of expressions is configured to work with data in the ASCII character set and the rest of the expressions are configured to work with data in the UTF-8 character set, the character set specified for each individual expression is considered when the expressions are evaluated individually. However, when processing the compound expression, just before processing the operators, the appliance promotes the character set of the returned ASCII values to UTF-8. For example, in the following compound expression, the first simple expression evaluates data in the ASCII character set while the second simple expression evaluates data in the UTF-8 character set:

```
HTTP.REQ.HEADER("MyHeader") == HTTP.REQ.BODY(10).SET_CHAR_SET(UTF_8)
```

However, when processing the compound expression, just before evaluating the "is equal to" Boolean operator, the NetScaler appliance promotes the character set of the value returned by `HTTP.REQ.HEADER("MyHeader")` to UTF-8.

The first simple expression in the following example evaluates data in the ASCII character set. However, when the NetScaler appliance processes the compound expression, just before concatenating the results of the two simple expressions, the appliance promotes the character set of the value returned by `HTTP.REQ.BODY(10)` to UTF-8.

```
HTTP.REQ.BODY(10) + HTTP.REQ.HEADER("MyHeader").SET_CHAR_SET(UTF_8)
```

Consequently, the compound expression returns data in the UTF-8 character set.

Specifying the Character Set Based on the Character Set of Traffic

You can set the character set to UTF-8 on the basis of traffic characteristics. If you are not sure whether the character set of the traffic being evaluated is UTF-8, you can configure a compound expression in which the first expression checks for UTF-8 traffic and subsequent expressions set the character set to UTF-8. Following is an example of a compound expression that first checks the value of "charset" in the request's Content-Type header for "UTF-8" before checking whether the first 1000 bytes in the request contain the UTF-8 string `Bücher`:

```
HTTP.REQ.HEADER("Content-Type").SET_TEXT_MODE(IGNORECASE).TYPECAST_NV
LIST_T('=', '; ', '"').VALUE("charset").EQ("UTF-8") &&
HTTP.REQ.BODY(1000).SET_CHAR_SET(UTF_8).CONTAINS("Bücher")
```

If you are sure that the character set of the traffic being evaluated is UTF-8, the second expression in the example is sufficient.

Character and String Literals in Expressions

During expression evaluation, even if the current character set is ASCII, character literals and string literals, which are enclosed in single quotation marks (') and quotation marks (""), respectively, are considered to be literals in the UTF-8 character set. In a given expression, if a function is operating on character or string literals in the ASCII character set and you include a non-ASCII character in the literal, an error is returned.

Values in Hexadecimal and Octal Formats

When configuring an expression, you can enter values in octal and hexadecimal formats. However, each hexadecimal or octal byte is considered a UTF-8 byte. Invalid UTF-8 bytes result in errors regardless of whether the value is entered manually or pasted from the clipboard. For example, "\xce\x20" is an invalid UTF-8 character because "c8" cannot be followed by "20" (each byte in a multi-byte UTF-8 string must have the high bit set). Another example of an invalid UTF-8 character is "\xce \xa9," since the hexadecimal characters are separated by a white-space character.

Functions That Return UTF-8 Strings

Only the `<text>.XPATH` and `<text>.XPATH_JSON` functions always return UTF-8 strings. The following MYSQL routines determine at runtime which character set to return, depending on the data in the protocol:

- `MYSQL_CLIENT_T.USER`
- `MYSQL_CLIENT_T.DATABASE`
- `MYSQL_REQ_QUERY_T.COMMAND`
- `MYSQL_REQ_QUERY_T.TEXT`
- `MYSQL_REQ_QUERY_T.TEXT(<unsigned int>)`
- `MYSQL_RES_ERROR_T.SQLSTATE`
- `MYSQL_RES_ERROR_T.MESSAGE`
- `MYSQL_RES_FIELD_T.CATALOG`
- `MYSQL_RES_FIELD_T.DB`
- `MYSQL_RES_FIELD_T.TABLE`
- `MYSQL_RES_FIELD_T.ORIGINAL_TABLE`
- `MYSQL_RES_FIELD_T.NAME`
- `MYSQL_RES_FIELD_T.ORIGINAL_NAME`
- `MYSQL_RES_OK_T.MESSAGE`
- `MYSQL_RES_ROW_T.TEXT_ELEM(<unsigned int>)`

Terminal Connection Settings for UTF-8

When you set up a connection to the NetScaler appliance by using a terminal connection (by using PuTTY, for example), you must set the character set for transmission of data to UTF-8.

Classic Expressions in Default Syntax Expressions

Classic expressions describe basic characteristics of traffic. In some cases, you may want to use a classic expression in a default syntax expression. You can do so with the default syntax expression configuration tool. This can be helpful when manually migrating the older classic expressions to the default syntax.

Note that when you upgrade the NetScaler to version 9.0 or higher, Integrated Caching policies are automatically upgraded to default syntax policies, and the expressions in these policies are upgraded to the default syntax.

The following is the syntax for all default syntax expressions that use a classic expression:

```
SYS.EVAL_CLASSIC_EXPR("expression")
```

Following are examples of the `SYS.EVAL_CLASSIC_EXPR("expression")` expression:

```
sys.eval_classic_expr("req.ssl.client.cipher.bits > 1000")
sys.eval_classic_expr("url contains abc")
sys.eval_classic_expr("req.ip.sourceip == 10.102.1.61 -netmask 255.255.255.255")
sys.eval_classic_expr("time >= *:30:00GMT")
sys.eval_classic_expr("e1 || e2")
sys.eval_classic_expr("req.http.urllen > 50")
sys.eval_classic_expr("dayofweek == wedGMT")
```

Configuring Default Syntax Expressions in a Policy

You can configure a default syntax expression of up to 1,499 characters in a policy. The user interface for default syntax expressions depends to some extent on the feature for which you are configuring the expression, and on whether you are configuring an expression for a policy or for another use.

When configuring expressions on the command line, you delimit the expression by using quotation marks (“. . .” or '. . .'). Within an expression, you escape additional quotation marks by using a back-slash (\). For example, the following are standard methods for escaping quotation marks in an expression:

```
"\"abc\""
```

```
‘\"abc\"’
```

You must also use a backslash to escape question marks and other backslashes on the command line. For example, the expression `http.req.url.contains(“\?”)` requires a backslash so that the question mark is parsed. Note that the backslash character will not appear on the command line after you type the question mark. On the other hand, if you escape a backslash (for example, in the expression `'http.req.url.contains("\\\\http")'`), the escape characters are echoed on the command line.

To make an entry more readable, you can escape the quotation marks for an entire expression. At the start of the expression you enter the escape sequence “q” plus one of the following special characters: `/{<|~$^+=&%@`?`.

You enter only the special character at the end of the expression, as follows:

```
q@http.req.url.contains("sometext") && http.req.cookie.exists@
```

```
q~http.req.url.contains("sometext") && http.req.cookie.exists~
```

Note that an expression that uses the { delimiter is closed with }.

For some features (for example, Integrated Caching and Responder), the policy configuration dialog box provides a secondary dialog box for configuring expressions. This dialog enables you to choose from drop-down lists that show the available choices at each point during expression configuration. You cannot use arithmetic operators when using these configuration dialogs, but most other default syntax expression features are available. To use arithmetic operators , write your expressions in free-form format.

To configure a default syntax rule by using the command line interface

At the command prompt, type the following commands to configure a default syntax rule and verify the configuration:

1. `add cache|dns|rewrite|cs policy policyName` **`-rule`** `expression featureSpecificParameters` **`-action`**

2. `show cache|dns|rewrite|cs policy policyName`
   Following is an example of configuring a caching policy:

   Example

   > add cache policy pol-cache -rule http.req.content_length.le(5) -action INVAL
   Done

   > show cache policy pol-cache
   Name: pol-cache
   Rule: http.req.content_length.le(5)
   CacheAction: INVAL
   Invalidate groups: DEFAULT
   UndefAction: Use Global
   Hits: 0
   Undef Hits: 0

   Done

To configure a default syntax policy expression by using the configuration utility

1. In the navigation pane, click the name of the feature where you want to configure a policy, for example, you can select Integrated Caching, Responder, DNS, Rewrite, or Content Switching, and then click Policies.

2. Click Add.

3. For most features, click in the Expression field. For Content Switching, click Configure.

4. Click the Prefix icon (the house) and select the first expression prefix from the drop-down list. For example, in Responder, the options are HTTP, SYS, and CLIENT. The next set of applicable options appear in a drop-down list.

5. Double-click the next option to select it, and then type a period (.). Again, a set of applicable options appears in another drop-down list.

6. Continue selecting options until an entry field (signalled by parentheses) appears. When you see an entry field, enter an appropriate value in the parentheses. For example, if you select GT(int) (greater-than, integer format), you specify an integer in the parentheses. Text strings are delimited by quotation marks. Following is an example:

   ```
   HTTP.REQ.BODY(1000).BETWEEN("this","that")
   ```

7. To insert an operator between two parts of a compound expression, click the Operators icon (the sigma), and select the operator type. Following is an example of a configured expression with a Boolean OR (signalled by double vertical bars, ||):

   ```
   HTTP.REQ.URL.EQ("www.mycompany.com")||HTTP.REQ.BODY(1000).BETWEEN(
   "this","that")
   ```

8. To insert a named expression, click the down arrow next to the Add icon (the plus sign) and select a named expression.

9. To configure an expression using drop-down menus, and to insert built-in expressions, click the Add icon (the plus sign). The Add Expression dialog box works in a similar way to the main dialog box, but it provides drop-down lists for selecting options, and it provides text fields for data entry instead of parentheses. This dialog box also provides a Frequently Used Expressions drop-down list that inserts commonly used expressions. When you are done adding the expression, click OK.

10. When finished, click Create. A message in the status bar indicates that the policy expression is configured successfully.

To test a default syntax expression by using the configuration utility

1. In the navigation pane, click the name of the feature for which you want to configure a policy (for example, you can select Integrated Caching, Responder, DNS, Rewrite, or Content Switching), and then click Policies.

2. Select a policy and click Open.

3. To test the expression, click the Evaluate icon (the check mark).

4. In the expression evaluator dialog box, select the Flow Type that matches the expression.

5. In the HTTP Request Data or HTTP Response Data field, paste the HTTP request or response that you want to parse with the expression, and click Evaluate. Note that you must supply a complete HTTP request or response, and the header and body should be separated by blank line. Some programs that trap HTTP headers do not also trap the response. If you are copying and pasting only the header, insert a blank line at the end of the header to form a complete HTTP request or response.

6. Click Close to close this dialog box.

Configuring Named Default Syntax Expressions

Instead of retyping the same expression multiple times in multiple policies, you can configure a named expression and refer to the name any time you want to use the expression in a policy. For example, you could create the following named expressions:

ThisExpression:

```
http.req.body(100).contains("this")
```

ThatExpression:

```
http.req.body(100).contains("that")
```

You can then use these named expressions in a policy expression. For example, the following is a legal expression based on the preceding examples:

```
ThisExpression || ThatExpression
```

You can use the name of a default syntax expression as the prefix to a function. The named expression can be either a simple expression or a compound expression. The function must be one that can operate on the type of data that is returned by the named expression.

Example 1: Simple Named Expression as a Prefix

The following simple named expression, which identifies a text string, can be used as a prefix to the AFTER_STR("<string>")function, which works with text data:

```
HTTP.REQ.BODY(1000)
```

If the name of the expression is top1KB, you can use top1KB.AFTER_STR("username") instead of HTTP.REQ.BODY(1000).AFTER_STR("username").

Example 2: Compound Named Expression as a Prefix

You can create a compound named expression called basic_header_value to concatenate the user name in a request, a colon (:), and the user's password, as follows:

```
add policy expression basic_header_value "HTTP.REQ.USER.NAME + \":\"
+ HTTP.REQ.USER.PASSWD"
```

You can then use the name of the expression in a rewrite action, as shown in the following example:

```
add rewrite action insert_b64encoded_authorization insert_http_header
authorization '"Basic " + basic_header_value.b64encode'
-bypassSafetyCheck YES
```

In the example, in the expression that is used to construct the value of the custom header, the B64 encoding algorithm is applied to the string returned by the compound named expression.

You can also use a named expression (either by itself or as a prefix to a function) to create the text expression for the replacement target in a rewrite.

To configure a named default syntax expression by using the command line interface

At the command prompt, type the following commands to configure a named expression and verify the configuration:

- add policy expression <name><value>
- show policy expression <name>

Example

```
> add policy expression myExp "http.req.body(100).contains(\"the other\")"
 Done

> show policy expression myExp
1)      Name: myExp  Expr: "http.req.body(100).contains("the other")"  Hits: 0 Type : ADVANCED
 Done
```

The expression can be up to 1,499 characters.

To configure a named expression by using the configuration utility

1. In the navigation pane, expand AppExpert, and then click Expressions.
2. Click Advanced Expressions.
3. Click Add.
4. Enter a name and a description for the expression.
5. Configure the expression by using the process described in "To configure a default syntax policy expression by using the configuration utility." A message in the status bar indicates that the policy expression is configured successfully.

Configuring Default Syntax Expressions Outside the Context of a Policy

A number of functions, including the following, can require a default syntax expression that is not part of a policy:

Integrated Caching selectors:

You define multiple non-compound expressions (selectlets) in the definition of the selector. Each selectlet is in an implicit logical AND relationship with the others.

Load Balancing:

You configure an expression for the TOKEN method of load balancing for a load balancing virtual server.

Rewrite actions:

Expressions define the location of the rewrite action and the type of rewriting to be performed, depending on the type of rewrite action that you are configuring. For example, a DELETE action only uses a target expression. A REPLACE action uses a target expression and an expression to configure the replacement text.

Rate-based policies:

You use default syntax expressions to configure Limit Selectors. You can use these selectors when configuring policies to throttle the rate of traffic to various servers. You define up to five non-compound expressions (selectlets) in the definition of the selector. Each selectlet is in an implicit logical AND with the others.

To configure a default syntax expression outside a policy by using the command line interface (cache selector example)

At the command prompt, type the following commands to configure a default syntax expression outside a policy and verify the configuration:

- add cache selector <selectorName> <rule>
- show cache selector <selectorName>

Example

```
> add cache selector mainpageSelector "http.req.cookie.value(\"ABC_def\")"
"http.req.url.query.value(\"_ghi\")"selector "mainpageSelector" added
```

```
 Done
> show cache selector mainpageSelector
        Name: mainpageSelector
        Expressions:
                1) http.req.cookie.value("ABC_def")
                2) http.req.url.query.value("_ghi")
 Done
```

Following is an equivalent command that uses the more readable q delimiter, as described in "Configuring Default Syntax Expressions in a Policy":

```
> add cache selector mainpageSelector2 q~http.req.cookie.value("ABC_def")~
q~http.req.url.query.value("_ghi")~selector "mainpageSelector2" added
 Done
> show cache selector mainpageSelector2
        Name: mainpageSelector2
        Expressions:
                1) http.req.cookie.value("ABC_def")
                2) http.req.url.query.value("_ghi")
 Done
```

ns-pi-Adv-exp-eval-txt-wrapper-con

Due to technical difficulties, we are unable to display this topic. Citrix is currently fixing this problem. In the meantime, you can view this topic online:

http://support.citrix.com/proddocs/index.jsp?lang=en&topic=/ns-main-appexpert-10-map/ns-pi-Adv-exp-eval-txt-wrapper-con.html

About Text Expressions

You can configure various expressions for working with text that flows through the NetScaler appliance. Following are some examples of how you can parse text by using a default syntax expression:

- Determine that a particular HTTP header exists.

  For example, you may want to identify HTTP requests that contains a particular Accept-Language header for the purpose of directing the request to a particular server.

- Determine that a particular HTTP URL contains a particular string.

  For example, you may want to block requests for particular URLs. Note that the string can occur at the beginning, middle, or end of another string.

- Identify a POST request that is directed to a particular application.

  For example, you may want to identify all POST requests that are directed to a database application for the purpose of refreshing cached application data.

Note that there are specialized tools for viewing the data stream for HTTP requests and responses. For example, from the following URL, you can download a Firefox Web browser plug-in that displays HTTP request and response headers:

"https://addons.mozilla.org/en-US/firefox/addon/3829"

The following plug-in displays headers, query strings, POST data, and other information:

"https://addons.mozilla.org/en-US/firefox/addon/6647"

After you download these plug-ins, they are accessible from the Firefox Tools menu.

About Operations on Text

A text-based expression consists of at least one prefix to identify an element of data and usually (although not always) an operation on that prefix. Text-based operations can apply to any part of a request or a response. Basic operations on text include various types of string matches.

For example, the following expression compares a header value with a string:

```
http.req.header("myHeader").contains("some-text")
```

Following expressions are examples of matching a file type in a request:

```
http.req.url.suffix.contains("jpeg")

http.req.url.suffix.eq("jpeg")
```

In the preceding examples, the contains operator permits a partial match and the eq operator looks for an exact match.

Other operations are available to format the string before evaluating it. For example, you can use text operations to strip out quotes and white spaces, to convert the string to all lowercase, or to concatenate strings.

Note: Complex operations are available to perform matching based on patterns or to convert one type of text format to another type.

For more information, see the following topics:

- "Pattern Sets and Data Sets."
- "Regular Expressions."
- "Typecasting Data."

Compounding and Precedence in Text Expressions

You can apply various operators to combine text prefixes or expressions. For example, the following expression concatenates the returned values of each prefix:

```
http.req.hostname + http.req.url
```

Following is an example of a compound text expression that uses a logical AND. Both components of this expression must be TRUE for a request to match the expression:

```
http.req.method.eq(post) &&
http.req.body(1024).startswith("destination=")
```

Note: For more information on operators for compounding, see "Compound Default Syntax Expressions."

Categories of Text Expressions

The primary categories of text expressions that you can configure are:

- Information in HTTP headers, HTTP URLs, and the POST body in HTTP requests.

  For more information, see "Expression Prefixes for Text in HTTP Requests and Responses."

- Information regarding a VPN or a clientless VPN.

  For more information, see "Expression Prefixes for VPNs and Clientless VPNs."

- TCP payload information.

  For more information about TCP payload expressions, see "Default Syntax Expressions: Parsing HTTP, TCP, and UDP Data."

- Text in a Secure Sockets Layer (SSL) certificate.

For information about text expressions for SSL and SSL certificate data, see "Default Syntax Expressions: Parsing SSL Certificates" and "Expressions for SSL Certificate Dates."

Note: Parsing a document body, such as the body of a POST request, can affect performance. You may want to test the performance impact of policies that evaluate a document body.

Guidelines for Text Expressions

From a performance standpoint, it typically is best to use protocol-aware functions in an expression. For example, the following expression makes use of a protocol-aware function:

```
HTTP.REQ.URL.QUERY
```

The previous expression performs better than the following equivalent expression, which is based on string parsing:

```
HTTP.REQ.URL.AFTER_STR("?")
```

In the first case, the expression looks specifically at the URL query. In the second case, the expression scans the data for the first occurrence of a question mark.

There is also a performance benefit from structured parsing of text, as in the following expression:

```
HTTP.REQ.HEADER("Example").TYPECAST_LIST_T(',').GET(1)
```

(For more information on typecasting, see "Typecasting Data.") The typecasting expression, which collects comma-delimited data and structures it into a list, typically would perform better than the following unstructured equivalent:

```
HTTP.REQ.HEADER("Example").AFTER_STR(",").BEFORE_STR(",")
```

Finally, unstructured text expressions typically have better performance than regular expressions. For example, the following is an unstructured text expression:

```
HTTP.REQ.HEADER("Example").AFTER_STR("more")
```

The previous expression would generally provide better performance than the following equivalent, which uses a regular expression:

```
HTTP.REQ.HEADER("Example").AFTER_REGEX(re/more/)
```

For more information on regular expressions, see "Regular Expressions."

Expression Prefixes for Text in HTTP Requests and Responses

An HTTP request or response typically contains text, such as in the form of headers, header values, URLs, and POST body text. You can configure expressions to operate on one or more of these text-based items in an HTTP request or response.

The following table describes the expression prefixes that you can configure to extract text from different parts of an HTTP request or response.

Table 1. HTTP Expression Prefixes That Return Text

	Description
`nteger>)`	Returns the body of an HTTP request as a multiline text object, up to the character <integer>. There is no maximum value for the body argument, but you should use as small a va values can affect performance. **Note:** Although it is possible to specify this prefix without an integer argument, th
`ME`	Returns the HTTP host name in the first line of the request, if there is one. Otherwi in the last occurrence of the HOST header. Note that there are two similar prefixes that return host names, as follows: · `http.req.url.hostname` only returns the host name from the URL · `http.req.header("Host")` only returns the value from the Host header. To you must typecast this string, as illustrated in the following example: `http.req.header("host").typecast_http_hostname_t` For more information on typecasting, see "Typecasting Data."
`ME. DOMAIN`	Returns the domain name part of the host name. For example, if the host name is w www.myhost.com:8080, the domain is myhost.com. Returns incorrect results if the host name has an IP address. For information on exp "Default Syntax Expressions: IP and MAC Addresses, Throughput, VLAN IDs." All text operations that you specify after this prefix are case insensitive.
`ME. SERVER`	Returns the server name part of the host name. If the host name is www.myhost.co the server is www.myhost.com. All text operations that you specify after this prefix are case insensitive.
	Returns the value of the METHOD in an HTTP request, or matches the method type argument, for example, `http.req.method.eq(get)`. If you enclose the argumen sensitive.

	Returns the HTTP URL.
STNAME	Returns the host name in the HTTP URL. Do not use this prefix in bidirectional policies. Note that there are two similar prefixes that return host names, as follows: · `HTTP.REQ.HOSTNAME` returns the host name from the URL if there is one; oth the last occurrence of the Host header. · `HTTP.REQ.HEADER("Host")` only returns the value from the Host header. To you must typecast this string, as illustrated in the following example: `http.req.header("host").typecast_http_hostname_t` For more information on typecasting, see "Typecasting Data."
STNAME.DOMAIN	Returns the domain name part of the host name. For example, if the host name is w www.myhost.com:8080, the domain is myhost.com. This operation returns incorrect results if the host name has an IP address. For infor addresses, see "Default Syntax Expressions: IP and MAC Addresses, Throughput, VLA All text operations that you specify after this prefix are case insensitive unless expl SET_TEXT_MODE operator.
STNAME.SERVER	Returns the server name part of the host name. For example, if the host name is ww www.myhost.com:8080, the server is www.myhost.com. All text operations that you specify after this prefix are case insensitive.
STNAME.PORT	Returns the port in the host name. The string following and including the first colon value. For example, if the host name is www.mycompany.com:8080, the port is ":80 www.mycompany.com: the port is ":". If the host name is www.mycompany.com, th location just after ".com". If the numerical value in the port is missing, it assumes a default value of 80 or 443
TH	Returns a slash- (/) separated list from the path in a URL. For example, if the URL is http://www.myhost.com/a/b/c/mypage.html?a=1, this p /a/b/c/mypage.html. The expression `http.req.url.path.get(1)` returns "a" from the preceding URL GET operation, see "Expressions for Extracting Segments of URLs."
TH_AND_QUERY	Returns the portion of the URL that follows the host name. For example, if the URL is http://www.myhost.com/a/b/c/mypage.html?a=1, this p /a/b/c/mypage.html?a=1.
OTOCOL	Returns the protocol in the URL. This prefix cannot be used in bidirectional policies. Following is an example: `http.req.hostname + http.req.url.protocol`

ERY	Returns a name-value list, using the delimiters “=” and “&” from the query compon Following is an example: `http.req.url.query.contains("viewReport && my_pagelabel")`
ERY.VALUE	Returns the value from the name-value pair in the argument supplied to this prefix, the query component in the URL. Following is an example: `http.req.url.query.value("action")` The first component that matches the name is selected. The matching process honc NOIGNORECASE text modes. The URLENCODED and the NOURLENCODED text modes
FFIX	Returns the file name suffix in a URL. For example, if the path in the URL is /a/b/c/mypage.html, this suffix selects “htm example: `http.req.url.suffix.contains("jpeg")`
	Returns the AAA user associated with the current HTTP transaction.
XTERNAL_GROUPS	Returns a list of the external groups to which a user belongs. The groups are separa For example, HTTP.REQ.USER.EXTERNAL_GROUPS returns a comma-separated list o which the user belongs.

XTERNAL_GROUPS.IGNORE_EMPTY_ELEMENTS	Ignores the empty elements in the list of external groups to which the user belongs.
	
	If the element delimiter in the list is a comma (","), then the following list has an er
	
	a=10,,b=11, ,c=89
	
	But the element following "b=11" is not considered an empty element.
	
	For example, consider the following header in an HTTP request packet:
	
	Cust_Header : 123,,24, ,15
	
	Then the following expression returns a value of 4:
	
	`HTTP.REQ.HEADER("Cust_Header").TYPECAST_LIST_T(',').  IGNORE_EMP`
	
	The following expression returns a value of 5:
	
	`HTTP.REQ.HEADER("Cust_Header").TYPECAST_LIST_T(',').COUNT.`

XTERNAL_GROUPS(sep)	Returns a list of all the external groups to which the user belongs. The groups are se For example, the following expression gives a list of all the external groups, and the colon (":"): HTTP.REQ.USER.EXTERNAL_GROUPS(':') Parameters: sep - delimiter
ROUPS	Returns a list of the internal and external groups to which the user belongs. The gro (","). In this list, internal groups are listed first, followed by external groups.
ROUPS.IGNORE_EMPTY_ELEMENTS	Ignores the empty elements in the list of groups to which the user belongs. If the element delimiter in the list is a comma (","), then the following list has an er a=10,,b=11, ,c=89 But the element that follows "b=11" is not considered an empty element. For example, consider the following header in an HTTP request packet: Cust_Header : 123,,24, ,15 The following expression returns a value of 4: HTTP.REQ.HEADER("Cust_Header").TYPECAST_LIST_T(','). IGNORE_EMP The following expression returns a value of 5: HTTP.REQ.HEADER("Cust_Header").TYPECAST_LIST_T(',').COUNT
ROUPS(sep)	Returns a list of groups to which the user belongs. The groups in the list are separat the argument. For example, the following expression returns a colon-separated list of all the group HTTP.REQ.USER.GROUPS(':') In this list, internal groups are listed first, followed by external groups. Parameters: sep - delimiter
NTERNAL_GROUPS	Returns a list of internal groups to which the user belongs. The groups are separate For example, the following expression returns a comma-separated list of all the inte belongs. HTTP.REQ.USER.INTERNAL_GROUPS

NTERNAL_GROUPS.IGNORE_EMPTY_ELEMENTS	Ignores the empty elements in the list of internal groups to which the user belongs.
	
	If the element delimiter in the list is a comma (","), then the following list has an er
	
	a=10,,b=11, ,c=89
	
	But the element following "b=11" is not considered an empty element.
	
	For example, consider the following header in an HTTP request packet:
	
	Cust_Header : 123,,24, ,15
	
	The following expression returns a value of 4:
	
	`HTTP.REQ.HEADER("Cust_Header").TYPECAST_LIST_T(',').  IGNORE_EMP`
	
	The following expression returns a value of 5:
	
	`HTTP.REQ.HEADER("Cust_Header").TYPECAST_LIST_T(',').COUNT`

NTERNAL_GROUPS(sep)	Returns a list of the internal groups to which the user belongs. The groups are separ For example, the following expression returns a colon-separated list of all the interr belongs. `HTTP.REQ.USER.INTERNAL_GROUPS(':')` Parameters: sep - delimiter
S_MEMBER_OF(group_name)	Returns a boolean TRUE if the user who is named in the request is a member of the Following is an example: `http.req.user.is_member_of("mygroup")` Parameter: group_name: The name of the group.
AME	Returns the name of the user in the request. Following is an example: `http.req.username.contains("rohit")`
ASSWD	Returns the password of the user.
N	Returns the HTTP version listed in the request. Following is an example: `http.req.version "\"HTTP/1.0\"`

nteger>)	Returns a portion of the HTTP response body. The length of the returned text is equ <integer> argument. If there are fewer characters in the body than are specified in <integer>, the entire an example: `http.res.body(100).suffix('L',1)`
_MSG	Returns the HTTP response status message.
N	Returns the HTTP version listed in the response.
STNAME.EQ(<hostname>)	Returns a Boolean TRUE value if the host name matches the <hostname> argument. insensitive and if textmode is URLENCODED, the host name is decoded before comp name is www.mycompany.com., the following is true: `http.req.url.hostname.eq("www.mycompany.com")`
M_OR_NEGOTIATE	Returns a Boolean TRUE if the request is a part of an NTLM or NEGOTIATE connectio
PN_ENCODE	Converts the URL to the clientless VPN format.

TH.IGNORE_EMPTY_ELEMENTS	Ignores the empty elements in the list. For example, if the element delimiter in the
	list has an empty element following a=10:
	
	a=10,b=11, ,c=89
	
	The element following b=11 is not considered an empty element.
	
	As another example, consider the following header:
	
	Cust_Header : 123,,24, ,15
	
	The following expression returns a value of 4:
	
	`http.req.header("Cust_Header").typecast_list_t(',').ignore_empt`
	
	The following expression returns a value of 5:
	
	`http.req.header("Cust_Header").typecast_list_t(','). count`

ERY.IGNORE_EMPTY_ELEMENTS	This method ignores the empty elements in a name-value list. For example, if the li
	following list has an empty element following a=10:
	
	a=10;;b=11; ;c=89
	
	The element following b=11 is not considered an empty element.
	
	For example, consider the following header:
	
	Cust_Header : a=1;;b=2; ;c=3
	
	The following expression returns a value of 4:
	
	`http.req.header("Cust_Header").typecast_nvlist_t('=',';').ignor`
	
	The following expression returns a value of 5:
	
	`http.req.header("Cust_Header").typecast_nvlist_t('=',';'). coun`

Expression Prefixes for VPNs and Clientless VPNs

The default syntax expression engine provides prefixes that are specific to parsing VPN or Clientless VPN data. This data includes the following:

- Host names, domains, and URLs in VPN traffic.
- Protocols in the VPN traffic.
- Queries in the VPN traffic.

These text elements are often URLs and components of URLs. In addition to applying the text-based operations on these elements, you can parse these elements by using operations that are specific to parsing URLs. For more information, see "Expressions for Extracting Segments of URLs."

The following table describes the expression prefixes for this type of data.

Table 1. VPN and Clientless VPN Expression Prefixes That Return Text

VPN Expression	Description
PN_DECODE	Extracts the original URL from a clientless VPN URL.
PN_ENCODE	Converts a URL to clientless VPN format.
STNAME	Extracts the HTTP host name from the host name in the URL. This prefix cannot be used in bidirectional policies.
STNAME.DOMAIN	Extracts the domain name from the host name. For example, if the host name is www.mycompany.com or www.mycompany.com:80 mycompany.com. This prefix returns incorrect results if the host name is an IP address. For information addresses, see "Default Syntax Expressions: IP and MAC Addresses, Throughput, VLAN All text operations after this prefix are case insensitive.
STNAME.EQ (<hostname>)	Returns a Boolean TRUE if the host name matches <hostname>. The comparison is ca For example, if the host name is www.mycompany.com, the following returns TRUE: `vpn.baseurl.hostname.eq("www.mycompany.com")` If the text mode is URLENCODED, the host name is decoded before comparison. For n "Operations for HTTP, HTML, and XML Encoding and “Safe” Characters."

STNAME.SERVER	Evaluates the server portion of the host name. For example, if the host name is www.mycompany.com or www.mycompany.com:80 www.mycompany.com. All text operations after this prefix are case insensitive.
TH	Extracts a slash- (/) separated list from the path component of the URL. For example /a/b/c/mypage.html from the following URL: http://www.mycompany.com/a/b/c/mypage.html?a=1 The following expression selects just the “a”: `http.req.url.path.get(1)` For more information on the GET operation, see "Expressions for Extracting Segments

TH.IGNORE_EMPTY_ELEMENTS	This prefix ignores the elements in a list. For example, the following comma-separat
	after “a=10”:
	
	a=10,,b=11, ,c=89
	
	The element following b=11 contains a space, and by default, is not considered an er
	
	Consider the following HTTP header:
	
	Cust_Header : 123,,24, ,15
	
	The following expression returns a count of 4 when evaluating this header:
	
	`http.req.header("Cust_Header").typecase_list_t(',').ignore_empty`
	
	The following expression returns a count of 5 when evaluating this header:
	
	`http.req.header("Cust_Header").typecase_list_t(','). count`

TH_AND_QUERY	Evaluates the text in the URL that follows the host name. For example, if the URL is http://www.mycompany.com/a/b/c/mypage.html?a=1, th /a/b/c/mypage.html?a=1.
OTOCOL	Evaluates the protocol in the URL. Do not use this prefix in bidirectional policies.
ERY	Extracts a name-value list, using the “=” and “&” delimiters from the query string in

ERY.IGNORE_EMPTY_ELEMENTS	This method ignores the empty elements in a name-value list. For example, in the fo is an empty element following “a=10”:
	
	a=10;;b=11; ;c=89
	
	The element following b=11 contains a space and is not considered an empty elemen
	
	Consider the following HTTP header:
	
	Cust_Header : a=1;;b=2; ;c=3
	
	The following expression produces a count of 4 after evaluating this header:
	
	`http.req.header("Cust_Header").typecast_nvlist_t('=',';').ignore`
	
	The following expression produces a count of 5 after evaluating the header:
	
	`http.req.header("Cust_Header").typecast_nvlist_t('=',';').`

FFIX	Evaluates the file name suffix in a URL. For example, if the path is /a/b/c/my.page.html, this operation selects “html.”
_BASEURL	Evaluates the clientless VPN base URL.
_BASEURL.CVPN_DECODE	Extracts the original URL from the clientless VPN formatted URL.
_BASEURL.CVPN_ENCODE	Converts a URL to the clientless VPN format.
_BASEURL.HOSTNAME	Evaluates the host name in the URL. Do not use this prefix in bidirectional policies.
_BASEURL.HOSTNAME.DOMAIN	Evaluates the domain name part of the host name. For example, if the host name is www.mycompany.com or www.mycompany.com:80 mycompany.com. This operation returns incorrect results if the host name is an IP address. For informa addresses, see "Default Syntax Expressions: IP and MAC Addresses, Throughput, VLAN All text operations after this prefix are case insensitive.
_BASEURL.HOSTNAME.EQ(<hostname>)	Returns a Boolean TRUE if the host name matches <hostname>. For example, if the host name is www.mycompany.com or www.mycompany.com:80 `vpn.clientless_baseurl. hostname.eq("www.mycompany.com")` The comparison is case insensitive. If the textmode is URLENCODED, the host name is For more information, see "Operations for HTTP, HTML, and XML Encoding and “Safe”
_BASEURL.HOSTNAME.SERVER	Evaluates the server part of a host name. For example, if the host name is www.mycompany.com or www.mycompany.com:80 www.mycompany.com. All text operations after this prefix are case insensitive.

_BASEURL.PATH	Evaluates a slash- (/) separated list in the URL path. For example, this prefix selects /a/b/c/mypage.html from the following URL: http://www.mycompany.com/a/b/c/mypage.html?a=1 The following expression selects “a” from the preceding URL: `http.req.url.path.get(1)` For more information on the GET operation, see "Expressions for Extracting Segments

_BASEURL.PATH.IGNORE_EMPTY_ELEMENTS	Ignores empty elements in a list. For example, if the list delimiter is a comma (,) the element following “a=10”:
	
	a=10,b=11, ,c=89
	
	The element following b=11 contains a space and is not considered an empty elemen
	
	Consider the following HTTP header:
	
	Cust_Header : 123,,24, ,15
	
	The following expression returns a value of 4 after evaluating this header:
	
	`http.req.header("Cust_Header").typecast_list_t(',').ignore_empty`
	
	The following expression returns a value of 5 after evaluating this header:
	
	`http.req.header("Cust_Header").typecast_list_t(',').`

_BASEURL.PATH_AND_QUERY	Evaluates the text following the host name in a URL. For example, this prefix selects /a/b/c/mypage.html?a=1 from the following URL: http://www.mycompany.com/a/b/c/mypage.html?a=1
_BASEURL.PROTOCOL	Evaluates the protocol in the URL. Do not use this prefix in bidirectional policies.
_BASEURL.QUERY	Extracts a name-value list that uses the delimiters “=” and “&” from a URL query str

_BASEURL.QUERY.IGNORE_EMPTY_ ELEMENTS	Ignores empty elements in a name-value list. For example, the following list contains “a=10”:
	
	a=10;;b=11; ;c=89
	
	The element following b=11 contains a space and is not considered an empty elemen
	
	As another example, consider the following http header:
	
	Cust_Header : a=1;;b=2; ;c=3
	
	The following expression returns a value of 4 after evaluating the preceding header:
	
	`http.req.header("Cust_Header").typecast_nvlist_t('=',';').ignore`
	
	The following expression returns a value of 5 after evaluating the preceding header:
	
	`http.req.header("Cust_Header").typecast_nvlist_t('=',';')`

_BASEURL.SUFFIX	Evaluates the file suffix in a URL. For example, if the URL path is /a/b/c/mypage.htm html.
_HOSTURL	Selects the clientless VPN host URL.
_HOSTURL.CVPN_DECODE	Selects the original URL from the clientless VPN formatted URL.
_HOSTURL.CVPN_ENCODE	Converts a URL to clientless VPN format.
_HOSTURL.HOSTNAME	Extracts the host name in the URL. Do not use this prefix in bidirectional policies.
_HOSTURL.HOSTNAME.DOMAIN	Extracts the domain name from the host name. For example, if the host name is www www.mycompany.com:8080, the domain is mycompany.com. This operation returns incorrect results if the host name contains an IP address. For i IP addresses, see "Default Syntax Expressions: IP and MAC Addresses, Throughput, VL All text operations after this prefix are case insensitive.
_HOSTURL.HOSTNAME.EQ(<hostname>)	Results in Boolean TRUE if the host name matches the <hostname> argument. The For example, if the host name is www.mycompany.com or www.mycompany.com., t TRUE: `vpn.clilentless_hosturl. hostname.eq("www.mycompany.com")` If the text mode is URLENCODED, the host name is decoded before comparison. For m "Operations for HTTP, HTML, and XML Encoding and “Safe” Characters."
_HOSTURL.HOSTNAME.SERVER	Evaluates the server part of the host name. For example, if the host name is www.mycompany.com or www.mycompany.com:80 www.mycompany.com. The comparison is case insensitive, and all text operations after this method are case

_HOSTURL.PATH	Evaluates a slash- (/) separated list on the path component of the URL. For example, consider the following URL: http://www.mycompany.com/a/b/c/mypage.html?a=1 This prefix selects /a/b/c/mypage.html from the preceding URL.

_HOSTURL.PATH.IGNORE_EMPTY_ELEMENTS	This method ignores the empty elements in a list. For example, if the delimiter in a l contains an empty element after the entry “a=10”:
	
	a=10,b=11, ,c=89
	
	The element following b=11 contains a space and is not considered an empty elemen
	
	Consider the following header:
	
	Cust_Header : 123,,24, ,15
	
	The following expression returns a value of 4 for this header:
	
	`http.req.header("Cust_Header").typecast_list_t(','). ignore_empt`
	
	The following expression returns a value of 5 for the same header:
	
	`http.req.header("Cust_Header").typecast_list_t(',').`

_HOSTURL.PATH_AND_QUERY	Evaluates the portion of the URL that follows the host name. For example, consider the following URL: http://www.mycompany.com/a/b/c/mypage.html?a=1 This prefix returns /a/b/c/mypage.html?a=1 from the preceding URL.
_HOSTURL.PROTOCOL	Evaluates the protocol in the URL. Do not use this prefix in bidirectional policies.
_HOSTURL.QUERY	Extracts a name-value list, using the “=” and “&” delimiters from a URL query string.

_HOSTURL.QUERY.IGNORE_EMPTY_ ELEMENTS	Ignores empty elements in a name-value list. For example, the following list uses a s contains an empty element after “a=10”:
	
	a=10;;b=11; ;c=89
	
	In the preceding example, the element following b=11 is not considered an empty ele
	
	Consider the following header:
	
	Cust_Header : a=1;;b=2; ;c=3
	
	The following expression returns a value of 4 after evaluating this header:
	
	`http.req.header("Cust_Header").typecast_nvlist_t('=',';').ignore`
	
	The following expression returns a value of 5 after evaluating the same header:
	
	`http.req.header("Cust_Header").typecast_nvlist_t('=',';')`

_HOSTURL.SUFFIX	Extracts a file name suffix in a URL. For example, if the path is /a/b/c/my.page.html, this prefix selects html.
N	Extracts the domain name part of the host name. For example, if the host name is w www.mycompany.com:8080, the domain is mycompany.com. This prefix returns incorrect results if the host name contains an IP address. For infor addresses, see "Default Syntax Expressions: IP and MAC Addresses, Throughput, VLAN All text operations after this prefix case insensitive.
ostname>)	Returns a Boolean TRUE value if the host name matches the <hostname>. The compa For example, if the host name is www.mycompany.com or www.mycompany.com:80 TRUE: `vpn.host.eq("www.mycompany.com")` If the text mode is URLENCODED the host name is decoded before comparison. For m "Operations for HTTP, HTML, and XML Encoding and “Safe” Characters."
R	Extracts the server name part of the host name. For example, if the host name is ww www.mycompany.com:8080, the server is www.mycompany.com. All text operations after this prefix are case insensitive.

Basic Operations on Text

Basic operations on text include operations for string matching, calculating the length of a string, and controlling case sensitivity. You can include white space in a string that is passed as an argument to an expression, but the string cannot exceed 255 characters.

String Comparison Functions

The following table lists basic string matching operations in which the functions return a Boolean TRUE or FALSE.

Table 1. String Comparison Functions

Function	Description
`<text>.CONTAINS(<string>)`	Returns a Boolean TRUE value if the target contains <string>. Following is an example: `http.req.url.contains(".jpeg")`
`<text>.EQ(<string>)`	Returns a Boolean TRUE value if the target is an exact match with <string>. For example, the following expression returns a Boolean TRUE for a URL with a host name of “myhostabc”: `http.req.url.hostname.eq("myhostabc")`
`<text>.STARTSWITH(<string>)`	Returns a Boolean TRUE value if the target begins with <string>. For example, the following expression returns a Boolean TRUE for a URL with a host name of “myhostabc”: `http.req.url.hostname.startswith("myhost")`
`<text>.ENDSWITH(<string>)`	Returns a Boolean TRUE value if the target ends with <string>. For example, the following expression returns a Boolean TRUE for a URL with a host name of “myhostabc”: `http.req.url.hostname.endswith("abc")`

`<text>.NE(<string>)`	Returns a Boolean TRUE value if the prefix is not equal to the string argument. If the prefix returns a non-string value, the function argument is compared to the string representation of the value returned by the prefix. You can use the functions with SET_TEXT_MODE(IGNORECASE) or SET_TEXT_MODE(NOIGNORECASE), and with both ASCII and UTF-8 character sets.
`<text>.GT(<string>)`	Returns a Boolean TRUE value if the prefix is alphabetically greater than the string argument. If the prefix returns a non-string value, the function argument is compared to the string representation of the value returned by the prefix. You can use the functions with SET_TEXT_MODE(IGNORECASE) or SET_TEXT_MODE(NOIGNORECASE), and with both ASCII and UTF-8 character sets.
`<text>.GE(<string>)`	Returns a Boolean TRUE value if the prefix is alphabetically greater than or equal to the string argument. If the prefix returns a non-string value, the function argument is compared to the string representation of the value returned by the prefix. You can use the functions with SET_TEXT_MODE(IGNORECASE) or SET_TEXT_MODE(NOIGNORECASE), and with both ASCII and UTF-8 character sets.
`<text>.LT(<string>)`	Returns a Boolean TRUE value if the prefix is alphabetically lesser than the string argument. If the prefix returns a non-string value, the function argument is compared to the string representation of the value returned by the prefix. You can use the functions with SET_TEXT_MODE(IGNORECASE) or SET_TEXT_MODE(NOIGNORECASE), and with both ASCII and UTF-8 character sets.
`<text>.LE(<string>)`	Returns a Boolean TRUE value if the prefix is alphabetically lesser than or equal to the string argument. If the prefix returns a non-string value, the function argument is compared to the string representation of the value returned by the prefix. You can use the functions with SET_TEXT_MODE(IGNORECASE) or SET_TEXT_MODE(NOIGNORECASE), and with both ASCII and UTF-8 character sets.

Calculating the Length of a String

The <text>.LENGTH operation returns a numeric value that is equal to the number of characters (not bytes) in a string:

```
<text>.LENGTH
```

For example, you may want to identify request URLs that exceed a particular length. Following is an expression that implements this example:

```
HTTP.REQ.URL.LENGTH < 500
```

After taking a count of the characters or elements in a string, you can apply numeric operations to them. For more information, see "Default Syntax Expressions: Working with Dates, Times, and Numbers."

Considering, Ignoring, and Changing Text Case

The following functions operate on the case (upper-case or lower-case) of the characters in the string.

Table 2. Functions for Considering, Ignoring, and Changing Text Case

Function	Description
`<text>.SET_TEXT_MODE(IGNORECASE|NOIGNORECASE)`	This function turns case sensitivity on or off for all text operations.
`<text>.TO_LOWER`	Converts the target to lowercase for a text block of up to 2 kilobyte (KB). Returns UNDEF if the target exceeds 2 KB. For example, the string “ABCd:” is converted to “abcd:”.
`<text>.TO_UPPER`	Converts the target to uppercase. Returns UNDEF if the target exceeds 2 KB. For example, the string “abcD:” is converted to “ABCD:”.

Stripping Specific Characters from a String

You can use the `STRIP_CHARS(<string>)` function to remove specific characters from the text that is returned by a default syntax expression prefix (the input string). All instances of the characters that you specify in the argument are stripped from the input string. You can use any text method on the resulting string, including the methods used for matching the string with a pattern set.

For example, in the expression `CLIENT.UDP.DNS.DOMAIN.STRIP_CHARS(".-_")`, the `STRIP_CHARS(<string>)` function strips all periods (`.`), hyphens (`-`), and underscores (`_`) from the domain name returned by the prefix `CLIENT.UDP.DNS.DOMAIN`. If the domain name that is returned is "a.dom_ai_n-name", the function returns the string "adomainname".

In the following example, the resulting string is compared with a pattern set called "listofdomains":

```
CLIENT.UDP.DNS.DOMAIN.STRIP_CHARS(".-_").CONTAINS_ANY("listofdomains"
)
```

Note: You cannot perform a rewrite on the string that is returned by the `STRIP_CHARS(<string>)` function.

The following functions strip matching characters from the beginning and end of a given string input.

Table 3. Functions for Stripping Characters From the Beginning or End of a String

Function	Description
`<text>.STRIP_START_CHARS(s)`	Strips matching characters from the beginning of the input string until the first non-matching character is found and returns the remainder of the string. You must specify the characters that you want to strip as a single string within quotation marks. For example, if the name of a header is `TestLang` and `://_en_us:` is its value, `HTTP.RES.HEADER("TestLang").STRIP_START_CHARS(":/_")` strips the specified characters from the beginning of the value of the header until the first non-matching character `e` is found and returns `en_us:` as a string.
`<text>.STRIP_END_CHARS(s)`	Strips matching characters from the end of the input string to the first non-matching character is found and returns the remainder of the string. You must specify the characters that you want to strip as a single string within quotation marks. For example, if the name of a header is `TestLang` and `://_en_us:` is its value, `HTTP.RES.HEADER("TestLang").STRIP_START_CHARS(":/_")` strips the specified characters from the end of the value of the header until the first non-matching character `s` is found and returns `://_en_us` as a string.

Appending a String to Another String

You can use the `APPEND()` function to append the string representation of the argument to the string representation of the value returned by the preceding function. The preceding function can be one that returns a number, unsigned long, double, time value, IPv4 address, or IPv6 address. The argument can be a text string, number, unsigned long, double, time value, IPv4 address, or IPv6 address. The resulting string value is the same string value that is obtained by using the `+` operator.

Complex Operations on Text

In addition to performing simple string matching, you can configure expressions that examine more complex aspects of text, including examining the length of a string and looking within a text block for patterns rather than specific strings.

Be aware of the following for any text-based operation:

- For any operation that takes a string argument, the string cannot exceed 255 characters.
- You can include white space when you specify a string in an expression.

Operations on the Length of a String

The following operations extract strings on the basis of a character count.

Table 1. String Operations Based on a Character Count

Character Count Operation	Description
`<text>.TRUNCATE(<count>)`	Returns a string after truncating the end of the target by the number of characters in <count>. If the entire string is shorter than <count>, nothing is returned.
`<text>.TRUNCATE(<character>, <count>)`	Returns a string after truncating the text after <character> by the number of characters specified in <count>.
`<text>.PREFIX(<character>, <count>)`	Selects the longest prefix in the target that has at most <count> occurrences of <character>.

	<text>.SUFFIX(<character>, <count>) Selects the longest suffix in the target that has at most <count> occurrences of <character>.
	
	For example, consider the following response body:
	
	`JLEwx`
	
	The following expression returns a value of “JLEwx”:
	
	`http.res.body(100).suffix('L',1)`
	
	The following expression returns “LLEwx”:
	
	`http.res.body(100).suffix('L',2)`

`<text>.SUBSTR(<starting_offset>, <length>)`	Select a string with <length> number of characters from the target object. Begin extracting the string after the <starting_offset>. If the number of characters after the offset are fewer than the value of the <length> argument, select all the remaining characters.
`<text>.SKIP(<character>, <count>)`	Select a string from the target after skipping over the longest prefix that has at most <count> occurrences of <character>.

Operations on a Portion of a String

You can extract a subset of a larger string by using one of the operations in the following table.

Table 1. Basic Operations on a Portion of a String

ext Operation	Description
>.BEFORE_STR(<string>)	Returns the text that precedes the first occurrence of <string>. If there is no match for <string>, the expression returns a text object of 0 length. Following is an example: `http.res.body(1024).after_str("start_string").before_str("end_string").conta`
>.AFTER_STR(<string>)	Returns the text that follows the first occurrence of <string>. If there is no match for <string>, the expression returns a text object of 0 length. Following is an example: `http.res.body(1024).after_str("start_string").before_str("end_string").conta`
>.BETWEEN(<starting g>, <ending string>)	Returns a Boolean TRUE value if the length of the text object is greater than or equal to the sum <sta <ending string> argument lengths, and if a prefix of the target matches <starting string>, and if the su matches <ending string>.
>.PREFIX(<prefix h>)	Returns the starting string from a target block of text that contains the number of characters in the < argument. If the <prefix length> argument exceeds the number of characters in the target, the entire string is se
>.SUFFIX(<suffix h>)	Returns the ending string from a target block of text that contains the number of characters in the <s argument. If the <suffix length> argument exceeds the number characters in the target, the entire str
>.SUBSTR(<string>)	Select the first block of text in the target that matches the <string>.
>.SKIP(<prefix length>)	Selects the text in the target after skipping over a <prefix length> number of characters. If the entire target has fewer characters than <prefix length>, the entire target is skipped.
>.STRIP_END_WS	Selects the text after removing white space from the end of the target.
>.STRIP_START_WS	Selects the text after removing white space from the beginning of the target.

>.UNQUOTE(<character>)	Selects the <character>, removes white space that immediately precedes and follows the <character> remaining text is quoted by <character>, this prefix also removes the quotes. For example, the operation UNQUOTE("") changes the following text: "abc xyz def " To the following: abc xyz def

Operations for Comparing the Alphanumeric Order of Two Strings

The COMPARE operation examines the first nonmatching character of two different strings. This operation is based on lexicographic order, which is the method used when ordering terms in dictionaries.

This operation returns the arithmetic difference between the ASCII values of the first nonmatching characters in the compared strings. The following differences are examples:

- The difference between “abc” and “abd” is -1 (based on the third pair-wise character comparison).
- The difference between “@” and “abc” is -33.
- The difference between “1” and “abc” is -47.

Following is the syntax for the COMPARE operation.

```
<text>.COMPARE(<string>)
```

Extracting an Integer from a String of Bytes That Represent Text

You can use the following functions to treat a string of bytes that represent text as a sequence of bytes, extract 8, 16, or 32 bits from the sequence, and then convert the extracted bits to an integer.

Table 1. Operations for Extracting an Integer from a String of Bytes That Represent Text

Function	Description
`<text>.GET_SIGNED8(<n>)`	Treats the string of bytes represented by text as a sequence of 8-bit signed integers and returns the integer at byte offset n. If the offset makes all or part of the value outside of the current text, an `UNDEF` condition is raised.
`<text>.GET_UNSIGNED8(<n>)`	Treats the string of bytes represented by text as a sequence of 8-bit unsigned integers and returns the integer at byte offset n. If the offset makes all or part of the value outside of the current text, an `UNDEF` condition is raised.

<text>.GET_SIGNED16(<n>, <endianness>)	Treats the text string returned by the prefix as a string of bytes, extracts 16 bits starting at byte offset n, and converts the extracted bit sequence to a 16-bit signed integer. If the offset makes all or part of the value outside of the current text, an UNDEF condition is raised. The first parameter n is the byte offset from the current position in the text string. Providing a byte offset enables the function to handle items that are not aligned on the boundaries that are required by indexes. The second parameter, endianness, takes a mnemonic value of LITTLE_ENDIAN or BIG_ENDIAN. **Note:** In NetScaler 9.2, the parameter n was an index into an array of 16-bit items. In NetScaler 9.3, the parameter is a byte offset. Therefore, if you used this function in NetScaler 9.2, after you upgrade to NetScaler 9.3, you must change n to 2*n to obtain the same results as you did earlier. For example, if the value of n before the upgrade was 4, you must change the value of n to 8. The parameter endianness also no longer takes the values that it did in NetScaler 9.2, which were 0 and 1. Instead, endianness accepts the mnemonic values mentioned earlier. **Example** HTTP.REQ.BODY(100).GET_SIGNED16(8, BIG_ENDIAN)

<text>.GET_UNSIGNED16(<n>, <endianness>)	Treats the text string returned by the prefix as a string of bytes, extracts 16 bits starting at byte offset n, and converts the extracted bit sequence to a 16-bit unsigned integer. If the offset makes all or part of the value outside of the current text, an UNDEF condition is raised. The first parameter n is the byte offset from the current position in the text string. Providing a byte offset enables the function to handle items that are not aligned on the boundaries that are required by indexes. The second parameter, endianness, takes a mnemonic value of LITTLE_ENDIAN or BIG_ENDIAN. **Note:** In NetScaler 9.2, the parameter n was an index into an array of 16-bit items. In NetScaler 9.3, the parameter is a byte offset. Therefore, if you used this function in NetScaler 9.2, after you upgrade to NetScaler 9.3, you must change n to 2*n to obtain the same results as you did earlier. For example, if the value of n before the upgrade was 4, you must change the value of n to 8. The parameter endianness also no longer takes the values that it did in NetScaler 9.2, which were 0 and 1. Instead, endianness accepts the mnemonic values mentioned earlier. **Example** HTTP.REQ.BODY(100).GET_UNSIGNED16(8, LITTLE_ENDIAN)

<text>.GET_SIGNED32(<n>, <endianness>)	Treats the text string returned by the prefix as a string of bytes, extracts 32 bits starting at byte offset n, and converts the extracted bit sequence to a 32-bit signed integer. If the offset makes all or part of the value outside of the current text, an UNDEF condition is raised. The first parameter n is the byte offset from the current position in the text string. Providing a byte offset enables the function to handle items that are not aligned on the boundaries that are required by indexes. The second parameter, endianness, takes a mnemonic value of LITTLE_ENDIAN or BIG_ENDIAN. **Note:** In NetScaler 9.2, the parameter n was an index into an array of 32-bit items. In NetScaler 9.3, the parameter is a byte offset. Therefore, if you used this function in NetScaler 9.2, after you upgrade to NetScaler 9.3, you must change n to 4*n to obtain the same results as you did earlier. For example, if the value of n before the upgrade was 4, you must change the value of n to 16. The parameter endianness also no longer takes the values that it did in NetScaler 9.2, which were 0 and 1. Instead, endianness accepts the mnemonic values mentioned earlier. **Example** HTTP.REQ.BODY(1000).GET_SIGNED32(12, BIG_ENDIAN)
<text>.GET_UNSIGNED32(<n>, <endianness>)	Treats the text string returned by the prefix as a string of bytes, extracts 32 bits starting at byte offset n, and returns the extracted bit sequence as part of a 64-bit unsigned long integer. If the offset makes all or part of the value outside of the current text, an UNDEF condition is raised. The first parameter n is the byte offset from the current position in the text string. Providing a byte offset enables the function to handle items that are not aligned on the boundaries that are required by indexes. The second parameter, endianness, takes a mnemonic value of LITTLE_ENDIAN or BIG_ENDIAN. **Example** HTTP.REQ.BODY(1000).GET_UNSIGNED32(30, LITTLE_ENDIAN)

Converting Text to a Hash Value

You can convert a text string to a hash value by using the `HASH` function. This function returns a 31-bit positive integer as a result of the operation. Following is the format of the expression:

```
<text>.HASH
```

This function ignores case and white spaces. For example, after the operation, the two strings `Ab c` and `a bc` would produce the same hash value.

Encoding and Decoding Text by Applying the Base64 Encoding Algorithm

The following two functions encode and decode a text string by applying the Base64 encoding algorithm

Table 1. Functions for Encoding and Decoding a Text String by Using Base64 Encoding

Function	Description
`text.B64ENCODE`	Encodes the text string (designated by text) by applying the Base64 encoding algorithm.
`text.B64DECODE`	Decodes the Base64-encoded string (designated by text) by applying the Base64 decoding algorithm. The operation raises an `UNDEF` if text is not in B64-encoded format.

Refining the Search in a Rewrite Action by Using the EXTEND Function

The EXTEND function is used in rewrite actions that specify patterns or pattern sets and target the bodies of HTTP packets. When a pattern match is found, the EXTEND function extends the scope of the search by a predefined number of bytes on both sides of the matching string. A regular expression can then be used to perform a rewrite on matches in this extended region. Rewrite actions that are configured with the EXTEND function perform rewrites faster than rewrite actions that evaluate entire HTTP bodies using only regular expressions.

The format of the EXTEND function is EXTEND(m,n), where m and n are the number of bytes by which the scope of the search is extended before and after the matching pattern, respectively. When a match is found, the new search scope comprises m bytes that immediately precede the matching string, the string itself, and the n bytes that follow the string. A regular expression can then be used to perform a rewrite on a portion of this new string.

The EXTEND function can be used only if the rewrite action in which it is used fulfills the following requirements:

- The search is performed by using patterns or patterns sets (not regular expressions)
- The rewrite action evaluates only the bodies of HTTP packets.

Additionally, the EXTEND function can be used only with the following types of rewrite actions:

- replace_all
- insert_after_all
- delete_all
- insert_before_all

For example, you might want to delete all instances of "http://exampleurl.com/" and "http://exampleurl.au/" in the first 1000 bytes of the body. To do this, you can configure a rewrite action to search for all instances of the string exampleurl, extend the scope of the search on both sides of the string when a match is found, and then use a regular expression to perform the rewrite in the extended region. The following example extends the scope of the search by 20 bytes to the left and 50 bytes to the right of the matching string:

```
add rewrite action delurl_example delete_all 'HTTP.REQ.BODY(1000)'
-pattern exampleurl -refineSearch
'extend(20,50).regex_select(re#http://exampleurl.(com|au)#)'
```

Converting Text to Hexadecimal Format

The following function converts text to hexadecimal format and extracts the resulting string:

```
<text>.BLOB_TO_HEX(<string>)
```

For example, this function converts the byte string “abc” to “61:62:63”.

Encrypting and Decrypting Text

In default syntax expressions, you can use the ENCRYPT and DECRYPT functions to encrypt and decrypt text. Data encrypted by the ENCRYPT function on a given NetScaler appliance or high availability (HA) pair is intended for decryption by the DECRYPT function on the same NetScaler appliance or HA pair. The appliance supports the RC4, DES3, AES128, AES192, and AES256 encryption methods. The key value that is required for encryption is not user-specifiable. When an encryption method is set, the appliance automatically generates a random key value that is appropriate for the specified method. The default method is AES256 encryption, which is the most secure encryption method and the one that Citrix recommends.

You do not need to configure encryption unless you want to change the encryption method or you want the appliance to generate a new key value for the current encryption method.

Note: You can also encrypt and decrypt XML payloads. For information about the functions for encrypting and decrypting XML payloads, see "Encrypting and Decrypting XML Payloads."

Configuring Encryption

During startup, the appliance runs the `set ns encryptionParams` command with, by default, the AES256 encryption method, and uses a randomly generated key value that is appropriate for AES256 encryption. The appliance also encrypts the key value and saves the command, with the encrypted key value, to the NetScaler configuration file. Consequently, the AES256 encryption method is enabled for the `ENCRYPT` and `DECRYPT` functions by default. The key value that is saved in the configuration file persists across reboots even though the appliance runs the command each time you restart it.

You can run the `set ns encryptionParams` command manually, or use the configuration utility, if you want to change the encryption method or if you want the appliance to generate a new key value for the current encryption method. To use the CLI to change the encryption method, set only the `method` parameter, as shown in "**Example 1: Changing the Encryption Method**." If you want the appliance to generate a new key value for the current encryption method, set the `method` parameter to the current encryption method and the `keyValue` parameter to an empty string (""), as shown in "**Example 2: Generating a New Key Value for the Current Encryption Method**." After you generate a new key value, you must save the configuration. If you do not save the configuration, the appliance uses the newly generated key value only until the next restart, after which it reverts to the key value in the saved configuration.

Parameters for configuring encryption

method

The cipher method (and key length) used to encrypt and decrypt content. Possible values: NONE, RC4, DES3, AES128, AES192, AES256. Default: AES256.

keyValue

The base64-encoded key generation number, method, and key value. Omit this parameter if you enter a command to change the encryption method. To generate a new key value for the current encryption method, specify an empty string ("") as the value of this parameter. The parameter is passed implicitly, with its automatically generated value, to the NetScaler packet engines even when it is not included in the command. Passing the parameter to the packet engines enables the appliance to save the key value to the configuration file and to propagate the key value to the secondary appliance in a high availability setup.

To configure encryption by using the configuration utility

1. Navigate to System > Settings.
2. In the Settings area, click Change Encryption parameters.
3. In the Change Encryption Parameters dialog box, do one of the following:
   - To change the encryption method, in the Method list, select the encryption method that you want.
   - To generate a new key value for the current encryption method, click Generate a new key for the selected method.
4. Click OK.

Using the ENCRYPT and DECRYPT Functions

You can use the ENCRYPT and DECRYPT functions with any expression prefix that returns text. For example, you can use the ENCRYPT and DECRYPT functions in rewrite policies for cookie encryption. In the following example, the rewrite actions encrypt a cookie named MyCookie, which is set by a back-end service, and decrypt the same cookie when it is returned by a client:

```
add rewrite action my-cookie-encrypt-action replace
"HTTP.RES.SET_COOKIE.COOKIE(\"MyCookie\").VALUE(0)"
"HTTP.RES.SET_COOKIE.COOKIE(\"MyCookie\").VALUE(0).ENCRYPT"
-bypassSafetyCheck YES

add rewrite action my-cookie-decrypt-action replace
"HTTP.REQ.COOKIE.VALUE(\"MyCookie\")"
"HTTP.REQ.COOKIE.VALUE(\"MyCookie\").DECRYPT" -bypassSafetyCheck YES
```

After you configure policies for encryption and decryption, save the configuration to bring the policies into effect.

Default Syntax Expressions: Working with Dates, Times, and Numbers

Most numeric data that the NetScaler appliance processes consists of dates and times. In addition to working with dates and times, the appliance processes other numeric data, such as the lengths of HTTP requests and responses. To process this data, you can configure default syntax expressions that process numbers.

A numeric expression consists of an expression prefix that returns a number and sometimes, but not always, an operator that can perform an operation on the number. Examples of expression prefixes that return numbers are `SYS.TIME.DAY`, `HTTP.REQ.CONTENT_LENGTH`, and `HTTP.RES.BODY.LENGTH`. Numeric operators can work with any prefix expression that returns data in numeric format. The GT(<int>) operator, for example, can be used with any prefix expression, such as `HTTP.REQ.CONTENT_LENGTH`, that returns an integer. Numeric expression prefixes and operators are also covered in "Compound Operations for Numbers" and "Default Syntax Expressions: Parsing HTTP, TCP, and UDP Data."

Format of Dates and Times in an Expression

When configuring a default syntax expression in a policy that works with dates and times (for example, the NetScaler system time or a date in an SSL certificate), you specify a time format as follows:

```
GMT|LOCAL [<yyyy>] [<month>] [<d>] [<h>] [<m>] [<s>]
```

Where:

- <yyyy> is a four-digit year after GMT or LOCAL.
- <month> is a three-character abbreviation for the month, for example, Jan, Dec.
- <d> is a day of the week or an integer for the date.

  You cannot specify the day as Monday, Tuesday, and so on. You specify either an integer for a specific day of the month, or you specify a date as the first, second, third weekday of the month, and so on. Following are examples of specifying a day of the week:

  - Sun_1 is the first Sunday of the month.
  - Sun_3 is the third Sunday of the month.
  - Wed_3 is the third Wednesday of the month.
  - 30 is an example of an exact date in a month.
- <h> is the hour, for example, 10h.
- <s> is the number of seconds, for example, 30s.

The following example expression is true if the date is between 2008 Jan and 2009 Jan, based on GMT.

```
http.req.date.between(GMT 2008 Jan, GMT 2009 Jan)
```

The following example expression is true for March and all months that follow March in the calendar year, based on GMT:

```
sys.time.ge(GMT 2008 Mar)
```

When you specify a date and time, note that the format is case sensitive and must preserve the exact number of blank spaces between entries.

Note: In an expression that requires two time values, both must use GMT or both must use LOCAL. You cannot mix the two in an expression.

Note: Unlike when you use the SYS.TIME prefix in a default syntax expression, if you specify SYS.TIME in a rewrite action, the NetScaler returns a string in conventional date format (for example, Sun, 06 Nov 1994 08:49:37 GMT). For example, the following rewrite action replaces the http.res.date header with the NetScaler system time in a conventional date format:

add rewrite action `sync_date replace http.res.date sys.time`

Expressions for the NetScaler System Time

The SYS.TIME expression prefix extracts the NetScaler system time. You can configure expressions that establish whether a particular event occurred at a particular time or within a particular time range according to the NetScaler system time.

The following table describes the expressions that you can create by using the SYS.TIME prefix.

Table 1. Expressions That Return NetScaler System Dates and Times

NetScaler Time Operation	Description
SYS.TIME.BETWEEN(<time1>, <time2>)	Returns a Boolean TRUE if the returned value is later than <time1> and earlier than <time2>. You format the <time1>, <time2> arguments as follows: · They must both be GMT or both LOCAL. · <time2> must be later than <time1>. For example, if the current time is GMT 2005 May 1 10h 15m 30s, and it is the first Sunday of the month, you can specify the following: · sys.time.between(GMT 2004, GMT 2006) · sys.time.between(GMT 2004 Jan, GMT 2006 Nov) · sys.time.between(GMT 2004 Jan, GMT 2006) · sys.time.between(GMT 2005 May Sun_1, GMT 2005 May Sun_3) · sys.time.between(GMT 2005 May 1, GMT May 2005 1) · sys.time.between(LOCAL 2005 May 1, LOCAL May 2005 1)
SYS.TIME.DAY	Returns the current day of the month as a number from 1 through 31.

SYS.TIME.EQ(<time>)	Returns a Boolean TRUE if the current time is equal to the <time> argument. For example, if the current time is GMT 2005 May 1 10h 15m 30s, and it is the first Sunday of the month, you can specify the following (evaluation results are shown in parentheses): · sys.time.eq(GMT 2005) (TRUE in this example.) · sys.time.eq(GMT 2005 Dec) (FALSE in this example.) · sys.time.eq(LOCAL 2005 May) (Evaluates to TRUE or FALSE in this example, depending on the current time zone.) · sys.time.eq(GMT 10h) (TRUE in this example.) · sys.time.eq(GMT 10h 30s) (TRUE in this example.) · sys.time.eq(GMT May 10h) (TRUE in this example.) · sys.time.eq(GMT Sun) (TRUE in this example.) · sys.time.eq(GMT May Sun_1) (TRUE in this example.)
SYS.TIME.NE(<time>)	Returns a Boolean TRUE if the current time is not equal to the <time> argument.

SYS.TIME.GE(<time>)	Returns a Boolean TRUE if the current time is later than or equal to <time>. For example, if the current time is GMT 2005 May 1 10h 15m 30s, and it is the first Sunday of the month, you can specify the following (evaluation results are shown in parentheses): · sys.time.ge(GMT 2004) (TRUE in this example.) · sys.time.ge(GMT 2005 Jan) (TRUE in this example.) · sys.time.ge(LOCAL 2005 May) (TRUE or FALSE in this example, depending on the current time zone.) · sys.time.ge(GMT 8h) (TRUE in this example.) · sys.time.ge(GMT 30m) (FALSE in this example.) · sys.time.ge(GMT May 10h) (TRUE in this example.) · sys.time.ge(GMT May 10h 0m) (TRUE in this example.) · sys.time.ge(GMT Sun) (TRUE in this example.) · sys.time.ge(GMT May Sun_1) (TRUE in this example.)

SYS.TIME.GT(<time>)	Returns a Boolean TRUE if the time value is later than the <time> argument. For example, if the current time is GMT 2005 May 1 10h 15m 30s, and it is the first Sunday of the month, you can specify the following (evaluation results are shown in parentheses): · sys.time.gt(GMT 2004) (TRUE in this example.) · sys.time.gt(GMT 2005 Jan) (TRUE in this example.) · sys.time.gt(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.) · sys.time.gt(GMT 8h) (TRUE in this example.) · sys.time.gt(GMT 30m) (FALSE in this example.) · sys.time.gt(GMT May 10h) (FALSE in this example.) · sys.time.gt(GMT May 10h 0m) (TRUE in this example.) · sys.time.gt(GMT Sun) (FALSE in this example.) · sys.time.gt(GMT May Sun_1) (FALSE in this example.)
SYS.TIME.HOURS	Returns the current hour as an integer from 0 to 23.

SYS.TIME.LE(<time>)	Returns a Boolean TRUE if the current time value precedes or is equal to the <time> argument. For example, if the current time is GMT 2005 May 1 10h 15m 30s, and it is the first Sunday of the month, you can specify the following (evaluation results are shown in parentheses): · sys.time.le(GMT 2006) (TRUE in this example.) · sys.time.le(GMT 2005 Dec) (TRUE in this example.) · sys.time.le(LOCAL 2005 May) (TRUE or FALSE depending on the current timezone.) · sys.time.le(GMT 8h) (FALSE in this example.) · sys.time.le(GMT 30m) (TRUE in this example.) · sys.time.le(GMT May 10h) (TRUE in this example.) · sys.time.le(GMT Jun 11h) (TRUE in this example.) · sys.time.le(GMT Wed) (TRUE in this example.) · sys.time.le(GMT May Sun_1) (TRUE in this example.)
SYS.TIME.LT(<time>)	Returns a Boolean TRUE if the current time value precedes the <time> argument. For example, if the current time is GMT 2005 May 1 10h 15m 30s, and it is the first Sunday of the month, you can specify the following (evaluation results are shown in parentheses): · sys.time.lt(GMT 2006) (TRUE in this example.) · sys.time.lt.time.lt(GMT 2005 Dec) (TRUE in this example.) · sys.time.lt(LOCAL 2005 May) (TRUE or FALSE depending on the current time zone.) · sys.time.lt(GMT 8h) (FALSE in this example.) · sys.time.lt(GMT 30m) (TRUE in this example.) · sys.time.lt(GMT May 10h) (FALSE in this example.) · sys.time.lt(GMT Jun 11h) (TRUE in this example.) · sys.time.lt(GMT Wed) (TRUE in this example.) · sys.time.lt(GMT May Sun_1) (FALSE in this example.)

SYS.TIME.MINUTES	Returns the current minute as an integer from 0 to 59.
SYS.TIME.MONTH	Extracts the current month and returns an integer from 1 (January) to 12 (December).
SYS.TIME.RELATIVE_BOOT	Calculates the number of seconds to the closest previous or scheduled reboot, and returns an integer. If the closest boot time is in the past, the integer is negative. If it is in the future, the integer is positive.
SYS.TIME.RELATIVE_NOW	Calculates the number of seconds between the current NetScaler system time and the specified time, and returns an integer showing the difference. If the designated time is in the past, the integer is negative; if it is in the future, the integer is positive.
SYS.TIME.SECONDS	Extracts the seconds from the current NetScaler system time, and returns that value as an integer from 0 to 59.
SYS.TIME.WEEKDAY	Returns the current weekday as a value from 0 (Sunday) to 6 (Saturday).
SYS.TIME.WITHIN (<time1>, <time2>)	If you omit an element of time in <time1>, for example, the day or hour, it is assumed to have the lowest value in its range. If you omit an element in <time2>, it is assumed to have the highest value of its range. The ranges for the elements of time are as follows: month 1-12, day 1-31, weekday 0-6, hour 0-23, minutes 0-59 and seconds 0-59. If you specify the year, you must do so in both <time1> and <time2>. For example, if the time is GMT 2005 May 10 10h 15m 30s, and it is the second Tuesday of the month, you can specify the following (evaluation results are shown in parentheses): · sys.time.within(GMT 2004, GMT 2006) (TRUE in this example.) · sys.time.within(GMT 2004 Jan, GMT 2006 Mar) (FALSE, May is not in the range of January to March.) · sys.time.within(GMT Feb, GMT) (TRUE, May is in the range of February to December.) · sys.time.within(GMT Sun_1, GMT Sun_3) (TRUE, the second Tuesday is between the first Sunday and the third Sunday.) · sys.time.within(GMT 2005 May 1 10h, GMT May 2005 1 17h) (TRUE in this example.) · sys.time.within(LOCAL 2005 May 1, LOCAL May 2005 1) (TRUE or FALSE, depending on the NetScaler system time zone.)

SYS.TIME.YEAR	Extracts the year from the current system time and returns that value as a four-digit integer.

Expressions for SSL Certificate Dates

You can determine the validity period for SSL certificates by configuring an expression that contains the following prefix:

```
CLIENT.SSL.CLIENT_CERT
```

The following example expression matches a particular time for expiration with the information in the certificate:

```
client.ssl.client_cert.valid_not_after.eq(GMT 2009)
```

The following table describes time-based operations on SSL certificates. To obtain the expression you want, replace *certificate* in the expression in the first column with the prefix expression, "`CLIENT.SSL.CLIENT_CERT`".

Table 1. Operations on Certificate (client.ssl.client_cert) Dates and Times

SSL Certificate Operation	Description
`<certificate>.VALID_NOT_AFTER`	Returns the last day before certificate expiration. The return format is the number of seconds since GMT January 1, 1970 (0 hours, 0 minutes, 0 seconds).

<certificate>.VALID_NOT_AFTER.BETWEEN(<time1>, <time2>)	Returns a Boolean TRUE value if the certificate validity is betw the <time1> and <time2> arguments. Both <time1> and <time2 must be fully specified. Following are examples: GMT 1995 Jan is fully specified. GMT Jan is not fully specified GMT 1995 20 is not fully specified. GMT Jan Mon_2 is not fully specified. The <time1> and <time2> arguments must be both GMT or both LOCAL, and <time2> must be greater than <time1>. For example, if it is GMT 2005 May 1 10h 15m 30s, and the first Sunday of the month, you can specify the following (evaluation results are in parentheses). · . . .between(GMT 2004, GMT 2006) (TRUE) · . . .between(GMT 2004 Jan, GMT 2006 Nov) (TR · . . .between(GMT 2004 Jan, GMT 2006) (TRUE) · . . .between(GMT 2005 May Sun_1, GMT 2005 Ma Sun_3) (TRUE) · . . .between(GMT 2005 May 1, GMT May 2005 1) (TRUE) · . . .between(LOCAL 2005 May 1, LOCAL May 200 (TRUE or FALSE, depending on the NetScaler system time zone.)
<certificate>.VALID_NOT_AFTER.DAY	Extracts the last day of the month that the certificate is valid, returns a number from 1 through 31, as appropriate for the dat

<certificate>.VALID_NOT_AFTER.EQ(<time>)	Returns a Boolean TRUE if the time is equal to the <time> argument. For example, if the current time is GMT 2005 May 1 10h 15m 3 and it is the first Sunday of the month, you can specify the foll (evaluation results for this example are in parentheses): · . . .eq(GMT 2005) (TRUE) · . . .eq(GMT 2005 Dec) (FALSE) · . . .eq(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone) · . . .eq(GMT 10h) (TRUE) · . . .eq(GMT 10h 30s) (TRUE) · . . .eq(GMT May 10h) (TRUE) · . . .eq(GMT Sun) (TRUE) · . . .eq(GMT May Sun_1) (TRUE)
<certificate>.VALID_NOT_AFTER.GE(<time>)	Returns a Boolean TRUE if the time value is greater than or eq the argument <time>. For example, if the time value is GMT 2005 May 1 10h 15m 30s it is the first Sunday of the month of May in 2005, you can spec the following (evaluation results for this example are in parentheses): · . . .ge(GMT 2004) (TRUE) · . . .ge(GMT 2005 Jan) (TRUE) · . . .ge(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.) · . . .ge(GMT 8h) (TRUE) · . . .ge(GMT 30m) (FALSE) · . . .ge(GMT May 10h) (TRUE) · . . .ge(GMT May 10h 0m) (TRUE) · . . .ge(GMT Sun) (TRUE) · . . .ge(GMT May Sun_1) (TRUE)

<certificate>.VALID_NOT_AFTER.GT(<time>)	Returns a Boolean TRUE if the time value is greater than the argument <time>. For example, if the time value is GMT 2005 May 1 10h 15m 30s, it is the first Sunday of the month of May in 2005, you can spec the following (evaluation results for this example are in parentheses): · . . .gt(GMT 2004) (TRUE) · . . .gt(GMT 2005 Jan) (TRUE) · . . .gt(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.) · . . .gt(GMT 8h) (TRUE) · . . .gt(GMT 30m) (FALSE) · . . .gt(GMT May 10h) (FALSE) · . . .gt(GMT Sun) (FALSE) · . . .gt(GMT May Sun_1) (FALSE)
<certificate>.VALID_NOT_AFTER.HOURS	Extracts the last hour that the certificate is valid and returns t value as an integer from 0 to 23.
<certificate>.VALID_NOT_AFTER.LE(<time>)	Returns a Boolean TRUE if the time precedes or is equal to the <time> argument. For example, if the time value is GMT 2005 May 1 10h 15m 30s, it is the first Sunday of the month of May in 2005, you can spec the following (evaluation results for this example are in parentheses): · . . .le(GMT 2006) (TRUE) · . . .le(GMT 2005 Dec) (TRUE) · . . .le(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.) · . . .le(GMT 8h) (FALSE) · . . .le(GMT 30m) (TRUE) · . . .le(GMT May 10h) (TRUE) · . . .le(GMT Jun 11h) (TRUE) · . . .le(GMT Wed) (TRUE) · . . .le(GMT May Sun_1) (TRUE)

<certificate>.VALID_NOT_AFTER.LT(<time>)	Returns a Boolean TRUE if the time precedes the <time> argum For example, if the current time is GMT 2005 May 1 10h 15m 3 and it is the first Sunday of the month, you can specify the following: · . . .lt(GMT 2006) (TRUE) · . . .lt(GMT 2005 Dec) (TRUE) · . . .lt(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.) · . . .lt(GMT 8h) (FALSE) · . . .lt(GMT 30m) (TRUE) · . . .lt(GMT May 10h) (FALSE) · . . .lt(GMT Jun 11h) (TRUE) · . . .lt(GMT Wed) (TRUE) · . . .lt(GMT May Sun_1) (FALSE)
<certificate>.VALID_NOT_AFTER.MINUTES	Extracts the last minute that the certificate is valid and return value as an integer from 0 to 59.
<certificate>.VALID_NOT_AFTER.MONTH	Extracts the last month that the certificate is valid and returns value as an integer from 1 (January) to 12 (December).
<certificate>.VALID_NOT_AFTER.RELATIVE_BOOT	Calculates the number of seconds to the closest previous or scheduled reboot and returns an integer. If the closest boot tir in the past, the integer is negative. If it is in the future, the in is positive.
<certificate>.VALID_NOT_AFTER.RELATIVE_NOW	Calculates the number of seconds between the current system and the specified time and returns an integer. If the time is in past, the integer is negative; if it is in the future, the integer i positive.
<certificate>.VALID_NOT_AFTER.SECONDS	Extracts the last second that the certificate is valid and return value as an integer from 0 to 59.
<certificate>.VALID_NOT_AFTER.WEEKDAY	Extracts the last weekday that the certificate is valid. Returns number between 0 (Sunday) and 6 (Saturday) to give the week the time value.

<certificate>.VALID_NOT_AFTER.WITHIN(<time1>, <time2>)	Returns a Boolean TRUE if the time lies within all the ranges de by the elements in <time1> and <time2>. If you omit an element of time from <time1>, it is assumed to the lowest value in its range. If you omit an element from <tim it is assumed to have the highest value of its range. If you spec year in <time1>, you must specify it in <time2>. The ranges for elements of time are as follows: month 1-12, da 1-31, weekday 0-6, hour 0-23, minutes 0-59 and seconds 0-59. the result to be TRUE, each element in the time must exist in t corresponding range that you specify in <time1>, <time2>. For example, if time is GMT 2005 May 10 10h 15m 30s, and it is second Tuesday of the month, you can specify the following (evaluation results are in parentheses): · . . .within(GMT 2004, GMT 2006) (TRUE) · . . .within(GMT 2004 Jan, GMT 2006 Mar) (FAL May is not in the range of January to March. · . . .within(GMT Feb, GMT) (TRUE, May is in t range for February to December) · . . .within(GMT Sun_1, GMT Sun_3) (TRUE, the second Tuesday lies within the range of the first Sunday through the third Sunday) · . . .within(GMT 2005 May 1 10h, GMT May 2005 17h) (TRUE) · . . .within(LOCAL 2005 May 1, LOCAL May 2005 (TRUE or FALSE, depending on the NetScaler system time zone)
<certificate>.VALID_NOT_AFTER.YEAR	Extracts the last year that the certificate is valid and returns a four-digit integer.
<certificate>.VALID_NOT_BEFORE	Returns the date that the client certificate becomes valid. The return format is the number of seconds since GMT January 1970 (0 hours, 0 minutes, 0 seconds).

`<certificate>.VALID_NOT_BEFORE.BETWEEN(<time1>, <time2>)`	Returns a Boolean TRUE if the time value is between the two t arguments. Both <time1> and <time2> arguments must be fully specified. Following are examples: · GMT 1995 Jan is fully specified. · GMT Jan is not fully specified. · GMT 1995 20 is not fully specified. · GMT Jan Mon_2 is not fully specified. The time arguments must be both GMT or both LOCAL, and <ti must be greater than <time1>. For example, if the time value is GMT 2005 May 1 10h 15m 30s it is the first Sunday of the month of May in 2005, you can spec the following (evaluation results for this example are in parentheses): · `. . .between(GMT 2004, GMT 2006) (TRUE)` · `. . .between(GMT 2004 Jan, GMT 2006 Nov) (TR` · `. . .between(GMT 2004 Jan, GMT 2006) (TRUE)` · `. . .between(GMT 2005 May Sun_1, GMT 2005 Ma Sun_3) (TRUE)` · `. . .between(GMT 2005 May 1, GMT May 2005 1) (TRUE)` · `. . .between(LOCAL 2005 May 1, LOCAL May 200 (TRUE or FALSE, depending on the NetScaler system time zone.)`
`<certificate>.VALID_NOT_BEFORE.DAY`	Extracts the last day of the month that the certificate is valid returns that value as a number from 1 through 31 representing day.

<certificate>.VALID_NOT_BEFORE.EQ(<time>)	Returns a Boolean TRUE if the time is equal to the <time> argument. For example, if the time value is GMT 2005 May 1 10h 15m 30s it is the first Sunday of the month of May in 2005, you can spec the following (evaluation results for this example are in parentheses): · . . .eq(GMT 2005) (TRUE) · . . .eq(GMT 2005 Dec) (FALSE) · . . .eq(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.) · . . .eq(GMT 10h) (TRUE) · . . .eq(GMT 10h 30s) (TRUE) · . . .eq(GMT May 10h) (TRUE) · . . .eq(GMT Sun) (TRUE) · . . .eq(GMT May Sun_1) (TRUE)
<certificate>.VALID_NOT_BEFORE.GE(<time>)	Returns a Boolean TRUE if the time is greater than (after) or e to the <time> argument. For example, if the time value is GMT 2005 May 1 10h 15m 30s it is the first Sunday of the month of May in 2005, you can spec the following (evaluation results are in parentheses): · . . .ge(GMT 2004) (TRUE) · . . .ge(GMT 2005 Jan) (TRUE) · . . .ge(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.) · . . .ge(GMT 8h) (TRUE) · . . .ge(GMT 30m) (FALSE) · . . .ge(GMT May 10h) (TRUE) · . . .ge(GMT May 10h 0m) (TRUE) · . . .ge(GMT Sun) (TRUE) · . . .ge(GMT May Sun_1) (TRUE)

<certificate>.VALID_NOT_BEFORE.GT(<time>)	Returns a Boolean TRUE if the time occurs after the <time> argument. For example, if the time value is GMT 2005 May 1 10h 15m 30s it is the first Sunday of the month of May in 2005, you can spec the following (evaluation results are in parentheses): · . . .gt(GMT 2004) (TRUE) · . . .gt(GMT 2005 Jan) (TRUE) · . . .gt(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.) · . . .gt(GMT 8h) (TRUE) · . . .gt(GMT 30m) (FALSE) · . . .gt(GMT May 10h) (FALSE) · . . .gt(GMT May 10h 0m) (TRUE) · . . .gt(GMT Sun) (FALSE) · . . .gt(GMT May Sun_1) (FALSE)
<certificate>.VALID_NOT_BEFORE.HOURS	Extracts the last hour that the certificate is valid and returns t value as an integer from 0 to 23.
<certificate>.VALID_NOT_BEFORE.LE(<time>)	Returns a Boolean TRUE if the time precedes or is equal to the <time> argument. For example, if the time value is GMT 2005 May 1 10h 15m 30s it is the first Sunday of the month of May in 2005, you can spec the following (evaluation results for this example are in parentheses): · . . .le(GMT 2006) (TRUE) · . . .le(GMT 2005 Dec) (TRUE) · . . .le(LOCAL 2005 May) (TRUE or FALSE,depen on the current time zone.) · . . .le(GMT 8h) (FALSE) · . . .le(GMT 30m) (TRUE) · . . .le(GMT May 10h) (TRUE) · . . .le(GMT Jun 11h) (TRUE) · . . .le(GMT Wed) (TRUE) · . . .le(GMT May Sun_1) (TRUE)

<certificate>.VALID_NOT_BEFORE.LT(<time>)	Returns a Boolean TRUE if the time precedes the <time> argum For example, if the time value is GMT 2005 May 1 10h 15m 30s, it is the first Sunday of the month of May in 2005, you can spec the following (evaluation results for this example are in parentheses): · . . .lt(GMT 2006) (TRUE) · . . .lt(GMT 2005 Dec) (TRUE) · . . .lt(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.) · . . .lt(GMT 8h) (FALSE) · . . .lt(GMT 30m) (TRUE) · . . .lt(GMT May 10h) (FALSE) · . . .lt(GMT Jun 11h) (TRUE) · . . .lt(GMT Wed) (TRUE) · . . .lt(GMT May Sun_1) (FALSE)
<certificate>.VALID_NOT_BEFORE.MINUTES	Extracts the last minute that the certificate is valid. Returns th current minute as an integer from 0 to 59.
<certificate>.VALID_NOT_BEFORE.MONTH	Extracts the last month that the certificate is valid. Returns th current month as an integer from 1 (January) to 12 (December
<certificate>.VALID_NOT_BEFORE.RELATIVE_BOOT	Calculates the number of seconds to the closest previous or scheduled NetScaler reboot and returns an integer. If the close boot time is in the past, the integer is negative; if it is in the future, the integer is positive.
<certificate>.VALID_NOT_BEFORE.RELATIVE_NOW	Returns the number of seconds between the current NetScaler system time and the specified time as an integer. If the design time is in the past, the integer is negative. If it is in the future integer is positive.
<certificate>.VALID_NOT_BEFORE.SECONDS	Extracts the last second that the certificate is valid. Returns th current second as an integer from 0 to 59.
<certificate>.VALID_NOT_BEFORE.WEEKDAY	Extracts the last weekday that the certificate is valid. Returns weekday as a number between 0 (Sunday) and 6 (Saturday).

`<certificate>.VALID_NOT_BEFORE.WITHIN(<time1>, <time2>)`	Returns a Boolean TRUE if each element of time exists within t range defined in the <time1>, <time2> arguments. If you omit an element of time from <time1>, it is assumed to the lowest value in its range. If you omit an element of time fr <time2>, it is assumed to have the highest value in its range. If specify a year in <time1>, it must be specified in <time2>. The ranges for elements of time are as follows: month 1-12, day 1- weekday 0-6, hour 0-23, minutes 0-59 and seconds 0-59. For example, if the time is GMT 2005 May 10 10h 15m 30s, and the second Tuesday of the month, you can specify the followin (evaluation results are in parentheses): · `. . .within(GMT 2004, GMT 2006) (TRUE)` · `. . .within(GMT 2004 Jan, GMT 2006 Mar)` (FALS is not in the range of January to March.) · `. . .within(GMT Feb, GMT)` (TRUE, May is in the ran February to December.) · `. . .within(GMT Sun_1, GMT Sun_3)` (TRUE, the se Tuesday is between the first Sunday and the third Sunday.) · `. . .within(GMT 2005 May 1 10h, GMT May 2005 17h) (TRUE)` · `. . .within(LOCAL 2005 May 1, LOCAL May 2005` (TRUE or FALSE, depending on the NetScaler system time z
`<certificate>.VALID_NOT_BEFORE.YEAR`	Extracts the last year that the certificate is valid. Returns the current year as a four-digit integer.

Expressions for HTTP Request and Response Dates

The following expression prefixes return the contents of the HTTP Date header as text or as a date object. These values can be evaluated as follows:

- As a number. The numeric value of an HTTP Date header is returned in the form of the number of seconds since Jan 1 1970.

  For example, the expression `http.req.date.mod(86400)` returns the number of seconds since the beginning of the day. These values can be evaluated using the same operations as other non-date-related numeric data. For more information, see "Expression Prefixes for Numeric Data Other Than Date and Time."

- As an HTTP header. Date headers can be evaluated using the same operations as other HTTP headers.

  For more information, see "Default Syntax Expressions: Parsing HTTP, TCP, and UDP Data."

- As text. Date headers can be evaluated using the same operations as other strings.

For more information, see "Default Syntax Expressions: Evaluating Text."

Table 1. Prefixes That Evaluate HTTP Date Headers

Prefix	Description
`HTTP.REQ.DATE`	Returns the contents of the HTTP Date header as text or as a date object. The date formats recognized are: RFC822. Sun, 06 Jan 1980 08:49:37 GMT RFC850. Sunday, 06-Jan-80 09:49:37 GMT ASCTIME. Sun Jan 6 08:49:37 1980
`HTTP.RES.DATE`	Returns the contents of the HTTP Date header as text or as a date object. The date formats recognized are: RFC822. Sun, 06 Jan 1980 8:49:37 GMT RFC850. Sunday, 06-Jan-80 9:49:37 GMT ASCTIME. Sun Jan 6 08:49:37 1980

Generating the Day of the Week, as a String, in Short and Long Formats

The functions, WEEKDAY_STRING_SHORT and WEEKDAY_STRING, generate the day of the week, as a string, in short and long formats, respectively. The strings that are returned are always in English. The prefix used with these functions must return the day of the week in integer format and the acceptable range for the value returned by the prefix is 0-6. Therefore, you can use any prefix that returns an integer in the acceptable range. An UNDEF condition is raised if the returned value is not in this range or if memory allocation fails.

Following are the descriptions of the functions:

Table 1. Functions That Generate the Day of the Week, as a String, in Short and Long Formats

Function	Description
<prefix>.WEEKDAY_STRING_SHORT	Returns the day of the week in short format. The short form is always 3 characters long with an initial capital and the remaining characters in lower case. For example, SYS.TIME.WEEKDAY.WEEKDAY_STRING_SHORT returns Sun if the value returned by the WEEKDAY function is 0 and Sat if the value returned by the prefix is 6.
<prefix>.WEEKDAY_STRING	Returns the day of the week in long format. The long form always has an initial capital, with the remaining characters in lower case. For example, SYS.TIME.WEEKDAY.WEEKDAY_STRING returns Sunday if the value returned by the WEEKDAY function is 0 and Saturday if the value returned by the prefix is 6.

Expression Prefixes for Numeric Data Other Than Date and Time

In addition to configuring expressions that operate on time, you can configure expressions for the following types of numeric data:

- The length of HTTP requests, the number of HTTP headers in a request, and so on.

  For more information, see "Expressions for Numeric HTTP Payload Data Other Than Dates."

- IP and MAC addresses.

  For more information, see "Expressions for IP Addresses and IP Subnets."

- Client and server data in regard to interface IDs and transaction throughput rate.

  For more information, see "Expressions for Numeric Client and Server Data."

- Numeric data in client certificates other than dates.

  For information on these prefixes, including the number of days until certificate expiration and the encryption key size, see "Prefixes for Numeric Data in SSL Certificates."

Converting Numbers to Text

The following functions produce binary strings from a number returned by an expression prefix. These functions are particularly useful in the TCP rewrite feature as replacement strings for binary data. For more information about the TCP rewrite feature, see "Rewrite."

All the functions return a value of type `text`. The `endianness` that some of the functions accept as a parameter is either LITTLE_ENDIAN or BIG_ENDIAN.

Table 1. Functions That Produce a Binary String From a Number

	Description
`TRING`	Produces an 8-bit signed binary string representing the number. If the value is out raised. **Example** `HTTP.REQ.BODY(100).GET_SIGNED8(16).SUB(3).SIGNED8_STRING`
`_STRING`	Produces an 8-bit unsigned binary string representing the number. If the value is ou raised. **Example** `HTTP.REQ.BODY(100).GET_UNSIGNED8(31).ADD(3).UNSIGNED8_STRING`
`STRING(<endianness>)`	Produces a 16-bit signed binary string representing the number. If the value is out raised. **Example** `HTTP.REQ.BODY(100).SKIP(12).GET_SIGNED16(0, BIG_ENDIAN).SUB(4).SIGNED16_STRING(BIG_ENDIAN)`
`6_STRING(<endianness>)`	Produces a 16-bit unsigned binary string representing the number. If the value is ou raised. **Example** `HTTP.REQ.BODY(100).GET_UNSIGNED16(47, LITTLE_ENDIAN).ADD(7).UNSIGNED16_STRING(LITTLE_ENDIAN)`
`STRING(<endianness>)`	Produces a 32-bit signed binary string representing the number. **Example** `HTTP.REQ.BODY(100).AFTER_STR("delim").GET_SIGNED32(0, BIG_ENDIAN).SUB(1).SIGNED32_STRING(BIG_ENDIAN)`

ber>.UNSIGNED8_STRING	Produces an 8-bit unsigned binary string representing the number. If the value is ou raised. **Example** `HTTP.REQ.BODY(100).GET_UNSIGNED8(24).TYPECAST_UNSIGNED_LONG_AT`
ber>.UNSIGNED16_STRING(<endianness>)	Produces a 16-bit unsigned binary string representing the number. If the value is ou raised. **Example** `HTTP.REQ.BODY(100).GET_UNSIGNED16(23, LITTLE_ENDIAN).TYPECAST_UNSIGNED_LONG_AT.ADD(10).UNSIGNED16_ST`
ber>.UNSIGNED32_STRING(<endianness>)	Produces a 32-bit unsigned binary string representing the number. If the value is ou raised. **Example** `HTTP.REQ.BODY(100).AFTER_STR("delim2").GET_UNSIGNED32(0, BIG_ENDIAN).ADD(2).UNSIGNED32_STRING(BIG_ENDIAN)`

Virtual Server Based Expressions

The SYS.VSERVER("<vserver-name>") expression prefix enables you to identify a virtual server. You can use the following functions with this prefix to retrieve information related to the specified virtual server:

- **THROUGHPUT.** Returns the throughput of the virtual server in Mbps (Megabits per second). The value returned is an unsigned long number.

  Usage: SYS.VSERVER("vserver").THROUGHPUT

- **CONNECTIONS.** Returns the number of connections being managed by the virtual server. The value returned is an unsigned long number.

  Usage: SYS.VSERVER("vserver").CONNECTIONS

- **STATE.** Returns the state of the virtual server. The value returned is UP, DOWN, or OUT_OF_SERVICE. One of these values can therefore be passed as an argument to the EQ() operator to perform a comparison that results in a Boolean TRUE or FALSE.

  Usage: SYS.VSERVER("vserver").STATE

- **HEALTH.** Returns the percentage of services in an UP state for the specified virtual server. The value returned is an integer.

  Usage: SYS.VSERVER("vserver").HEALTH

- **RESPTIME.** Returns the response time as an integer representing the number of microseconds. Response time is the average TTFB (Time To First Byte) from all the services bound to the virtual server.

  Usage: SYS.VSERVER("vserver").RESPTIME

- **SURGECOUNT.** Returns the number of requests in the surge queue of the virtual server. The value returned is an integer.

  Usage: SYS.VSERVER("vserver").SURGECOUNT

Example 1

The following rewrite policy aborts rewrite processing if the number of connections at the load balancing virtual server LBvserver exceeds 10000:

```
add rewrite policy norewrite_pol
sys.vserver("LBvserver").connections.gt(10000) norewrite
```

Example 2

The following rewrite action inserts a custom header, TP, whose value is the throughout at the virtual server LBvserver:

```
add rewrite action tp_header insert_http_header TP
SYS.VSERVER("LBvserver").THROUGHPUT
```

Example 3

The following audit log message action writes the average TTFB of the services bound to a virtual server, to the newnslog log file:

```
add audit messageaction log_vserver_resptime_act INFORMATIONAL "\"NS
Response Time to Servers:\" + sys.vserver(\"ssllb\").resptime + \"
millisec\"" -logtoNewnslog YES -bypassSafetyCheck YES
```

Default Syntax Expressions: Parsing HTTP, TCP, and UDP Data

You can configure default syntax expressions to evaluate and process the payload in HTTP requests and responses. The payload associated with an HTTP connection includes the various HTTP headers (both standard and custom headers), the body, and other connection information such as the URL. Additionally, you can evaluate and process the payload in a TCP or UDP packet. For HTTP connections, for example, you can check whether a particular HTTP header is present or if the URL includes a particular query parameter.

You can configure expressions to transform the URL encoding and apply HTML or XML “safe” coding for subsequent evaluation. You can also use XPATH and JSON prefixes to evaluate date in XML and JSON files, respectively.

You can also use text-based and numeric default syntax expressions to evaluate HTTP request and response data. For more information, see "Default Syntax Expressions: Evaluating Text" and "Default Syntax Expressions: Working with Dates, Times, and Numbers."

About Evaluating HTTP and TCP Payload

The payload of an HTTP request or response consists of HTTP protocol information such as headers, a URL, body content, and version and status information. When you configure a default syntax expression to evaluate HTTP payload, you use a default syntax expression prefix and, if necessary, an operator.

For example, you use the following expression, which includes the `http.req.header(“<header_name>“)` prefix and the `exists` operator, if you want to determine whether an HTTP connection includes a custom header named “myHeader”:

```
http.req.header("myHeader").exists
```

You can also combine multiple default syntax expressions with Boolean and arithmetic operators. For example, the following compound expression could be useful with various NetScaler features, such as Integrated Caching, Rewrite, and Responder. This expression first uses the && Boolean operator to determine whether an HTTP connection includes the Content-Type header with a value of "text/html." If that operation returns a value of FALSE, the expression determines whether the HTTP connection includes a "Transfer-Encoding" or "Content-Length" header.

```
(http.req.header("Content-Type").exists &&
http.req.header("Content-Type").eq("text/html")) ||
(http.req.header("Transfer-Encoding").exists) ||
(http.req.header("Content-Length").exists)
```

The payload of a TCP or UDP packet is the data portion of the packet. You can configure default syntax expressions to examine features of a TCP or UDP packet, including the following:

- Source and destination domains
- Source and destination ports
- The text in the payload
- Record types

The following expression prefixes extract text from the body of the payload:

- HTTP.REQ.BODY(integer). Returns the body of an HTTP request as a multiline text object, up to the character position designated in the *integer* argument. If there are fewer characters in the body than is specified in the argument, the entire body is returned.
- HTTP.RES.BODY(integer). Returns a portion of the HTTP response body. The length of the returned text is equal to the number in the *integer* argument. If there are fewer characters in the body than is specified in integer, the entire body is returned.
- CLIENT.TCP.PAYLOAD(integer). Returns TCP payload data as a string, starting with the first character in the payload and continuing for the number of characters in the

integer argument.

Following is an example that evaluates to TRUE if a response body of 1024 bytes contains the string “https”, and this string occurs after the string “start string” and before the string “end string”:

```
http.res.body(1024).after_str("start_string").before_str("end_string"
).contains("https")
```

Note: You can apply any text operation to the payload body. For information on operations that you can apply to text, see "Default Syntax Expressions: Evaluating Text."

Expressions for Identifying the Protocol in an Incoming IP Packet

The following table lists the expressions that you can use to identify the protocol in an incoming packet.

Expression	Description
CLIENT.IP.PROTOCOL	Identifies the protocol in IPv4 packets sent by clients.
CLIENT.IPV6.PROTOCOL	Identifies the protocol in IPv6 packets sent by clients.
SERVER.IP.PROTOCOL	Identifies the protocol in IPv4 packets sent by servers.
SERVER.IPV6.PROTOCOL	Identifies the protocol in IPv6 packets sent by servers.

Arguments to the PROTOCOL function

You can pass the Internet Assigned Numbers Authority (IANA) protocol number to the `PROTOCOL` function. For example, if you want to determine whether the protocol in an incoming packet is TCP, you can use `CLIENT.IP.PROTOCOL.EQ(6)`, where `6` is the IANA-assigned protocol number for TCP. For some protocols, you can pass an enumeration value instead of the protocol number. For example, instead of `CLIENT.IP.PROTOCOL.EQ(6)`, you can use `CLIENT.IP.PROTOCOL.EQ(TCP)`. The following table lists the protocols for which you can use enumeration values, and the corresponding enumeration values for use with the `PROTOCOL` function.

Protocol	Enumeration value
Transmission Control Protocol (TCP)	`TCP`
User Datagram Protocol (UDP)	`UDP`
Internet Control Message Protocol (ICMP)	`ICMP`
IP Authentication Header (AH), for providing authentication services in IPv4 and IPv6	`AH`
Encapsulating Security Payload (ESP) protocol	`ESP`
General Routing Encapsulation (GRE)	`GRE`
IP-within-IP Encapsulation Protocol	`IPIP`
Internet Control Message Protocol for IPv6 (ICMPv6)	`ICMPv6`
Fragment Header for IPv6	`FRAGMENT`

Use Case Scenarios

The protocol expressions can be used in both request-based and response-based policies. You can use the expressions in various NetScaler features, such as load balancing, WAN optimization, content switching, rewrite, and listen policies. You can use the expressions with functions such as `EQ()` and `NE()`, to identify the protocol in a policy and perform an action.

Following are some use cases for the expressions:

- In Branch Repeater load balancing configurations, you can use the expressions in a listen policy for the wildcard virtual server. For example, you can configure the wildcard virtual server with the listen policy `CLIENT.IP.PROTOCOL.EQ(TCP)` so that the virtual server processes only TCP traffic and simply bridges all non-TCP traffic. Even though you can use an Access Control List instead of the listen policy, the listen policy provides better control over what traffic is processed.

- For content switching virtual servers of type `ANY`, you can configure content switching policies that switch requests on the basis of the protocol in incoming packets. For example, you can configure content switching policies to direct all TCP traffic to one load balancing virtual server and all non-TCP traffic to another load balancing virtual server.

- You can use the client-based expressions to configure persistence based on the protocol. For example, you can use `CLIENT.IP.PROTOCOL` to configure persistence on the basis of the protocols in incoming IPv4 packets.

Expressions for HTTP and Cache-Control Headers

One common method of evaluating HTTP traffic is to examine the headers in a request or a response. A header can perform a number of functions, including the following:

- Provide cookies that contain data about the sender.
- Identify the type of data that is being transmitted.
- Identify the route that the data has traveled (the Via header).

Note: Note that if an operation is used to evaluate both header and text data, the header-based operation always overrides the text-based operation. For example, the AFTER_STR operation, when applied to a header, overrides text-based AFTER_STR operations for all instances of the current header type.

Prefixes for HTTP Headers

The following table describes expression prefixes that extract HTTP headers.

Table 1. Prefixes That Extract HTTP Headers

	Description
eader_name>")	Returns the contents of the HTTP header specified by the <header_nam cannot exceed 32 characters. Note that this prefix returns the value from the Host header by default you need to typecast it as follows: `http.req.header("host").typecast_http_hostname_t` For more information on typecasting, see "Typecasting Data."
R	Returns the contents of the complete set of HTTP header fields includi "GET /brochures/index.html HTTP/1.1") and the terminating \r\n\r\
	Returns the contents of the HTTP Date header. The following date form RFC822. Sun, 06 Jan 1980 8:49:37 GMT RFC850. Sunday, 06-Jan-80 9:49:37 GMT ASCII TIME. Sun Jan 6 08:49:37 1980 To evaluate a Date header as a date object, see "Default Syntax Expres and Numbers."
	(Name/Value List) Returns the contents of the HTTP Cookie header.

	Returns the HTTP transaction ID. The value is a function of an internal time and system MAC address.
eader_name>")	Returns the contents of the HTTP header specified by the <header_nam cannot exceed 32 characters.
R	Returns the contents of the complete set of HTTP header fields includi "HTTP/1.1 200 OK") and the terminating \r\n\r\n sequence.
2	Returns the HTTP Set-Cookie header object in a response.
("<name>") 2("<name>")	Returns the cookie of the specified name if it is present. If it is not pre 0. Returns UNDEF if more than 15 Set-Cookie headers are present and t these headers.
("<name>").DOMAIN 2("<name>").DOMAIN	Returns the value of the first Domain field in the cookie. For example, Customer = "ABC"; DOMAIN=".abc.com"; DOMAIN=.xyz.com, the followin `http.res.set_cookie.cookie("customer").domain` A string of zero length is returned if the Domain field or its value is abs
.EXISTS("<name>") 2.EXISTS("<name>")	Returns a Boolean TRUE if a Cookie with the name specified in the <nam Set-Cookie header. This prefix returns UNDEF if more than 15 Set-Cookie headers are prese the first 15 headers.
.COOKIE("<name>").EXPIRES 2.COOKIE("<name>").EXPIRES	Returns the Expires field of the cookie. This is a date string that can be object, or as text. If multiple Expires fields are present, the first one is absent, a text object of length zero is returned. To evaluate the returned value as a time object, see "Default Syntax Ex Times, and Numbers."

.COOKIE("<name>").PATH|PATH.GET(n)
2.COOKIE("<name>").PATH|PATH.GET(n)
	Returns the value of Path field of the cookie as a slash- (“/”) separated are treated as single slash. If multiple Path fields are present, the valu
	For example, the following is a cookie with two path fields:
	`Set-Cookie : Customer = "ABC"; PATH="/a//b/c"; PATH=`
	The following expression returns /a//b/c from this cookie:
	`http.res.set_cookie.cookie("Customer").path`
	The following expression returns b:
	`http.res.set_cookie.cookie("Customer").path.get(2)`
	Quotes are stripped from the returned value. A string of zero length is value is absent.

.COOKIE("<name>").PATH.IGNORE_EMPTY_ELEMENTS
 	
2.COOKIE("<name>").PATH.IGNORE_EMPTY_ELEMENTS
	Ignores the empty elements in the list. For example, in the list a=10,b=
	the list is , and the list has an empty element following a=10. The elem
	an empty element.
	
	As another example, in the following expression, if a request contains
	following expression returns a value of 4:
	
	`http.req.header("Cust_Header").typecast_list_t(',').i`
	
	The following expression returns a value of 5:
	
	`http.req.header("Cust_Header").typecast_list_t(',').c`

.COOKIE("<name>").PORT 2.COOKIE("<name>").PORT	Returns the value of Port field of the cookie. Operate as a comma-sepa For example, the following expression returns 80. 2580 from Set-Cookie PATH="/a/b/c"; PORT= "80, 2580": `http.res.set_cookie.cookie("ABC").port` A string of zero length is returned if the Port field or value is absent.

.COOKIE("<name>").PORT.IGNORE_EMPTY_ELEMENTS
 	
2.COOKIE("<name>").PORT.IGNORE_EMPTY_ELEMENTS
	Ignores the empty elements in the list. For example, in the list a=10,b=
	the list is , and the list has an empty element following a=10. The elem
	an empty element.
	
	As another example, in the following expression, if a request contains
	following expression returns a value of 4:
	
	`http.req.header("Cust_Header").typecast_list_t(',').i`
	
	The following expression returns a value of 5:
	
	`http.req.header("Cust_Header").typecast_list_t(',').c`

.COOKIE("<name>").VERSION 2.COOKIE("<name>").VERSION	Returns the value of the first Version field in the cookie as a decimal in For example, the following expression returns 1 from the cookie Set-Co "1"; VERSION = "0" `http.res.set_cookie.cookie("CUSTOMER").version` A zero is returned if the Version field or its value is absent or if the val
.COOKIE("<name>", <integer>) 2.COOKIE("<name>", <integer>)	Returns the nth instance (0-based) of the cookie with the specified nam text object of length 0. Returns UNDEF if more than 15 Set-Cookie headers are present and the
.COOKIE("<name>", <integer>).DOMAIN 2.COOKIE("<name>", <integer>).DOMAIN	Returns the value of the Domain field of the first cookie with the speci following expression returns a value of abc.com from the cookie Set-Co DOMAIN=".abc.com"; DOMAIN=.xyz.com `http.res.set_cookie.cookie("CUSTOMER").domain` A string of zero length is returned if the Domain field or its value is abs

.COOKIE("<name>", <integer>).EXPIRES 2.COOKIE("<name>", <integer>).EXPIRES	Returns the *n*th instance (0-based) of the Expires field of the cookie wi string. The value can be operated upon as a time object that supports Expires attribute is absent a string of length zero is returned.

.COOKIE("<name>", <integer>).PATH | PATH.GET(i)
 	
2.COOKIE("<name>", <integer>).PATH |
	Returns the value of the Path field of the nth cookie, as a '/' separated
	single /.
	
	For example, the following expression returns /a//b/c from the cookie
	PATH="/a//b/c"; PATH= "/x/y/z"
	
	`http.res.set_cookie.cookie("CUSTOMER").path`
	
	The following returns b:
	
	`http.res.set_cookie.cookie("CUSTOMER").path.get(2)`
	
	A string of zero length is returned if the Path field or its value is absen

.COOKIE("<name>",
ORE_EMPTY_ELEMENTS
 	
2.COOKIE("<name>",
ORE_EMPTY_ELEMENTS
	Ignores the empty elements in the list. For example, in the list a=10,b=
	the list is , and the list has an empty element following a=10. The elem
	an empty element.
	
	As another example, in the following expression, if a request contains
	following expression returns a value of 4:
	
	`http.req.header("Cust_Header").typecast_list_t(',').i`
	
	The following expression returns a value of 5:
	
	`http.req.header("Cust_Header").typecast_list_t(',').c`

.COOKIE("<name>", <integer>).PORT 2.COOKIE("<name>", <integer>).PORT	Returns the value or values of the Port field of the named cookie as a ' following expression returns 80, 2580 from the cookie Set-Cookie : Cust PORT= "80, 2580" `http.res.set_cookie.cookie("ABC").port` A string of zero length is returned if the Port field or its value is absent

.COOKIE("<name>",
ORE_EMPTY_ELEMENTS
 	
2.COOKIE("<name>",
ORE_EMPTY_ELEMENTS
	Ignores the empty elements in the list. For example, in the list a=10,b=
	the list is , and the list has an empty element following a=10. The elem
	an empty element.
	
	As another example, in the following expression, if a request contains
	following expression returns a value of 4:
	
	`http.req.header("Cust_Header").typecast_list_t(',').i`
	
	The following expression returns a value of 5:
	
	`http.req.header("Cust_Header").typecast_list_t(',').c`

.COOKIE("<name>", <integer>).VERSION 2.COOKIE("<name>", <integer>).VERSION	Returns the value of Version field of the *n*th cookie as a decimal intege A string of zero length is returned if the Port field or its value is absent
	Returns the HTTP transaction ID. The value is a function of an internal time and system MAC address.

Operations for HTTP Headers

The following table describes operations that you can specify with the prefixes for HTTP headers.

Table 2. Operations That Evaluate HTTP Headers

HTTP Header Operation	Description
`http header .EXISTS`	Returns a Boolean TRUE if an instance of the specified header type exists. Following is an example: `http.req.header("Cache-Control").exists`

`http header.CONTAINS" http header . CONTAINS("<string>")`	Returns a Boolean TRUE if the <string> argument appears in any instance of the header value.
	
	Note: This operation overrides any text-based Contains operations on all instances of the current header type.
	
	Following is an example of request with two headers:
	
	`HTTP/1.1 200 OK\r\n`
	
	`MyHeader: abc\r\n`
	
	`Content-Length: 200\r\n`
	
	`MyHeader: def\r\n`
	
	`\r\n`
	
	The following returns a Boolean TRUE:
	
	`http.res.header("MyHeader"). contains("de")`
	
	The following returns FALSE. Note that the NetScaler does not concatenate the different values.
	
	`http.res.header("MyHeader"). contains("bcd")`

`http header .COUNT`	Returns the number of headers in a request or response, to a maximum of 15 headers of the same type. The result is undefined if there are more than 15 instances of the header.
	
	Following is sample data in a request:
	
	`HTTP/1.1 200 OK\r\n`
	
	`MyHeader: abc\r\n`
	
	`Content-Length: 200\r\n`
	
	`MyHeader: def\r\n`
	
	`\r\n`
	
	When evaluating the preceding request, the following returns a count of 2:
	
	`http.res.header("MyHeader").count`

`http header.AFTER_STR("<string>")`	Extracts the text that follows the first occurrence of the <string> argument. The headers are evaluated from the last instance to the first.
	
	Following is an example of a request:
	
	`HTTP/1.1 200 OK\r\n`
	
	`MyHeader: 111abc\r\n`
	
	`Content-Length: 200\r\n`
	
	`MyHeader: 111def\r\n`
	
	`\r\n`
	
	The following extracts the string "def" from the last instance of MyHeader. This is value "111def."
	
	`http.res.header("MyHeader").after_str("111")`
	
	The following extracts the string "c" from the first instance of MyHeader. This is the value "abc111."
	
	`http.res.header("MyHeader").after_str("1ab")`

`http header.BEFORE_STR("<string>")`	Extracts the text that appears prior to the first occurrence of the input <string> argument. The headers are evaluated from the last instance to the first.
	
	Following is an example of a request that contains headers:
	
	`HTTP/1.1 200 OK\r\n`
	
	`MyHeader: abc111\r\n`
	
	`Content-Length: 200\r\n`
	
	`MyHeader: def111\r\n`
	
	`\r\n`
	
	The following extracts the string "def" from the last instance of MyHeader. This is the value "def111."
	
	`http.res.header("MyHeader").before_str("111")`
	
	The following extracts the string "a" from the first instance of MyHeader. This is the value "abc111."
	
	`http.res.header("MyHeader").before_str("bc1")`

`http header.INSTANCE(<instance number>)`	An HTTP header can occur multiple times in a request or a response. This operation returns the header that occurs <instance number> of places before the final instance. For example, instance(0) selects the last instance of the current type, instance(1) selects the next-to-last instance, and so on. This prefix cannot be used in bidirectional policies.
	
	The <instance number> argument cannot exceed 14. Following is an example of a request with two headers:
	
	`HTTP/1.1 200 OK\r\n`
	
	`MyHeader: abc\r\n`
	
	`Content-Length: 200\r\n`
	
	`MyHeader: def\r\n`
	
	`\r\n`
	
	The following returns a text object that refers to "MyHeader: abc\r\n":
	
	`http.res.header("MyHeader").instance(1)`

`http header.SUBSTR("<string>")`	Extracts the text that matches the <string> argument. The headers are evaluated from the last instance to the first. Following is an example of a request with two headers that contain the string “111”:
	
	`HTTP/1.1 200 OK\r\n`
	
	`MyHeader: abc111\r\n`
	
	`Content-Length: 200\r\n`
	
	`MyHeader: 111def\r\n`
	
	`\r\n`
	
	The following returns "111" from the last instance of MyHeader. This is the header with the value "111def."
	
	`http.res.header("MyHeader").substr("111")`

`http header.VALUE(<instance number>)`	An HTTP header can occur multiple times in a request or a response. VALUE(0) selects the value in the last instance, VALUE(1) selects the value in the next-to-last instance, and so on. The <instance number> argument cannot exceed 14.
	
	Following is an example of a request with two headers:
	
	`HTTP/1.1 200 OK\r\n`
	
	`MyHeader: abc\r\n`
	
	`Content-Length: 200\r\n`
	
	`MyHeader: def\r\n`
	
	`\r\n`
	
	The following returns "abc\r\n":
	
	`http.res.header("MyHeader").value(1)`

Prefixes for Cache-Control Headers

The following prefixes apply specifically to Cache-Control headers.

Table 3. Prefixes That Extract Cache-Control Headers

HTTP Header Prefix	Description
`HTTP.REQ.CACHE_CONTROL`	Returns a Cache-Control header in an HTTP request.
`HTTP.RES.CACHE_CONTROL`	Returns a Cache-Control header in an HTTP response.

Operations for Cache-Control Headers

You can apply any of the operations for HTTP headers to Cache-Control headers. For more information, see "Operations for HTTP Headers."

In addition, the following operations identify specific types of Cache-Control headers. See RFC 2616 for information about these header types.

Table 4. Operations That Evaluate Cache-Control Headers

HTTP Header Operation	Description
`Cache-Control header.NAME(<integer>)`	Returns as a text value the name of the Cache-Control header that corresponds to the nth component in a name-value list, as specified by <integer>. The index of the name-value component is 0-based. If the <integer> that is specified by the integer argument is greater than the number of components in the list, a zero-length text object is returned. Following is an example: `http.req.cache_control.name(3).contains("some_text")`
`Cache-Control header.IS_INVALID`	Returns a Boolean TRUE if the Cache-Control header is not present in the request or response. Following is an example: `http.req.cache_control.is_invalid`
`Cache-Control header.IS_PRIVATE`	Returns a Boolean TRUE if the Cache-Control header has the value Private. Following is an example: `http.req.cache_control.is_private`
`Cache-Control header.IS_PUBLIC`	Returns a Boolean TRUE if the Cache-Control header has the value Private. Following is an example: `http.req.cache_control.is_public`
`Cache-Control header.IS_NO_STORE`	Returns a Boolean TRUE if the Cache-Control header has the value No-Store. Following is an example: `http.req.cache_control.is_no_store`

`Cache-Control header.IS_NO_CACHE`	Returns a Boolean TRUE if the Cache-Control header has the value No-Cache. Following is an example: `http.req.cache_control.is_no_cache`
`Cache-Control header.IS_MAX_AGE`	Returns a Boolean TRUE if the Cache-Control header has the value Max-Age. Following is an example: `http.req.cache_control.is_max_age`
`Cache-Control header.IS_MIN_FRESH`	Returns a Boolean TRUE if the Cache-Control header has the value Min-Fresh. Following is an example: `http.req.cache_control.is_min_fresh`
`Cache-Control header.IS_MAX_STALE`	Returns a Boolean TRUE if the Cache-Control header has the value Max-Stale. Following is an example: `http.req.cache_control.is_max_stale`
`Cache-Control header.IS_MUST_REVALIDATE`	Returns a Boolean TRUE if the Cache-Control header has the value Must-Revalidate. Following is an example: `http.req.cache_control.is_must_revalidate`
`Cache-Control header.IS_NO_TRANSFORM`	Returns a Boolean TRUE if the Cache-Control header has the value No-Transform. Following is an example: `http.req.cache_control.is_no_transform`
`Cache-Control header.IS_ONLY_IF_CACHED`	Returns a Boolean TRUE if the Cache-Control header has the value Only-If-Cached. Following is an example: `http.req.cache_control.is_only_if_cached`
`Cache-Control header.IS_PROXY_REVALIDATE`	Returns a Boolean TRUE if the Cache-Control header has the value Proxy-Revalidate. Following is an example: `http.req.cache_control.is_proxy_revalidate`

`Cache-Control header.IS_S_MAXAGE`	Returns a Boolean TRUE if the Cache-Control header has the value S-Maxage. Following is an example: `http.req.cache_control.is_s_maxage`
`Cache-Control header.IS_UNKNOWN`	Returns a Boolean TRUE if the Cache-Control header is of an unknown type. Following is an example: `http.req.cache_control.is_unknown`
`Cache-Control header.MAX_AGE`	Returns the value of the Cache-Control header Max-Age. If this header is absent or invalid, 0 is returned. Following is an example: `http.req.cache_control.max_age.le(3)`
`Cache-Control header.MAX_STALE`	Returns the value of the Cache-Control header Max-Stale. If this header is absent or invalid, 0 is returned. Following is an example: `http.req.cache_control.max_stale.le(3)`
`Cache-Control header.MIN_FRESH`	Returns the value of the Cache-Control header Min-Fresh. If this header is absent or invalid, 0 is returned. Following is an example: `http.req.cache_control.min_fresh.le(3)`
`Cache-Control header.S_MAXAGE`	Returns the value of the Cache-Control header S-Maxage. If this header is absent or invalid, 0 is returned. Following is an example: `http.req.cache_control.s_maxage.eq(2)`

Expressions for Extracting Segments of URLs

You can extract URLs and portions of URLs, such as the host name, or a segment of the URL path. For example, the following expression identifies HTTP requests for image files by extracting image file suffixes from the URL:

```
http.req.url.suffix.eq("jpeg") || http.req.url.suffix.eq("gif")
```

Most expressions for URLs operate on text and are described in "Expression Prefixes for Text in HTTP Requests and Responses." This section discusses the GET operation. The GET operation extracts text when used with the following prefixes:

- `HTTP.REQ.URL.PATH`
- `VPN.BASEURL.PATH`
- `VPN.CLIENTLESS_BASEURL.PATH`

The following table describes prefixes for HTTP URLs.

Table 1. Prefixes That Extract URLs

URL Prefix	Description

`HTTP.REQ.URL.PATH.GET(<n>)`	Returns a slash- (“/”) separated list from the URL path. For example, consider the following URL:
	
	`http://www.mycompany.com/dir1/dir2/dir3/index.html?a=1`
	
	The following expression returns dir1 from this URL:
	
	`http.req.url.path.get(1)`
	
	The following expression returns dir2:
	
	`http.req.url.path.get(2)`

`HTTP.REQ.URL.PATH.GET_REVERSE(<n>)`	Returns a slash- (“/”) separated list from the URL path, starting from the end of the path. For example, consider the following URL:
	
	`http://www.mycompany.com/dir1/dir2/dir3/index.html?a=1`
	
	The following expression returns index.html from this URL:
	
	`http.req.url.path.get_reverse(0)`
	
	The following expression returns dir3:
	
	`http.req.url.path.get_reverse(1)`

Expressions for HTTP Status Codes and Numeric HTTP Payload Data Other Than Dates

The following table describes prefixes for numeric values in HTTP data other than dates.

Table 1. Prefixes That Evaluate HTTP Request or Response Length

Prefix	Description
`HTTP.REQ.CONTENT_LENGTH`	Returns the length of an HTTP request as a number. Following is an example: `http.req.content_length < 500`
`HTTP.RES.CONTENT_LENGTH`	Returns the length of the HTTP response as a number. Following is an example: `http.res.content_length <= 1000`
`HTTP.RES.STATUS`	Returns the response status code

HTTP.RES.IS_REDIRECT	Returns a Boolean TRUE if the response code is associated with a redirect. Following are the redirect response codes:
	· 300 (Multiple Choices)
	· 301 (Moved Permanently)
	· 302 (Found)
	· 303 (See Other)
	· 305 (Use Proxy)
	· 307 (Temporary Redirect)
	Note: Status code 304 is not considered a redirect HTTP response status code. Status code 306 is unused.
	In the following example, the rewrite action replaces http in the Location header of an HTTP response with https if the response is associated with an HTTP redirect.
	`add rewrite action redloc replace 'http.res.header("Location").before_regex(re#://#)' '"https"'`
	`add rewrite policy pol1 HTTP.RES.IS_REDIRECT red_location`
	`bind rewrite global pol1 100`

SIP Expressions

Introduction

The NetScaler default expressions language contains a number of expressions that operate on Session Initiation Protocol (SIP) connections. These expressions are intended to be used in policies for any supported protocol that operates on a request/response basis. (These expressions can be bound only to `sip_udp` virtual servers and global bind points.) These expressions can be used in content switching, rate limiting, responder, and rewrite policies.

Certain limitations apply to SIP expressions used with responder policies. The NetScaler operating system currently supports only SIP over UDP. Only the DROP, NOOP or RESPONDWITH actions are allowed on a SIP load balancing virtual server. Responder policies can be bound to a load balancing virtual server, an override global bind point, a default global bind point, or a `sip_udp` policy label.

The header format used by the SIP protocol is similar to that used by the HTTP protocol, so many of the new expressions look and function much like their HTTP analogs. Each SIP header consists of a line that includes the SIP method, the URL, and the version, followed by a series of name-value pairs that look like HTTP headers.

Following is a sample SIP header that is referred to in the expressions tables beneath it:

```
INVITE sip:16@www.sip.com:5060;transport=udp SIP/2.0
Record-Route: <sip:200.200.100.22;lr=on>
Via: SIP/2.0/UDP 200.200.100.22;branch=z9hG4bK444b.c8e103d1.0;rport=5060;
   received=10.102.84.18
Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;
   received=10.102.84.160
From: "12" <sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185
To: "16" <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185
Call-ID: 00127f54-ec850017-0e46f5b9-5ec149c2@10.102.84.180
Max-Forwards: 69CSeq: 101 INVITE
User-Agent: Cisco-CP7940G/8.0
Contact: <sip:12@10.102.84.180:5060;transport=udp>
Expires: 180
Accept: application/sdp
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE
Supported: replaces,join,norefersub
Content-Length: 277
Content-Type: application/sdp
Content-Disposition: session;handling=optiona
```

SIP Reference Tables

The following tables contain lists of expressions that operate on SIP headers. The first table contains expressions that apply to request headers. Most response-based expressions are nearly the same as the corresponding request-based expressions. To create a response expression from the corresponding request expression, you change the first two sections of the expression from `SIP.REQ` to `SIP.RES`, and make other obvious adjustments. The second table contains those response expressions that are unique to responses and have no request equivalents. You can use any element in the following tables as a complete expression on its own, or you can use various operators to combine these expression elements with others to form more complex expressions.

Table 1. SIP Request Expressions

	Description
	Operates on the method of the SIP request. The supported SIP request me MESSAGE, NOTIFY, OPTIONS, PRACK, PUBLISH, REFER, REGISTER, SUBSCRIB the text class, so all operations that are applicable to text are applicable `INVITE sip:16@10.102.84.181:5060;transport=udp SIP/2.0`, t
	Operates on the SIP request URL. This expression is a derivative of the tex are applicable to this method. For example, for a SIP request of `INVITE sip:16@10.102.84.181:5060;transport=udp SIP/2.0`, this expre `sip:16@10.102.84.181:5060;transport=udp`.
	Returns the URL protocol. For example, for a SIP URL of `sip:16@www.si` returns `sip`.
	Returns the hostname portion of the SIP URL. For example, for a SIP URL o this expression returns `www.sip.com:5060`.
	Returns the port portion of the SIP URL hostname. If no port is specified, t For example, for a SIP hostname of `www.sip.com:5060`, this expression
	Returns the domain name portion of the SIP URL hostname. If the host is a incorrect result. For example, for a SIP hostname of `www.sip.com:5060` hostname of `192.168.43.15:5060`, this expression returns an error.
	Returns the server portion of the host. For example, for a SIP hostname of
	Returns the username that precedes the @ character. For example, for a S sip:16@www.sip.com:5060;transport=udp, this expression returns 16.
	Returns the SIP version number in the request. For example, for a SIP requ `sip:16@10.102.84.181:5060;transport=udp SIP/2.0`, this expre
	Returns the major version number (the number to the left of the period). this expression returns 2.
	Returns the minor version number (the number to the right of the period). `SIP/2.0`, this expression returns `0`.
	Returns the contents of the Content-Length header. This expression is a de operations that are available for SIP headers can be used. For example, fo `Content-Length: 277`, this expression returns 277.
	Returns the contents of the To header. For example, for a SIP To header o `<sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53` `<sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53`

	Returns the SIP URI, which is found in the sip_url object. All operations tha example, for a SIP To header of `To: "16" <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53 sip:16@sip_example.com`.
	Returns the display name portion of the To header. For example, for a SIP `<sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53`
	Returns the “tag” vale from the “tag” name value pair in the TO header. F `<sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53 00127f54ec85a6d90cc14f45-53cc0185`.
	Returns the contents of the From header. For example, for a SIP From hea `<sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53 sip:12@sip_example.com`.
	Returns the SIP URI, which is found in the sip_url object. All operations tha example, for a SIP From header of `From: "12" <sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53 sip:12@sip_example.com`.
	Returns the display name portion of the To header. For example, for a SIP `<sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53`
	Returns the “tag” value from the “tag” name/value pair in the TO header. `"12" <sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f 00127f54ec85a6d90cc14f45-53cc0185`.
	Returns the complete Via header. If there are multiple Via headers in the for the two Via headers in the sample SIP header, this expression returns `10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;rec`
	Returns the address that sent the request. For example, for the Via heade `10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;rec 10.102.84.180`.
	Returns the port that sent the request. For example, for the Via header `Vi 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;rec 5060`.
	Returns the value from the rport name/value pair. For example, for the Vi `10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;rec 5060`.
	Returns the value from the branch name/value pair. For example, for the `10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;rec z9hG4bK03e76d0b`.
	Returns the value from the received name/value pair. For example, for th `10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;rec 10.102.84.160`.
	Returns the contents of the Callid header. This expression is a derivative c are available for SIP headers can be used. For example, for a SIP Callid hea `00127f54-ec850017-0e46f5b9-5ec149c2@10.102.84.180`, this exp `00127f54-ec850017-0e46f5b9-5ec149c2@10.102.84.180`.
	Returns the CSEQ number from the CSEQ, as an integer. For example, for a expression returns `101`.
)	Returns the specified SIP header. For `<header_name>`, substitute the nam return the SIP From header, you would type `SIP.REQ.HEADER("From")`.

.INSTANCE(<line_number>)	Returns the specified instance of the specified SIP header. Multiple instanc want a specific instance of such a SIP header (for example, a specific Via h number as the <line_number>. Header instances are matched from last SIP.REQ.HEADER("Via").INSTANCE(0) returns the last instance of th SIP.REQ.HEADER("Via").INSTANCE(1) returns the last instance but For example, if used on the example SIP header, SIP.REQ.HEADER("Via 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060.
.VALUE(<line_number>)	Returns the contents of the specified instance of the specified SIP header. expression. For example, if used on the SIP header example in the precedi SIP.REQ.HEADER("Via").VALUE(1) returns SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060.
.COUNT	Returns the number of instances of a particular header as an integer. For e SIP.REQ.HEADER("Via").COUNT returns 2.
.EXISTS	Returns a boolean value of true or false, depending upon whether the spec the SIP header example above, SIP.REQ.HEADER("Expires").EXISTS SIP.REQ.HEADER("Caller-ID").EXISTS returns false.
.LIST	Returns the comma-separated parameter list in the specified header. For e SIP.REQ.HEADER("Allow").LIST returns ACK,BYE,CANCEL,INVITE,NOTIFY,OP You can append the string .GET(<list_item_number>) to select a specific li from the above list, you would type SIP.REQ.HEADER("Allow").LIST.GET(0) SIP.REQ.HEADER("Allow").LIST.GET(1). **Note:** If the specified header contains a list of name/value pairs, the ent
.TYPECAST_SIP_HEADER_T("<in_header_name>")	Typecasts <header_name> to <in_header_name>. Any text can be typ all header-based operations can be used. After you perform this operation <in_header_name>. For example, the expression SIP.REQ.CONTENT_LENGTH.TYPECAST_SI Content-Length header. After you perform this operation, you can apply a header.
.CONTAINS("<string>").	Returns boolean true if the specified text string is present in any instance instances of the specified header. Header instances are matched from last
.EQUALS_ANY(<patset>)	Returns boolean true if any pattern associated with <patset> matches a Operates on all the instances of the specified header. Header instances ar
.CONTAINS_ANY(<patset>)	Returns Boolean true if any pattern associated with <patset> matches a Operates on all the instances of the specified header. Header instances ar
.CONTAINS_INDEX(<patset>)	Returns the index of the matching pattern associated with <patset> if th the specified header. Operates on all the instances of the specified heade first.
.EQUALS_INDEX(<patset>)	Returns the index of the matching pattern associated with <patset> if that header. Operates on all the instances of the specified header. Header inst
.SUBSTR("<string>")	If the specified string is present in any instance of the specified header, th the SIP header Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;rec SIP.REQ.HEADER("Via").SUBSTR("rport=5060") returns "rport= SIP.REQ.HEADER("Via").SUBSTR("rport=5061") returns an empty

.AFTER_STR("<string>")	If the specified string is present in any instance of the specified header, th that string. For example, for the SIP header `Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;rec` `SIP.REQ.HEADER("Via").AFTER_STR("rport=")` returns `5060`.
.REGEX_MATCH(<regex>)	Returns boolean true if the specified regular expression (*regex*) matches a specify the regular expression in the following format: re<delimiter>regular expression<same delimiter> The regular expression cannot be larger than 1499 characters in length. It library. See http://www.pcre.org/pcre.txt for documentation on PCRE reg page also has useful information on specifying patterns by using PCRE regu The regular expression syntax supported in this expression has some differ You should avoid recursive regular expressions; although some work, many newlines. Unicode is not supported. `SET_TEXT_MODE(IGNORECASE)` ove regular expression.
.REGEX_SELECT(<regex>)	If the specified regex matches any text in any instance of the specified he for the SIP header `Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;rec` `SIP.REQ.HEADER("Via").REGEX_SELECT("received=[0-9]{1,3}\` returns `received=10.102.84.160`.
.AFTER_REGEX(<regex>)	If the specified regex matches any text in any instance of the specified he after that text. For example, for the SIP header `Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;rec` `SIP.REQ.HEADER("Via").AFTER_REGEX("received=")` returns `10.`
.BEFORE_REGEX(<regex>)	If the specified regex matches any text in any instance of the specified he before that text. For example, for the SIP header `Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;rec` `SIP.REQ.HEADER("Via").BEFORE_REGEX("[0-9]{1,3}\.[0-9]{1,` `received=`.
	Returns the entire SIP header, including the terminating CR/LF.
	Returns boolean `true` if the request format is valid.
	Returns the request body, up to the specified length. If the specified lengt this expression returns the entire request body.
	Returns the name of the load balancing virtual server (*LB vserver*) that is s
	Returns the name of the content switching virtual server (*CS vserver*) that

Table 2. SIP Response Expressions

Expression	Description
`SIP.RES.STATUS`	Returns the SIP response status code. For example, if the first line of the response is `SIP/2.0 100 Trying`, this expression returns `100`.
`SIP.RES.STATUS_MSG`	Returns the SIP response status message. For example, if the first line of the response is `SIP/2.0 100 Trying`, this expression returns `Trying`.

SIP.RES.IS_REDIRECT	Returns boolean `true` if the response code is a redirect.
SIP.RES.METHOD	Returns the response method extracted from the request method string in the CSeq header.

Operations for HTTP, HTML, and XML Encoding and “Safe” Characters

The following operations work with the encoding of HTML data in a request or response and XML data in a POST body.

Table 1. Operations That Evaluate HTML and XML Encoding

peration	Description
_XML_SAFE	Transforms special characters into XML safe format, examples: · A left-pointing angle bracket (<) is converted to · A right-pointing angle bracket (>) is converted to · An ampersand (&) is converted to & This operation safeguards against cross-site scripting of the transformed text is 2048 bytes. This is a read- After applying the transformation, additional operat expression are applied to the selected text. Followin `http.req.url.query.html_xml_safe. conta`
_HEADER_SAFE	Converts all new line ('\n') characters in the input te input to be used safely in HTTP headers. This operation safeguards against response-splitting The maximum length of the transformed text is 2048 operation.

_URL_SAFE	Converts unsafe URL characters to '%xx' values, wher representation of the input character. For example, represented as %26 in URL-safe encoding. The maxin transformed text is 2048 bytes. This is a read-only o Following are URL safe characters. All others are uns · Alpha-numeric characters: a-z, A-Z, 0-9 · Asterix: "*" · Ampersand: "&" · At-sign: "@" · Colon: ":" · Dollar: "$" · Dot: "." · Equals: "=" · Exclamation mark: "!" · Hyphen: "-" · Open and close parentheses: "(", ")" · Plus: "+" · Semicolon: ";" · Single quote: "'" · Slash: "/" · Tilde: "~" · Underscore: "_"
_SAFE	Marks the text as safe without applying any type of

TEXT_MODE(URLENCODED|NOURLENCODED)	Transforms all %HH encoding in the byte stream. Thi characters (not bytes). By default, a single byte repr ASCII encoding. However, if you specify URLENCODE represent a character.
	
	In the following example, a PREFIX(3) operation sele in a target.
	
	`http.req.url.hostname.prefix(3)`
	
	In the following example, the NetScaler can select u target:
	
	`http.req.url.hostname.set_text_mode(url`

TEXT_MODE(PLUS_AS_SPACE|NO_PLUS_AS_SPACE)	Specifies how to treat the plus character (+). The PL replaces a plus character with white space. For exar “hello+world” becomes “hello world.” The NO_PLUS plus characters as they are.
TEXT_MODE(BACKSLASH_ENCODED|NO_BACKSLASH_ENCODED)	Specifies whether or not backslash decoding is perfo represented by <text>. If BACKSLASH_ENCODED is specified, the SET_TEX performs the following operations on the text object · All occurrences of “\XXX” will be replaced with t XXX represents a number in the octal system and equivalent of XXX). The valid range of octal valu encoding is 0 to 377. For example, the encoded "http\072//" will both be decoded to "http://", w ASCII equivalent of the octal value “72”. · All occurrences of “\xHH” will be replaced with represents a number in the hexadecimal system equivalent of HH. For example, the encoded tex decoded to "http://", where the colon (:) is the hexadecimal value “3a“. · All occurrences of “\\uWWXX” will be replaced w sequence “YZ” (Where WW and XX represent tw values and Y and Z represent their ASCII equivale respectively. For example, the encoded text "ht "http%u003a//" will both be decoded to "http:// are two hexadecimal values and the colon (:) an represent their ASCII equivalents respectively. · All occurrences of "\b", "\n", "\t", "\f", and "\r" are corresponding ASCII characters. If NO_BACKSLASH_ENCODED is specified, backslash performed on the text object.

TEXT_MODE(BAD_ENCODE_RAISE_UNDEF|NO_BAD_ENCODE_RAISE_UNDEF)	Performs the associated undefined action if either th BACKSLASH_ENCODED mode is set and bad encodin specified encoding mode is encountered in the text <text>. If NO_BAD_ENCODE_RAISE_UNDEF is specified, the action will not be performed when bad encoding is e object represented by<text>.

Expressions for TCP, UDP, and VLAN Data

TCP and UDP data take the form of a string or a number. For expression prefixes that return string values for TCP and UDP data, you can apply any text-based operations. For more information, see "Default Syntax Expressions: Evaluating Text."

For expression prefixes that return numeric value, such as a source port, you can apply an arithmetic operation. For more information, see "Basic Operations on Expression Prefixes" and "Compound Operations for Numbers."

The following table describes prefixes that extract TCP and UDP data.

Table 1. Prefixes That Extract TCP and UDP Data

GET Operation	Description
`CLIENT.TCP.PAYLOAD(<integer>)`	Returns TCP payload data as a string, starting with the first character in the payload and continuing for the number of characters in the <integer> argument. You can apply any text-based operation to this prefix.
`CLIENT.TCP.SRCPORT`	Returns the ID of the current packet's source port as a number.
`CLIENT.TCP.DSTPORT`	Returns the ID of the current packet's destination port as a number.
`CLIENT.TCP.OPTIONS`	Returns the TCP options set by the client. Examples of TCP options are Maximum Segment Size (MSS), Window Scale, Selective Acknowledgements (SACK), and Time Stamp Option. The `COUNT`, `TYPE(<type>)`, and `TYPE_NAME(<m>)` operators can be used with this prefix. For the TCP options set by the server, see the `SERVER.TCP.OPTIONS` prefix.
`CLIENT.TCP.OPTIONS.COUNT`	Returns the number of TCP options that the client has set.

`CLIENT.TCP.OPTIONS.TYPE(<type>)`	Returns the value of the TCP option whose type (or *option kind*) is specified as the argument. The value is returned as a string of bytes in big endian format (or *network byte order*). **Parameters:** `type` - Type value
`CLIENT.TCP.OPTIONS.TYPE_NAME(<m>)`	Returns the value of the TCP option whose enumeration constant is specified as the argument. The enumeration constants that you can pass as the argument are REPEATER, TIMESTAMP, SACK_PERMITTED, WINDOW, and MAXSEG. To specify the TCP option kind instead of these enumeration constants, use `CLIENT.TCP.OPTIONS.TYPE(<type>)`. For other TCP options, you must use `CLIENT.TCP.OPTIONS.TYPE(<type>)`. **Parameters:** `m` - TCP option enumeration constant
`CLIENT.TCP.REPEATER_OPTION.EXISTS`	Returns a Boolean TRUE if Repeater TCP options exist.
`CLIENT.TCP.REPEATER_OPTION.IP`	Returns the branch repeater's IPv4 address from the Repeater TCP options.
`CLIENT.TCP.REPEATER_OPTION.MAC`	Returns the branch repeater's MAC address from the Repeater TCP options.
`CLIENT.UDP.DNS.DOMAIN`	Returns the DNS domain name.
`CLIENT.UDP.DNS.DOMAIN.EQ("<hostname>")`	Returns a Boolean TRUE if the domain name matches the <hostname> argument. The comparison is case insensitive. Following is an example: `client.udp.dns.domain.eq("www.mycompany.com")`
`CLIENT.UDP.DNS.IS_AAAAREC`	Returns a Boolean TRUE if the record type is AAAA. These types of records indicate an IPv6 address in forward lookups.
`CLIENT.UDP.DNS.IS_ANYREC`	Returns a Boolean TRUE if it is of any record type.
`CLIENT.UDP.DNS.IS_AREC`	Returns a Boolean TRUE if the record is type A. Type A records provide the host address.

CLIENT.UDP.DNS.IS_CNAMEREC	Returns a Boolean TRUE if the record is of type CNAME. In systems that use multiple names to identify a resource, there is one canonical name and a number of aliases. The CNAME provides the canonical name.
CLIENT.UDP.DNS.IS_MXREC	Returns a Boolean TRUE if the record is of type MX (mail exchanger). This DNS record describes a priority and a host name. The MX records for the same domain name specify the email servers in the domain and the priority for each server.
CLIENT.UDP.DNS.IS_NSREC	Returns a Boolean TRUE if the record is of type NS. This is a name server record that includes a host name with an associated A record. This enables locating the domain name that is associated with the NS record.
CLIENT.UDP.DNS.IS_PTRREC	Returns a Boolean TRUE if the record is of type PTR. This is a domain name pointer and is often used to associate a domain name with an IPv4 address.
CLIENT.UDP.DNS.IS_SOAREC	Returns a Boolean TRUE if the record is of type SOA. This is a start of authority record.
CLIENT.UDP.DNS.IS_SRVREC	Returns a Boolean TRUE if the record is of type SRV. This is a more general version of the MX record.
CLIENT.UDP.DSTPORT	Returns the numeric ID of the current packet's UDP destination port.
CLIENT.UDP.SRCPORT	Returns the numeric ID of the current packet's UDP source port.
CLIENT.UDP.RADIUS	Returns RADIUS data for the current packet.
CLIENT.UDP.RADIUS.ATTR_TYPE(<type>)	Returns the value for the attribute type specified as the argument.
CLIENT.UDP.RADIUS.USERNAME	Returns the RADIUS user name.
CLIENT.TCP.MSS	Returns the maximum segment size (MSS) for the current connection as a number.
CLIENT.VLAN.ID	Returns the numeric ID of the VLAN through which the current packet entered the NetScaler.
SERVER.TCP.DSTPORT	Returns the numeric ID of the current packet's destination port.
SERVER.TCP.SRCPORT	Returns the numeric ID of the current packet's source port.

SERVER.TCP.OPTIONS	Returns the TCP options set by the server. Examples of TCP options are Maximum Segment Size (MSS), Window Scale, Selective Acknowledgements (SACK), and Time Stamp Option. The COUNT, TYPE(<type>), and TYPE_NAME(<m>) operators can be used with this prefix. For the TCP options set by the client, see the CLIENT.TCP.OPTIONS prefix.
SERVER.TCP.OPTIONS.COUNT	Returns the number of TCP options that the server has set.
SERVER.TCP.OPTIONS.TYPE(<type>)	Returns the value of the TCP option whose type (or *option kind*) is specified as the argument. The value is returned as a string of bytes in big endian format (or *network byte order*). **Parameters:** type - Type value
SERVER.TCP.OPTIONS.TYPE_NAME(<m>)	Returns the value of the TCP option whose enumeration constant is specified as the argument. The enumeration constants that you can pass as the argument are REPEATER, TIMESTAMP, SACK_PERMITTED, WINDOW, and MAXSEG. To specify the TCP option kind instead of these enumeration constants, use CLIENT.TCP.OPTIONS.TYPE(<type>). For other TCP options, you must use CLIENT.TCP.OPTIONS.TYPE(<type>). **Parameters:** m - TCP option enumeration constant
SERVER.VLAN	Operates on the VLAN through which the current packet entered the NetScaler.
SERVER.VLAN.ID	Returns the numeric ID of the VLAN through which the current packet entered the NetScaler.

Expressions for Evaluating a DNS Message and Identifying Its Carrier Protocol

You can evaluate DNS requests and responses by using expressions that begin with `DNS.REQ` and `DNS.RES`, respectively. You can also identify the transport layer protocol that is being used to send the DNS messages.

The following functions return the contents of a DNS query.

Table 1. Functions that return the contents of a DNS query

Function	Description
`DNS.REQ.QUESTION.DOMAIN`	Return the domain name (the value of the `QNAME` field) in the question section of the DNS query. The domain name is returned as a text string, which can be passed to `EQ()`, `NE()`, and any other functions that work with text.

DNS.REQ.QUESTION.TYPE	Return the query type (the value of the QTYPE field) in the DNS query. The field indicates the type of resource record (for example, A, NS, or CNAME) for which the name server is being queried. The returned value can be compared to one of the following values by using the EQ() and NE() functions: · A · AAAA · NS · SRV · PTR · CNAME · SOA · MX · ANY **Note:** You can use only the EQ() and NE() functions with the TYPE function. **Example:** DNS.REQ.QUESTION.TYPE.EQ(MX)

The following functions return the contents of a DNS response.

Table 2. Functions that return the contents of a DNS response

Function	Description
DNS.RES.HEADER.RCODE	Return the response code (the value of the RCODE field) in the header section of the DNS response. You can use only the EQ() and NE() functions with the RCODE function. Following are the possible values: · NOERROR · FORMERR · SERVFAIL · NXDOMAIN · NOTIMP · REFUSED

DNS.RES.QUESTION.DOMAIN	Return the domain name (the value of the QNAME field) in the question section of the DNS response. The domain name is returned as a text string, which can be passed to EQ(), NE(), and any other functions that work with text.
DNS.RES.QUESTION.TYPE	Return the query type (the value of the QTYPE field) in the question section of the DNS response. The field indicates the type of resource record (for example, A, NS, or CNAME) that is contained in the response. The returned value can be compared to one of the following values by using the EQ() and NE() functions: · A · AAAA · NS · SRV · PTR · CNAME · SOA · MX · ANY You can use only the EQ() and NE() functions with the TYPE function. **Example:** DNS.RES.QUESTION.TYPE.EQ(SOA)

The following functions return the transport layer protocol name.

Table 3. Functions that return the transport layer protocol name

Function	Description
DNS.REQ.TRANSPORT	Return the name of the transport layer protocol that was used to send the DNS query. Possible values returned are TCP and UDP. You can use only the EQ() and NE() functions with the TRANSPORT function. **Example:** DNS.REQ.TRANSPORT.EQ(TCP)

DNS.RES.TRANSPORT	Return the name of the transport layer protocol that was used for the DNS response. Possible values returned are TCP and UDP. You can use only the EQ() and NE() functions with the TRANSPORT function. **Example:** DNS.RES.TRANSPORT.EQ(TCP)

XPath and HTML, XML, or JSON Expressions

The default syntax expression engine supports expressions for evaluating and retrieving data from HTML, XML, and JavaScript Object Notation (JSON) files. This enables you to find specific nodes in an HTML, XML, or JSON document, determine if a node exists in the file, locate nodes in XML contexts (for example, nodes that have specific parents or a specific attribute with a given value), and return the contents of such nodes. Additionally, you can use XPath expressions in rewrite expressions.

The default syntax expression implementation for XPath comprises a default syntax expression prefix (such as "`HTTP.REQ.BODY`") that designates HTML or XML text, and the XPATH operator that takes the XPath expression as its argument.

HTML files are a largely free-form collection of tags and text elements. You can use the XPATH_HTML operator, which takes an XPath expression as its argument, to process HTML files. JSON files are either a collection of name/value pairs or an ordered list of values. You can use the XPATH_JSON operator, which takes an XPath expression as its argument, to process JSON files.

Table 1. XPath and JSON Expression Prefixes That Return Text

XPath Prefix	Description
`<text>.XPATH(xpathex)`	Operate on an XML file and return a Boolean value. For example, the following expression returns a Boolean TRUE if a node calle "creator" exists under the node "Book" within the first 1000 bytes of the XM `HTTP.REQ.BODY(1000).XPATH(xp%boolean(//Book/creator)%)` Parameters: xpathex - XPath Boolean expression
`<text>.XPATH(xpathex)`	Operate on an XML file and return a value of data type "double." For example, the following expression converts the string "36" (a price valu value of data type "double" if the string is in the first 1000 bytes of the XML `HTTP.REQ.BODY(1000).XPATH(xp%number(/Book/price)%)` Parameters: xpathex - XPath numeric expression

`<text>.XPATH(xpathex)`	Operate on an XML file and return a node-set or a string. Node-sets are conv to corresponding strings by using the standard XPath string conversion routin For example, the following expression selects all the nodes that are enclose “/Book/creator” (a node-set) in the first 1000 bytes of the body: `HTTP.REQ.BODY(1000).XPATH(xp%/Book/creator%)` Parameters: xpathex - XPath expression
`<text>.XPATH_HTML(xpathex)`	Operate on an HTML file and return a text value. For example, the following expression operates on an HTML file and returns text enclosed in <title></title> tags if the title HTML element is found in the 1000 bytes: `HTTP.REQ.BODY(1000).XPATH_HTML(xp%/html/head/title%)` Parameters: xpathex - XPath text expression
`<text>.XPATH_HTML_WITH_MARKUP(xpathex)`	Operate on an HTML file and return a string that contains the entire selecte portion of the document, including markup such as including the enclosing e tags. The following expression operates on the HTML file and selects all content w the <title> tag, including markup. `HTTP.REQ.BODY(1000).XPATH_HTML_WITH_MARKUP( xp%/html/head/title%)` The portion of the HTML body that is selected by the expression is marked fo further processing. Parameters: xpathex - XPath expression
`<text>.XPATH_JSON(xpathex)`	Operate on a JSON file and return a Boolean value. For example, consider the following JSON file: { "Book":{ "creator":{ "person":{ "name":'<name>' } }, "title":'<title>' } } The following expression operates on the JSON file and returns a Boolean TR the JSON file contains a node named “creator,” whose parent node is “Book the first 1000 bytes: `HTTP.REQ.BODY(1000).XPATH_JSON(xp%boolean(/Book/creator)%` Parameters: xpathex - XPath Boolean expression

`<text>.XPATH_JSON(xpathex)`	Operate on a JSON file and return a value of data type “double.” For example, consider the following JSON file: { "Book":{ "creator":{ "person":{ "name":'<name>' } }, "title":'<title>', "price":"3 The following expression operates on the JSON file and converts the string “ a value of data type “double” if the string is present in the first 1000 bytes o JSON file. `HTTP.REQ.BODY(1000).XPATH_JSON(xp%number(/Book/price)%)` Parameters: xpathex - XPath numeric expression
`<text>.XPATH_JSON(xpathex)`	Operate on a JSON file and return a node-set or a string. Node-sets are conv to corresponding strings by using the standard XPath string conversion routin For example, consider the following JSON file: { "Book":{ "creator":{ "person":{ "name":'<name>' } }, "title":'<title>' } } The following expression selects all the nodes that are enclosed by “/Book" (node-set) in the first 1000 bytes of the body of the JSON file and returns the corresponding string value, which is "<name><title>": `HTTP.REQ.BODY(1000).XPATH_JSON(xp%/Book%)` Parameters: xpathex - XPath expression
`<text>.XPATH_JSON_WITH_MARKUP(xpathex)`	Operate on an XML file and return a string that contains the entire portion o document for the result node, including markup such as including the enclos element tags. For example, consider the following JSON file: {"Book":{ "creator":{ "person":{ "name":'<name>' } }, "title":'<title>' } } The following expression operates on the JSON file and selects all the nodes are enclosed by “/Book/creator" in the first 1000 bytes of the body, which is “creator:{ person:{ name:'<name>' } }.” `HTTP.REQ.BODY(1000).XPATH_JSON_WITH_MARKUP(xp%/Book/creat` The portion of the JSON body that is selected by the expression is marked fo further processing. Parameters: xpathex - XPath expression

`<text>.XPATH_WITH_MARKUP(xpathex)`	Operate on an XML file and return a string that contains the entire portion o document for the result node, including markup such as including the enclos element tags. For example, the following expression operates on an XML file and selects al nodes enclosed by “/Book/creator" in the first 1000 bytes of the body. `HTTP.REQ.BODY(1000).XPATH_WITH_MARKUP(xp%/Book/creator%)` The portion of the JSON body that is selected by the expression is marked fo further processing. Parameters: xpathex - XPath expression

Encrypting and Decrypting XML Payloads

You can use the XML_ENCRYPT() and XML_DECRYPT() functions in default syntax expressions to encrypt and decrypt, respectively, XML data. These functions conform to the W3C XML Encryption standard defined at "http://www.w3.org/TR/2001/PR-xmldsig-core-20010820/." XML_ENCRYPT() and XML_DECRYPT() support a subset of the XML Encryption specification. In the subset, data encryption uses a bulk cipher method (RC4, DES3, AES128, AES192, or AES256), and an RSA public key is used to encrypt the bulk cipher key.

Note: If you want to encrypt and decrypt text in a payload, you must use the ENCRYPT and DECRYPT functions. For more information about these functions, see "Encrypting and Decrypting Text."

The XML_ENCRYPT() and XML_DECRYPT() functions are not dependent on the encryption/decryption service that is used by the ENCRYPT and DECRYPT commands for text. The cipher method is specified explicitly as an argument to the XML_ENCRYPT() function. The XML_DECRYPT() function obtains the information about the specified cipher method from the <xenc:EncryptedData> element. Following are synopses of the XML encryption and decryption functions:

- **XML_ENCRYPT(<certKeyName>, <method> [, <flags>])**. Returns an <xenc:EncryptedData> element that contains the encrypted input text and the encryption key, which is itself encrypted by using RSA.
- **XML_DECRYPT(<certKeyName>)**. Returns the decrypted text from the input <xenc:EncryptedData> element, which includes the cipher method and the RSA-encrypted key.

Note: The <xenc:EncryptedData> element is defined in the W3C XML Encryption specification.

Following are descriptions of the arguments:

certKeyName

Selects an X.509 certificate with an RSA public key for XML_ENCRYPT() or an RSA private key for XML_DECRYPT(). The certificate key must have been previously created by an add ssl certKey command.

method

Specifies which cipher method to use for encrypting the XML data. Possible values: RC4, DES3, AES128, AES192, AES256.

flags

A bitmask specifying the following optional key information (<ds:KeyInfo>) to be included in the <xenc:EncryptedData> element that is generated by XML_ENCRYPT():

- **1** - Include a `KeyName` element with the `certKeyName`. The element is `<ds:KeyName>`.
- **2** - Include a `KeyValue` element with the RSA public key from the certificate. The element is `<ds:KeyValue>`.
- **4** - Include an `X509IssuerSerial` element with the certificate serial number and issuer DN. The element is `<ds:X509IssuserSerial>`.
- **8** - Include an `X509SubjectName` element with the certificate subject DN. The element is `<ds:X509SubjectName>`.
- **16** - Include an `X509Certificate` element with the entire certificate. The element is `<ds:X509Certificate>`.

Using the *XML_ENCRYPT( )* and *XML_DECRYPT( )* Functions in Expressions

The XML encryption feature uses SSL certificate-key pairs to provide X.509 certificates (with RSA public keys) for key encryption and RSA private keys for key decryption. Therefore, before you use the `XML_ENCRYPT( )` function in an expression, you must create an SSL certificate-key pair. The following command creates an SSL certificate-key pair, `my-certkey`, with the X.509 certificate, `my-cert.pem`, and the private key file, `my-key.pem`.

```
add ssl certKey my-certkey -cert my-cert.pem -key my-key.pem
-passcrypt kxPeMRYnitY=
```

The following CLI commands create rewrite actions and policies for encrypting and decrypting XML content.

```
add rewrite action my-xml-encrypt-action replace
"HTTP.RES.BODY(10000).XPATH_WITH_MARKUP(xp%/%)" "HTTP.RES.BODY(10000)
.XPATH_WITH_MARKUP(xp%/%).XML_ENCRYPT(\"my-certkey\", AES256, 31)"
-bypassSafetyCheck YES

add rewrite action my-xml-decrypt-action replace
"HTTP.REQ.BODY(10000).XPATH_WITH_MARKUP(xp%//xenc:EncryptedData%)" "H
TTP.REQ.BODY(10000).XPATH_WITH_MARKUP(xp%//xenc:EncryptedData%).XML_D
ECRYPT(\"my-certkey\")" -bypassSafetyCheck YES

add rewrite policy my-xml-encrypt-policy
"HTTP.REQ.URL.CONTAINS(\"xml-encrypt\")" my-xml-encrypt-action

add rewrite policy my-xml-decrypt-policy
"HTTP.REQ.BODY(10000).XPATH(xp%boolean(//xenc:EncryptedData)%)"
my-xml-decrypt-action

bind rewrite global my-xml-encrypt-policy 30

bind rewrite global my-xml-decrypt-policy 30
```

In the above example, the rewrite action `my-xml-encrypt-action` encrypts the entire XML document (`XPATH_WITH_MARKUP(xp%/%)`) in the request by using the AES-256 bulk encryption method and the RSA public key from `my-certkey` to encrypt the bulk encryption key. The action replaces the document with an `<xenc:EncryptedData>` element containing the encrypted data and an encrypted key. The flags represented by 31 include all of the optional `<ds:KeyInfo>` elements.

The action `my-xml-decrypt-action` decrypts the first `<xenc:EncryptedData>` element in the response (`XPATH_WITH_MARKUP(xp%//xenc:EncryptedData%)`). This requires the prior addition of the `xenc` XML namespace by use of the following CLI command:

```
add ns xmlnamespace xenc http://www.w3.org/2001/04/xmlenc#
```

The `my-xml-decrypt-action` action uses the RSA private key in `my-certkey` to decrypt the encrypted key and then uses the bulk encryption method specified in the element to decrypt the encrypted contents. Finally, the action replaces the encrypted data element with the decrypted content.

The rewrite policy `my-xml-encrypt-policy` applies `my-xml-encrypt-action` to requests for URLs containing `xml-encrypt`. The action encrypts the entire response from a service configured on the NetScaler appliance.

The rewrite policy `my-xml-decrypt-policy` applies `my-xml-decrypt-action` to requests that contain an `<xenc:EncryptedData>` element (`(XPATH(xp%//xenc:EncryptedData%)` returns a non-empty string). The action decrypts the encrypted data in requests that are bound for a service configured on the NetScaler appliance.

Default Syntax Expressions: Parsing SSL Certificates

You can use default syntax expressions to evaluate X.509 Secure Sockets Layer (SSL) client certificates. A client certificate is an electronic document that can be used to authenticate a user's identity. A client certificate contains (at a minimum) version information, a serial number, a signature algorithm ID, an issuer name, a validity period, a subject (user) name, a public key, and signatures.

You can examine both SSL connections and data in client certificates. For example, you may want to send SSL requests that use low-strength ciphers to a particular load balancing virtual server farm. The following command is an example of a Content Switching policy that parses the cipher strength in a request and matches cipher strengths that are less than or equal to 40:

```
add cs policy p1 -rule "client.ssl.cipher_bits.le(40)"
```

As another example, you can configure a policy that determines whether a request contains a client certificate:

```
add cs policy p2 -rule "client.ssl.client_cert EXISTS"
```

Or, you might want to configure a policy that examines particular information in a client certificate. For example, the following policy verifies that the certificate has one or more days before expiration:

```
add cs policy p2 -rule "client.ssl.client_cert exists &&
client.ssl.client_cert.days_to_expire.ge(1)"
```

Note: For information on parsing dates and times in a certificate, see "Format of Dates and Times in an Expression" and "Expressions for SSL Certificate Dates."

Prefixes for Text-Based SSL and Certificate Data

The following table describes expression prefixes that identify text-based items in SSL transactions and client certificates.

Table 1. Prefixes That Return Text or Boolean Values for SSL and Client Certificate Data

Prefix	Description
`CLIENT.SSL.CLIENT_CERT`	Returns the SSL client certificate in the current SSL transaction.
`CLIENT.SSL.CLIENT_CERT.TO_PEM`	Returns the SSL client certificate in binary format.
`CLIENT.SSL.CIPHER_EXPORTABLE`	Returns a Boolean TRUE if the SSL cryptographic SSL cryptographic cipher is exportable.
`CLIENT.SSL.CIPHER_NAME`	Returns the name of the SSL Cipher if invoked from an SSL connection, and a NULL string if invoked from a non-SSL connection.
`CLIENT.SSL.IS_SSL`	Returns a Boolean TRUE if the current connection is SSL-based.

Prefixes for Numeric Data in SSL Certificates

The following table describes prefixes that evaluate numeric data other than dates in SSL certificates. These prefixes can be used with the operations that are described in "Basic Operations on Expression Prefixes" and "Compound Operations for Numbers."

Table 1. Prefixes That Evaluate Numeric Data Other Than Dates in SSL Certificates

Prefix	Description
`CLIENT.SSL.CLIENT_CERT.DAYS_TO_EXPIRE`	Returns the number of days that the certificate is valid, or returns -1 for expired certificates.
`CLIENT.SSL.CLIENT_CERT.PK_SIZE`	Returns the size of the public key used in the certificate.
`CLIENT.SSL.CLIENT_CERT.VERSION`	Returns the version number of the certificate. If the connection is not SSL-based, returns zero (0).
`CLIENT.SSL.CIPHER_BITS`	Returns the number of bits in the cryptograhic key. Returns 0 if the connection is not SSL-based.
`CLIENT.SSL.VERSION`	Returns a number that represents the SSL protocol version, as follows: · 0. The transaction is not SSL-based. · 0x002. The transaction is SSLv2. · 0x300. The transaction is SSLv3. · 0x301. The transaction is TLSv1.

Note: For expressions related to expiration dates in a certificate, see "Expressions for SSL Certificate Dates."

Expressions for SSL Certificates

You can parse SSL certificates by configuring expressions that use the following prefix:

```
CLIENT.SSL.CLIENT_CERT
```

This section discusses the expressions that you can configure for certificates, with the exception of expressions that examine certificate expiration. Time-based operations are described in "Default Syntax Expressions: Working with Dates, Times, and Numbers."

The following table describes operations that you can specify for the `CLIENT.SSL.CLIENT_CERT prefix`.

Table 1. Operations That Can Be Specified with the CLIENT.SSL.CLIENT_CERT Prefix

SSL Certificate Operation	Description
`<certificate>.EXISTS`	Returns a Boolean TRUE if the client has an SSL certificate.
`<certificate>.ISSUER`	Returns the Distinguished Name (DN) of the Issuer in the certificate as a name-value list. An equals sign (“=”) is the delimiter for the name and the value, and the slash (“/”) is the delimiter that separates the name-value pairs. Following is an example of the returned DN: `/C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@mycompany.com`

<certificate>.ISSUER. IGNORE_EMPTY_ELEMENTS	Returns the Issuer and ignores the empty elements in a name-value list. For example, consider the following: Cert-Issuer: /c=in/st=kar//l=bangelore //o=mycompany/ou=sales/ /emailAddress=myuserid@mycompany.com The following Rewrite action returns a count of 6 based on the preceding Issuer definition: sh rewrite action insert_ssl_header Name: insert_ssl Operation: insert_http_header Target:Cert-Issuer Value:CLIENT.SSL.CLIENT_CERT.ISSUER.COUNT However, if you change the value to the following, the returned count is 9: CLIENT.SSL.CLIENT_CERT.ISSUER.IGNORE_EMPTY_ELEMENTS.COUNT
<certificate>.AUTH_KEYID	Returns a string that contains the Authority Key Identifier extension of the X.509 V3 certificate.
<certificate>.AUTH_KEYID.CERT_SERIALNUMBER	Returns the SerialNumber field of the Authority Key Identifier as a blob.
<certificate>.AUTH_KEYID.EXISTS	Returns a Boolean TRUE if the certificate contains an Authority Key Identifier extension.
<certificate>.AUTH_KEYID.ISSUER_NAME	Returns the Issuer Distinguished Name in the certificate as a name-value list. An equals sign (“=”) is the delimiter for the name and the value, and the slash (“/”) is the delimiter that separates the name-value pairs. Following is an example: /C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@mycompany.com
<certificate>.AUTH_KEYID.ISSUER_NAME.IGNORE_EMPTY_ELEMENTS	Returns the Issuer Distinguished Name in the certificate as a name-value list and ignores the empty elements in the list. For example, the following name-value list has an empty element following “a=10”: a=10;;b=11; ;c=89 The element following b=11 is not considered an empty element.

`<certificate>.AUTH_KEYID.KEYID`	Returns the keyIdentifier field of the Authority Key Identifier as a blob.
`<certificate>.CERT_POLICY`	Returns a string that contains the client certificate policy. Note that this represents a sequence of certificate policies.
`<certificate>.KEY_USAGE(string)`	Returns a Boolean value to indicate whether the specified key usage extension bit value in the X.509 certificate is set. The string argument specifies which bit is checked. Following are valid arguments: · `DIGITAL_SIGNATURE.` Returns TRUE if the digital signature bit is set; otherwise, it returns FALSE. · `NONREPUDIATION.` Returns TRUE if the nonrepudiation bit is set; otherwise, it returns FALSE. · `KEYENCIPHERMENT.` Returns TRUE if the key encipherment bit is set; otherwise, it returns FALSE. · `DATAENCIPHERMENT.` Returns TRUE if the data encipherment bit is set; otherwise, it returns FALSE. · `KEYAGREEMENT.` Returns TRUE if the key agreement bit is set; otherwise, it returns FALSE. · `KEYCERTSIGN.` Returns TRUE if the key cert sign bit is set; otherwise, it returns FALSE. · `CRLSIGN.` Returns TRUE if the CRL bit is set; otherwise, it returns FALSE. · `ENCIPHERONLY.` Returns TRUE if the encipher only bit is set; otherwise, it returns FALSE. · `DECIPHERONLY.` Returns TRUE if the decipher only bit is set; otherwise, it returns FALSE.
`<certificate>.PK_ALGORITHM`	Returns the name of the public key algorithm used by the certificate.
`<certificate>.PK_SIZE`	Returns the size of the public key used in the certificate.
`<certificate>.SERIALNUMBER`	Returns the serial number of the client certificate. If this is a non-SSL transaction or there is an error in the certificate, this operation returns an empty string.
`<certificate>.SIGNATURE_ALGORITHM`	Returns the name of the cryptographic algorithm used by the CA to sign this certificate.

<certificate>.SUBJECT	Returns the Distinguished Name of the Subject as a name-value. An equals sign (“=”) separates names and values and a slash (“/”) delimits name-value pairs. Following is an example: /C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@mycompany.com
<certificate>.SUBJECT.IGNORE_EMPTY_ELEMENTS	Returns the Subject as a name-value list, but ignores the empty elements in the list. For example, consider the following: Cert-Issuer: /c=in/st=kar//l=bangelore //o=mycompany/ou=sales/ /emailAddress=myuserid@mycompany.com The following Rewrite action returns a count of 6 based on the preceding Issuer definition: sh rewrite action insert_ssl_header Name: insert_ssl Operation: insert_http_header Target:Cert-Issuer Value:CLIENT.SSL.CLIENT_CERT.ISSUER.COUNT However, if you change the value to the following, the returned count is 9: CLIENT.SSL.CLIENT_CERT.ISSUER.IGNORE_EMPTY_ELEMENTS.COUNT
<certificate>.SUBJECT_KEYID	Returns the Subject KeyID of the client certificate. If there is no Subject KeyID, this operation returns a zero-length text object.

Default Syntax Expressions: IP and MAC Addresses, Throughput, VLAN IDs

You can use default syntax expression prefixes that return IPv4 and IPv6 addresses, MAC addresses, IP subnets, useful client and server data such as the throughput rates at the interface ports (Rx, Tx, and RxTx), and the IDs of the VLANs through which packets are received. You can then use various operators to evaluate the data that is returned by these expression prefixes.

Expressions for IP Addresses and IP Subnets

You can use default syntax expressions to evaluate addresses and subnets that are in Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) format. Expression prefixes for IPv6 addresses and subnets include IPv6 in the prefix. Expression prefixes for IPv4 addresses and subnets include IP in the prefix. Following is an example of an expression that identifies whether a request has originated from a particular IPv4 subnet.

client.ip.src.in_subnet(147.1.0.0/16)

Following are two examples of Rewrite policies that examine the subnet from which the packet is received and perform a rewrite action on the Host header. With these two policies configured, the rewrite action that is performed depends on the subnet in the request. These two policies evaluate IP addresses that are in the IPv4 address format.

```
add rewrite action URL1-rewrite-action replace "http.req.header(\"Host\")" "\"www.mycompany1.com\""
add rewrite policy URL1-rewrite-policy "http.req.header(\"Host\").contains(\"www.test1.com\") && client.ip.
add rewrite action URL2-rewrite-action replace "http.req.header(\"Host\")" "\"www.mycompany2.com\""
add rewrite policy URL2-rewrite-policy "http.req.header(\"Host\").contains(\"www.test2.com\") && client.ip.
```

Note: The preceding examples are commands that you type at the NetScaler command-line interface (CLI) and, therefore, each quotation mark must be preceded by a backslash (\). For more information, see "Configuring Default Syntax Expressions in a Policy."

Prefixes for IPV4 Addresses and IP Subnets

The following table describes prefixes that return IPv4 addresses and subnets, and segments of IPv4 addresses. You can use numeric operators and operators that are specific to IPv4 addresses with these prefixes. For more information about numeric operations, see "Basic Operations on Expression Prefixes" and "Compound Operations for Numbers."

Table 1. Prefixes That Evaluate IP and MAC Addresses

Prefix	Description
`CLIENT.IP.SRC`	Returns the source IP of the current packet as an IP address or as a number.
`CLIENT.IP.DST`	Returns the destination IP of the current packet as an IP address or as a number.
`SERVER.IP.SRC`	Returns the source IP of the current packet as an IP address or as a number.
`SERVER.IP.DST`	Returns the destination IP of the current packet as an IP address or as a number.

Operations for IPV4 Addresses

The following table describes the operators that can be used with prefixes that return an IPv4 address.

Table 1. Operations on IPV4 Addresses

Prefix	Description
`<ip address>.EQ(<address>)`	Returns a Boolean TRUE if the IP address value is same as the <address> argument. The following example checks whether the client's destination IP address is equal to 10.100.10.100: `client.ip.dst.eq(10.100.10.100)`

`<ip address>.GET1. . .GET4`	Returns a portion of an IP address as a numeric value. For example, if the IP address value is 10.100.200.1, the following is returned:
	
	`client.ip.src.get1 Returns 10`
	
	`client.ip.src.get2 returns 100`
	
	`client.ip.src.get3 returns 200`

`<ip address>.IN_SUBNET(<subnet>)`	Returns a Boolean TRUE if the <subnet> argument matches the subnet of the address value. For example, the following determines whether the client's destination IP address subnet is 10.100.10.100/18: `client.ip.dst.eq(10.100.10.100/18)`
`<ip address>.SUBNET(<n>)`	Returns the IP address after applying the subnet mask specified as the argument. The subnet mask can take values between 0 and 32. For example: `CLIENT.IP.SRC.SUBNET(24) returns 192.168.1.0 if the IP address represented by the prefix is 192.168.1.[0-255].`
`<ip address>.IS_IPV6`	Returns a Boolean TRUE if this is an Internet Protocol version 6 (IPv6) host for the client or server. Following is an example: `client.ip.src.is_ipv6`
`<ip address>.MATCHES(<hostname>)`	Returns a Boolean TRUE if the IP address for the host specified in <hostname> matches the current IP address. The <hostname> cannot exceed 255 charac

`<ip address>.MATCHES_LOCATION(<location>)`	Returns a Boolean TRUE if the location of the IP address matches the <locat argument. The Location string can take the following form: *qual1.qual2.qual3.qual4.qual5.qual6*, for example: NorthAmeria.CA.* Following is an example: `client.ip.src.matches_location(\"Europe.GB.17.London.*.*\`

About IPv6 Expressions

The IPv6 address format allows more flexibility than the older IPv4 format. IPv6 addresses are in the hexadecimal format (RFC 2373). In the following examples, Example 1 is an IPv6 address, Example 2 is a URL that includes the IPv6 address, and Example 3 includes the IPv6 address and a port number.

Example 1:

9901:0ab1:22a2:88a3:3333:4a4b:5555:6666

Example 2:

http://[9901:0ab1:22a2:88a3:3333:4a4b:5555:6666]/

Example 3:

https://[9901:0ab1:22a2:88a3:3333:4a4b:5555:6666]:8080/

In Example 3, the brackets separate the IP address from the port number (8080).

Note that you can only use the '+' operator to combine IPv6 expressions with other expressions. The output is a concatenation of the string values that are returned from the individual expressions. You cannot use any other arithmetic operator with an IPv6 expression. The following syntax is an example:

client.ipv6.src + server.ip.dst

For example, if the client source IPv6 address is ABCD:1234::ABCD, and the server destination IPv4 address is 10.100.10.100, the preceding expression returns "ABCD:1234::ABCD10.100.10.100".

Note that when the NetScaler appliance receives an IPv6 packet, it assigns a temporary IPv4 address from an unused IPv4 address range and changes the source address of the packet to this temporary address. At response time, the outgoing packet's source address is replaced with the original IPv6 address.

Note: You can combine an IPv6 expression with any other expression except an expression that produces a Boolean result.

Expression Prefixes for IPv6 Addresses

The IPv6 addresses that are returned by the expression prefixes in the following table can be treated as text data. For example, the prefix client.ipv6.dst returns the destination IPv6 address as a string that can be evaluated as text.

The following table describes expression prefixes that return an IPv6 address.

Table 1. IPv6 Expression Prefixes That Return Text

Prefix	Description
`CLIENT.IPV6`	Operates on the IPv6 address in with the current packet.
`CLIENT.IPV6.DST`	Returns the IPv6 address in the destination field of the IP header.

`CLIENT.IPV6.SRC`	Returns the IPv6 address in the source field of the IP header. Following are examples:
	
	`client.ipv6.src.in_subnet(2007::2008/64)`
	
	`client.ipv6.src.get1.le(2008)`

`SERVER.IPV6`	Operates on the IPv6 address in with the current packet.
`SERVER.IPV6.DST`	Returns the IPv6 address in the destination field of the IP header.

`SERVER.IPV6.SRC`	Returns the IPv6 address in the source field of the IP header. Following are examples:
	
	`server.ipv6.src.in_subnet(2007::2008/64)`
	
	`server.ipv6.src.get1.le(2008)`

Operations for IPV6 Prefixes

The following table describes the operators that can be used with prefixes that return an IPv6 address:

Table 1. Operations That Evaluate IPv6 Addresses

IPv6 Operation	Description
`<ipv6>.EQ(<IPv6_address> )`	Returns a Boolean TRUE if the IP address value is same as the <IPv6_address> argument. Following is an example: `client.ipv6.dst.eq(ABCD:1234::ABCD)`
`<ipv6>.GET1. . .GET8`	Returns a segment of an IPv6 address as a number. The following example expressions retrieve segments from the ipv6 address 1000:1001:CD10:0000:0000:89AB:4567:CDEF: · `client.ipv6.dst.get5` extracts 0000, which is the fifth set of bits in the address. · `client.ipv6.dst.get6 extracts 89AB.` · `client.ipv6.dst.get7` extracts 4567. You can perform numeric operations on these segments. Note that you cannot perform numeric operations when you retrieve an entire IPv6 address. This is because expressions that return an entire IPv6 address, such as `CLIENT.IPV6.SRC`, return the address in text format.
`<ipv6>.IN_SUBNET(<subnet>)`	Returns a Boolean TRUE if the IPv6 address value is in the subnet specified by the <subnet> argument. Following is an example: `client.ipv6.dst.eq(1000:1001:CD10:0000:0000:89AB:4567:CDEF/60)`
`<ipv6>.IS_IPV4`	Returns a Boolean TRUE if this is an IPv4 client, and returns a Boolean FALSE if it is not.
`<ipv6>.SUBNET(<n>)`	Returns the IPv6 address after applying the subnet mask specified as the argument. The subnet mask can take values between 0 and 128. For example: `CLIENT.IPV6.SRC.SUBNET(24)`

Expressions for MAC Addresses

A MAC address consists of colon-delimited hexadecimal values in the format ##:##:##:##:##:##, where each “#” represents either a number from 0 through 9 or a letter from A through F. Default syntax expression prefixes and operators are available for evaluating source and destination MAC addresses.

Prefixes for MAC Addresses

The following table describes prefixes that return MAC addresses.

Table 1. Prefixes That Evaluate MAC Addresses

Prefix	Description
`client.ether.dstmac`	Returns the MAC address in the destination field of the Ethernet header.
`client.ether.srcmac`	Returns the MAC address in the source field of the Ethernet header.

Operations for MAC Addresses

The following table describes the operators that can be used with prefixes that return a MAC address.

Table 1. Operations on MAC Addresses

Prefix	Description
`<mac address>.EQ(<address>)`	Returns a Boolean TRUE if the MAC address value is same as the <address> argument.
`<mac address>.GET1. . .GET4`	Returns a numeric value extracted from the segment of the MAC address that is specified in the GET operation. For example, if the MAC address is 12:34:56:78:9a:bc, the following returns 34: `client.ether.dstmac.get2`

Expressions for Numeric Client and Server Data

The following table describes prefixes for working with numeric client and server data, including throughput, port numbers, and VLAN IDs.

Table 1. Prefixes That Evaluate Numeric Client and Server Data

Prefix	Description
`client.interface.rxthroughput`	Returns an integer representing the raw received traffic throughput in kilobytes per second (KBps) for the previous seven seconds.
`client.interface.txthroughput`	Returns an integer representing the raw transmitted traffic throughput in KBps for the previous seven seconds.
`client.interface.rxtxthroughput`	Returns an integer representing the raw received and transmitted traffic throughput in KBps for the previous seven seconds.
`server.interface.rxthroughput`	Returns an integer representing the raw received traffic throughput in KBps for the previous seven seconds.
`server.interface.txthroughput`	Returns an integer representing the raw transmitted traffic throughput in KBps for the previous seven seconds.
`server.interface.rxtxthroughput`	Returns an integer representing the raw received and transmitted traffic throughput in KBps for the previous seven seconds.
`server.vlan.id`	Returns a numeric ID of the VLAN through which the current packet entered the NetScaler.
`client.vlan.id`	Returns a numeric ID for the VLAN through which the current packet entered the NetScaler.

Default Syntax Expressions: Stream Analytics Functions

Stream Analytics expressions begin with the `ANALYTICS.STREAM(<identifier_name>)` prefix. The following list describes the functions that can be used with this prefix.

`COLLECT_STATS`

Collect statistical data from the requests that are evaluated against the policy and create a record for each request.

`REQUESTS`

Return the number of requests that exist for the specified record grouping. The value returned is of type unsigned long.

`BANDWIDTH`

Return the bandwidth statistic for the specified record grouping. The value returned is of type unsigned long.

`RESPTIME`

Return the response time statistic for the specified record grouping. The value returned is of type unsigned long.

`CONNECTIONS`

Return the number of concurrent connections that exist for the specified record grouping. The value returned is of type unsigned long.

`IS_TOP(n)`

Return a Boolean `TRUE` if the statistical value for the specified record grouping is one among the top `n` groups. Otherwise, return a Boolean `FALSE`.

`CHECK_LIMIT`

Return a Boolean `TRUE` if the statistic for the specified record grouping has hit the preconfigured limit. Otherwise, return a Boolean `FALSE`.

Default Syntax Expressions: DataStream

The policy infrastructure on the Citrix NetScaler appliance includes expressions that you can use to evaluate and process database server traffic when the appliance is deployed between a farm of application servers and their associated database servers.

Expressions for the MySQL Protocol

The following expressions evaluate traffic associated with MySQL database servers. You can use the request-based expressions (expressions that begin with `MYSQL.CLIENT` and `MYSQL.REQ`) in policies to make request switching decisions at the content switching virtual server bind point and the response-based expressions (expressions that begin with `MYSQL.RES`) to evaluate server responses to user-configured health monitors.

- **`MYSQL.CLIENT`.** Operates on the client properties of a MySQL connection.
- **`MYSQL.CLIENT.CAPABILITIES`.** Returns the set of flags that the client has set in the capabilities field of the handshake initialization packet during authentication. Examples of the flags that are set are `CLIENT_FOUND_ROWS`, `CLIENT_COMPRESS`, and `CLIENT_SSL`.
- **`MYSQL.CLIENT.CHAR_SET`.** Returns the enumeration constant assigned to the character set that the client uses. The `EQ(<m>)` and `NE(<m>)` operators, which return Boolean values to indicate the result of a comparison, are used with this prefix. Following are the character set enumeration constants:
  - `LATIN2_CZECH_CS`
  - `DEC8_SWEDISH_CI`
  - `CP850_GENERAL_CI`
  - `GREEK_GENERAL_CI`
  - `LATIN1_GERMAN1_CI`
  - `HP8_ENGLISH_CI`
  - `KOI8R_GENERAL_CI`
  - `LATIN1_SWEDISH_CI`
  - `LATIN2_GENERAL_CI`
  - `SWE7_SWEDISH_CI`
  - `ASCII_GENERAL_CI`
  - `CP1251_BULGARIAN_CI`
  - `LATIN1_DANISH_CI`
  - `HEBREW_GENERAL_CI`
  - `LATIN7_ESTONIAN_CS`
  - `LATIN2_HUNGARIAN_CI`

- KOI8U_GENERAL_CI
- CP1251_UKRAINIAN_CI
- CP1250_GENERAL_CI
- LATIN2_CROATIAN_CI
- CP1257_LITHUANIAN_CI
- LATIN5_TURKISH_CI
- LATIN1_GERMAN2_CI
- ARMSCII8_GENERAL_CI
- UTF8_GENERAL_CI
- CP1250_CZECH_CS
- CP866_GENERAL_CI
- KEYBCS2_GENERAL_CI
- MACCE_GENERAL_CI
- MACROMAN_GENERAL_CI
- CP852_GENERAL_CI
- LATIN7_GENERAL_CI
- LATIN7_GENERAL_CS
- MACCE_BIN
- CP1250_CROATIAN_CI
- LATIN1_BIN
- LATIN1_GENERAL_CI
- LATIN1_GENERAL_CS
- CP1251_BIN
- CP1251_GENERAL_CI
- CP1251_GENERAL_CS
- MACROMAN_BIN
- CP1256_GENERAL_CI
- CP1257_BIN

- CP1257_GENERAL_CI
- ARMSCII8_BIN
- ASCII_BIN
- CP1250_BIN
- CP1256_BIN
- CP866_BIN
- DEC8_BIN
- GREEK_BIN
- HEBREW_BIN
- HP8_BIN
- KEYBCS2_BIN
- KOI8R_BIN
- KOI8U_BIN
- LATIN2_BIN
- LATIN5_BIN
- LATIN7_BIN
- CP850_BIN
- CP852_BIN
- SWE7_BIN
- UTF8_BIN
- GEOSTD8_GENERAL_CI
- GEOSTD8_BIN
- LATIN1_SPANISH_CI
- UTF8_UNICODE_CI
- UTF8_ICELANDIC_CI
- UTF8_LATVIAN_CI
- UTF8_ROMANIAN_CI
- UTF8_SLOVENIAN_CI

- UTF8_POLISH_CI
- UTF8_ESTONIAN_CI
- UTF8_SPANISH_CI
- UTF8_SWEDISH_CI
- UTF8_TURKISH_CI
- UTF8_CZECH_CI
- UTF8_DANISH_CI
- UTF8_LITHUANIAN_CI
- UTF8_SLOVAK_CI
- UTF8_SPANISH2_CI
- UTF8_ROMAN_CI
- UTF8_PERSIAN_CI
- UTF8_ESPERANTO_CI
- UTF8_HUNGARIAN_CI
- INVAL_CHARSET

- **MYSQL.CLIENT.DATABASE.** Returns the name of the database specified in the authentication packet that the client sends to the database server. This is the `databasename` attribute.
- `MYSQL.CLIENT.USER.` Returns the user name (in the authentication packet) with which the client is attempting to connect to the database. This is the `user` attribute.
- **MYSQL.REQ.** Operates on a MySQL request.
- **MYSQL.REQ.COMMAND.** Identifies the enumeration constant assigned to the type of command in the request. The `EQ(<m>)` and `NE(<m>)` operators, which return Boolean values to indicate the result of a comparison, are used with this prefix. Following are the enumeration constant values:
  - SLEEP
  - QUIT
  - INIT_DB
  - QUERY
  - FIELD_LIST
  - CREATE_DB

    - DROP_DB
    - REFRESH
    - SHUTDOWN
    - STATISTICS
    - PROCESS_INFO
    - CONNECT
    - PROCESS_KILL
    - DEBUG
    - PING
    - TIME
    - DELAYED_INSERT
    - CHANGE_USER
    - BINLOG_DUMP
    - TABLE_DUMP
    - CONNECT_OUT
    - REGISTER_SLAVE
    - STMT_PREPARE
    - STMT_EXECUTE
    - STMT_SEND_LONG_DATA
    - STMT_CLOSE
    - STMT_RESET
    - SET_OPTION
    - STMT_FETCH
- **MYSQL.REQ.QUERY.** Identifies the query in the MySQL request.
- **MYSQL.REQ.QUERY.COMMAND.** Returns the first keyword in the MySQL query.
- **MYSQL.REQ.QUERY.SIZE.** Returns the size of the request query in integer format. The SIZE method is similar to the CONTENT_LENGTH method that returns the length of an HTTP request or response.
- **MYSQL.REQ.QUERY.TEXT.** Returns a string covering the entire query.

- **MYSQL.REQ.QUERY.TEXT(<n>).** Returns the first `n` bytes of the MySQL query as a string. This is similar to `HTTP.BODY(<n>)`.

  Parameters:

  `n` - Number of bytes to be returned

- **MYSQL.RES.** Operates on a MySQL response.

- **MYSQL.RES.ATLEAST_ROWS_COUNT(<i>).** Checks whether the response has at least `i` number of rows and returns a Boolean `TRUE` or `FALSE` to indicate the result.

  Parameters:

  `i` - Number of rows

- **MYSQL.RES.ERROR.** Identifies the MySQL error object. The error object includes the error number and the error message.

- **MYSQL.RES.ERROR.MESSAGE.** Returns the error message that is retrieved from the server's error response.

- **MYSQL.RES.ERROR.NUM.** Returns the error number that is retrieved from the server's error response.

- **MYSQL.RES.ERROR.SQLSTATE.** Returns the value of the `SQLSTATE` field in the server's error response. The MySQL server translates error number values to `SQLSTATE` values.

- **MYSQL.RES.FIELD(<i>).** Identifies the packet that corresponds to the i^{th} individual field in the server's response. Each field packet describes the properties of the associated column. The packet count (`i`) begins at 0.

  Parameters:

  `i` - Packet number

- **MYSQL.RES.FIELD(<i>).CATALOG.** Returns the `catalog` property of the field packet.

- **MYSQL.RES.FIELD(<i>).CHAR_SET.** Returns the character set of the column. The `EQ(<m>)` and `NE(<m>)` operators, which return Boolean values to indicate the result of a comparison, are used with this prefix.

- **MYSQL.RES.FIELD(<i>).DATATYPE.** Returns an enumeration constant that represents the data type of the column. This is the `type` (also called `enum_field_type`) attribute of the column. The `EQ(<m>)` and `NE(<m>)` operators, which return Boolean values to indicate the result of a comparison, are used with this prefix. The possible values for the various data types are:

  - `DECIMAL`
  - `TINY`
  - `SHORT`

- LONG
- FLOAT
- DOUBLE
- NULL
- TIMESTAMP
- LONGLONG
- INT24
- DATE
- TIME
- DATETIME
- YEAR
- NEWDATE
- VARCHAR (new in MySQL 5.0)
- BIT (new in MySQL 5.0)
- NEWDECIMAL (new in MySQL 5.0)
- ENUM
- SET
- TINY_BLOB
- MEDIUM_BLOB
- LONG_BLOB
- BLOB
- VAR_STRING
- STRING
- GEOMETRY

- **MYSQL.RES.FIELD(<i>).DB.** Returns the database identifier (db) attribute of the field packet.
- **MYSQL.RES.FIELD(<i>).DECIMALS.** Returns the number of positions after the decimal point if the type is DECIMAL or NUMERIC. This is the decimals attribute of the field packet.

- **MYSQL.RES.FIELD(<i>).FLAGS.** Returns the `flags` property of the field packet. Following are the possible hexadecimal flag values:
  - `0001`: `NOT_NULL_FLAG`
  - `0002`: `PRI_KEY_FLAG`
  - `0004`: `UNIQUE_KEY_FLAG`
  - `0008`: `MULTIPLE_KEY_FLAG`
  - `0010`: `BLOB_FLAG`
  - `0020`: `UNSIGNED_FLAG`
  - `0040`: `ZEROFILL_FLAG`
  - `0080`: `BINARY_FLAG`
  - `0100`: `ENUM_FLAG`
  - `0200`: `AUTO_INCREMENT_FLAG`
  - `0400`: `TIMESTAMP_FLAG`
  - `0800`: `SET_FLAG`
- **MYSQL.RES.FIELD(<i>).LENGTH.** Returns the length of the column. This is the value of the `length` attribute of the field packet. The value that is returned might be larger than the actual value. For example, an instance of a `VARCHAR(2)` column might return a value of `2` even when it contains only one character.
- **MYSQL.RES.FIELD(<i>).NAME.** Returns the column identifier (the name after the `AS` clause, if any). This is the `name` attribute of the field packet.
- **MYSQL.RES.FIELD(<i>).ORIGINAL_NAME.** Returns the original column identifier (before the `AS` clause, if any). This is the `org_name` attribute of the field packet.
- **MYSQL.RES.FIELD(<i>).ORIGINAL_TABLE.** Returns the original table identifier of the column (before the `AS` clause, if any). This is the `org_table` attribute of the field packet.
- **MYSQL.RES.FIELD(<i>).TABLE.** Returns the table identifier of the column (after the `AS` clause, if any). This is the `table` attribute of the field packet.
- **MYSQL.RES.FIELDS_COUNT.** Returns the number of field packets in the response (the `field_count` attribute of the `OK` packet).
- **MYSQL.RES.OK.** Identifies the `OK` packet sent by the database server.
- **MYSQL.RES.OK.AFFECTED_ROWS.** Returns the number of rows affected by an `INSERT`, `UPDATE`, or `DELETE` query. This is the value of the `affected_rows` attribute of the `OK` packet.
- **MYSQL.RES.OK.INSERT_ID.** Identifies the `unique_id` attribute of the `OK` packet. If an auto-increment identity is not generated by the current MySQL statement or query, the value of `unique_id`, and hence the value returned by the expression, is `0`.

- **MYSQL.RES.OK.MESSAGE.** Returns the `message` property of the `OK` packet.
- **MYSQL.RES.OK.STATUS.** Identifies the bit string in the `server_status` attribute of the `OK` packet. Clients can use the server status to check whether the current command is a part of a running transaction. The bits in the `server_status` bit string correspond to the following fields (in the given order):
  - `IN TRANSACTION`
  - `AUTO_COMMIT`
  - `MORE RESULTS`
  - `MULTI QUERY`
  - `BAD INDEX USED`
  - `NO INDEX USED`
  - `CURSOR EXISTS`
  - `LAST ROW SEEN`
  - `DATABASE DROPPED`
  - `NO BACKSLASH ESCAPES`
- **MYSQL.RES.OK.WARNING_COUNT.** Returns the `warning_count` attribute of the `OK` packet.
- **MYSQL.RES.ROW(<i>).** Identifies the packet that corresponds to the i^{th} individual row in the database server's response.

  Parameters:

  `i` - Row number
- **MYSQL.RES.ROW(<i>).DOUBLE_ELEM(<j>).** Checks whether the j^{th} column of the i^{th} row of the table is `NULL`. Following C conventions, both indexes `i` and `j` start from 0. Therefore, row `i` and column `j` are actually the $(i+1)^{th}$ row and the $(j+1)^{th}$ column, respectively.

  Parameters:

  `i` - Row number

  `j` - Column number
- **MYSQL.RES.ROW(<i>).IS_NULL_ELEM(j).** Checks whether the j^{th} column of the i^{th} row of the table is `NULL`. Following C conventions, both indexes `i` and `j` start from 0. Therefore, row `i` and column `j` are actually the $(i+1)^{th}$ row and the $(j+1)^{th}$ column, respectively.

  Parameters:

  `i` - Row number

`j` - Column number

- **`MYSQL.RES.ROW(<i>).NUM_ELEM(<j>).`** Returns an integer value from the j^{th} column of the i^{th} row of the table. Following C conventions, both indexes `i` and `j` start from 0. Therefore, row `i` and column `j` are actually the $(i+1)^{th}$ row and the $(j+1)^{th}$ column, respectively.

  Parameters:

  `i` - Row number

  `j` - Column number

- **`MYSQL.RES.ROW(<i>).TEXT_ELEM(j).`** Returns a string from the j^{th} column of the i^{th} row of the table. Following C conventions, both indexes `i` and `j` start from 0. Therefore, row `i` and column `j` are actually the $(i+1)^{th}$ row and the $(j+1)^{th}$ column, respectively.

  Parameters:

  `i` - Row number

  `j` - Column number

- **`MYSQL.RES.TYPE.`** Returns an enumeration constant for the response type. Its values can be `ERROR`, `OK`, and `RESULT_SET`. The `EQ(<m>)` and `NE(<m>)` operators, which return Boolean values to indicate the result of a comparison, are used with this prefix.

Expressions for Evaluating Microsoft SQL Server Connections

The following expressions evaluate traffic associated with Microsoft SQL Server database servers. You can use the request-based expressions (expressions that begin with MSSQL.CLIENT and MSSQL.REQ) in policies to make request switching decisions at the content switching virtual server bind point and the response-based expressions (expressions that begin with MSSQL.RES) to evaluate server responses to user-configured health monitors.

Table 1. Expressions for Evaluating Microsoft SQL Server Connections

Expression	Description
MSSQL.CLIENT.CAPABILITIES	Returns the OptionFlags1, OptionFlags2, OptionFlags3, and TypeFlags fields of the LOGIN7 authentication packet, in that order, as a 4-byte integer. Each field is 1 byte long and specifies a set of client capabilities.
MSSQL.CLIENT.DATABASE	Returns the name of the client database. The value returned is of type text.
MSSQL.CLIENT.USER	Returns the user name with which the client authenticated. The value returned is of type text.
MSSQL.REQ.COMMAND	Returns an enumeration constant that identifies the type of command in the request sent to a Microsoft SQL Server database server. The value returned is of type text. Examples of the values of the enumeration constant are QUERY, RESPONSE, RPC, and ATTENTION. The EQ(<m>) and NE(<m>) operators, which return Boolean values to indicate the result of a comparison, are used with this expression.
MSSQL.REQ.QUERY.COMMAND	Returns the first keyword in the SQL query. The value returned is of type text.
MSSQL.REQ.QUERY.SIZE	Returns the size of the SQL query in the request. The value returned is a number.
MSSQL.REQ.QUERY.TEXT	Returns the entire SQL query as a string. The value returned is of type text.
MSSQL.REQ.QUERY.TEXT(<n>)	Returns the first n bytes of the SQL query. The value returned is of type text. **Parameters:** n - Number of bytes
MSSQL.REQ.RPC.NAME	Returns the name of the procedure that is being called in a remote procedure call (RPC) request. The name is returned as a string.

MSSQL.REQ.RPC.IS_PROCID	Returns a Boolean value that indicates whether the remote procedure call (RPC) request contains a procedure ID or an RPC name. A return value of TRUE indicates that the request contains a procedure ID and a return value of FALSE indicates that the request contains an RPC name.
MSSQL.REQ.RPC.PROCID	Returns the procedure ID of the remote procedure call (RPC) request as an integer.
MSSQL.REQ.RPC.BODY **Note:** Not available for releases before 10.1.	Returns the body of the SQL request as a string in the form of parameters represented as "a=b" clauses separated by commas, where "a" is the RPC parameter name and "b" is its value.
MSSQL.REQ.RPC.BODY(n) **Note:** Not available for releases before 10.1.	Returns part of the body of the SQL request as a string in the form of parameters represented as "a=b" clauses separated by commas, where "a" is the RPC parameter name and "b" is its value. Parameters are returned from only the first "n" bytes of the request, skipping the SQL header. Only complete name-value pairs are returned.
MSSQL.RES.ATLEAST_ROWS_COUNT(i)	Checks whether the response has at least i number of rows. The value returned is a Boolean TRUE or FALSE value. **Parameters:** i - Number of rows
MSSQL.RES.DONE.ROWCOUNT	Returns a count of the number of rows affected by an INSERT, UPDATE, or DELETE query. The value returned is of type unsigned long.
MSSQL.RES.DONE.STATUS	Returns the status field from the DONE token sent by a Microsoft SQL Server database server. The value returned is a number.
MSSQL.RES.ERROR.MESSAGE	Returns the error message from the ERROR token sent by a Microsoft SQL Server database server. This is the value of the MsgText field in the ERROR token. The value returned is of type text.
MSSQL.RES.ERROR.NUM	Returns the error number from the ERROR token sent by a Microsoft SQL Server database server. This is the value of the Number field in the ERROR token. The value returned is a number.
MSSQL.RES.ERROR.STATE	Returns the error state from the ERROR token sent by a Microsoft SQL Server database server. This is the value of the State field in the ERROR token. The value returned is a number.

MSSQL.RES.FIELD(<i>).DATATYPE	Returns the data type of the i^{th} field in the server response. The EQ(<m>) and NE(<m>) functions, which return Boolean values to indicate the result of a comparison, are used with this prefix. For example, the following expression returns a Boolean TRUE if the DATATYPE function returns a value of datetime for the third field in the response: MSSQL.RES.FIELD(<2>).DATATYPE.EQ(datetime) **Parameters:** i - Row number
MSSQL.RES.FIELD(<i>).LENGTH	Returns the maximum possible length of the i^{th} field in the server response. The value returned is a number. **Parameters:** i - Row number
MSSQL.RES.FIELD(<i>).NAME	Returns the name of the i^{th} field in the server response. The value returned is of type text. **Parameters:** i - Row number
MSSQL.RES.ROW(<i>).DOUBLE_ELEM(<j>)	Returns a value of type double from the j^{th} column of the i^{th} row of the table. If the value is not a double value, an UNDEF condition is raised. Following C conventions, both indexes i and j start from 0 (zero). Therefore, row i and column j are actually the $(i + 1)^{th}$ row and the $(j + 1)^{th}$ column, respectively. **Parameters:** i - Row number j - Column number
MSSQL.RES.ROW(<i>).NUM_ELEM(j)	Returns an integer value from the j^{th} column of i^{th} row of the table. If the value is not an integer value, an UNDEF condition is raised. Following C conventions, both indexes i and j start from 0 (zero). Therefore, row i and column j are actually the $(i + 1)^{th}$ row and the $(j + 1)^{th}$ column, respectively. **Parameters:** i - Row number j - Column number

MSSQL.RES.ROW(<i>).IS_NULL_ELEM(j)	Checks whether the j^{th} column of the i^{th} row of the table is NULL and returns a Boolean TRUE or FALSE to indicate the result. Following C conventions, both indexes i and j start from 0 (zero). Therefore, row i and column j are actually the $(i + 1)^{th}$ row and the $(j + 1)^{th}$ column, respectively. **Parameters:** i - Row number j - Column number
MSSQL.RES.ROW(<i>).TEXT_ELEM(j)	Returns a text string from the j^{th} column of i^{th} row of the table. Following C conventions, both indexes i and j start from 0 (zero). Therefore, row i and column j are actually the $(i + 1)^{th}$ row and the $(j + 1)^{th}$ column, respectively. **Parameters:** i - Row number j - Column number
MSSQL.RES.TYPE	Returns an enumeration constant that identifies the response type. Following are the possible return values: · ERROR · OK · RESULT_SET The EQ(<m>) and NE(<m>) operators, which return Boolean values to indicate the result of a comparison, are used with this expression.

Typecasting Data

You can extract data of one type (for example, text or an integer) from requests and responses and transform it to data of another type. For example, you can extract a string and transform the string to time format. You can also extract a string from an HTTP request body and treat it like an HTTP header or extract a value from one type of request header and insert it in a response header of a different type.

After typecasting the data, you can apply any operation that is appropriate for the new data type. For example, if you typecast text to an HTTP header, you can apply any operation that is applicable to HTTP headers to the returned value.

The following table describes various typecasting operations.

Table 1. Typecasting Functions

	Description

TYPECAST_LIST_T(<separator>)	Treats the text in an HTTP request or response body as a list whose elem by the character in the <separator> argument. Index values in the list th with zero (0). Text mode settings have no effect on the separator. For example, even i mode to IGNORECASE, and the separator is the letter “p,” an uppercase a separator. The following example creates a Rewrite action that constructs a list fro body and extracts the fourth item in the list: add rewrite action myreplace_action REPLACE 'http.req.body(100)' 'http.req.body(100).typecast_list_t('?').get(4)' set rewrite policy myreplace_policy -action myreplace_action This policy returns the string “fourth item” from the following request: GET?first item?second item?third item?fourth item? The following example extracts the fourth-from-last item from the list. add rewrite action myreplace_action1 REPLACE 'http.req.body(100)' 'http.req.body(100).typecast_list_t('?').get_reverse(4)' set rewrite policy myreplace_policy1 -action myreplace_action1 This policy returns the string “first item” from the following request: GET?first item?second item?third item?fourth item.

TYPECAST_ NVLIST_T(<separator>, <delimiter>) PECAST_ NVLIST_T(<separator>, <delimiter>,)	Treats the text as a name-value list. The <separator> argument identifie separates the name and the value. The <delimiter> argument identifies separates each name-value pair. The <quote> character is required whe into a name-value list that supports quoted strings. Any delimiters that a quoted string are ignored. The text mode has no effect on the delimiters. For example, if the curre IGNORECASE and you specify “p” as the delimiter, an uppercase “P” is n delimiter. For example, the following policy counts the number of name-value pair result in a header named name-value-count: add rewrite action mycount_action insert_http_header name-value-coun 'http.req.header("Cookie").typecast_nvlist_t('=',';').count' set rewrite policy mycount_policy -action mycount_action This policy can extract a count of arguments in Cookie headers and inser name-value-count header: `Cookie: name=name1; rank=rank1`
TYPECAST_TIME_T	Treats the designated text as a date string. The following formats are su · RFC822: Sun, 06 Nov 1994 08:49:37 GMT · RFC850: Sunday, 06-Nov-94 08:49:37 GMT · ASCII TIME: Sun Nov 6 08:49:37 1994 · HTTP Set-Cookie Expiry date: Sun, 06-Nov-1994 08:49:37 GMT For example, the following policy converts the string to a time value and day. This policy matches all requests that have a day value lesser than o Add rewrite policy mytime_policy "http.req.body(100) .typecast_time_t.day.le(10)" mytime_action bind rewrite global mytime_policy 100

c string>.TYPECAST_IP_ ADDRESS_T	Treats a numeric string as an IP address. For example, the following policy matches HTTP requests that contains C a value of: 12.34.56.78\r\n. set rewrite policy ip_check_policy -rule 'http.req.cookie .value("ip").typecast_ip_address_t.eq(12.34.56.78)' bind rewrite global ip_check_policy 200 -type req_default
c string>.TYPECAST_IPV6_ADDRESS_T	Treats a string as an IPv6 address in the following format: 0000:0000:CD00:0000:0000:00AB:0000:CDEF
TYPECAST_HTTP_ URL_T	Treats the designated text as the URL in the first line of an HTTP reques supported format is [<protocol>://<hostname>]<path>?<query> is set to URLENCODED by default. For example, the following policy replaces a URL-encoded part of a strin named Test. add rewrite action replace_header_string replace "http.req.header(\"Test\").typecast_http_url_t.path .before_str(\"123\").after_str(\"ABC\")" "\"string\"" add rewrite policy rewrite_test_header_policy true replace_header_strin bind rewrite global rewrite_test_header_policy 1 END -type res_override Consider the following header: Test: ABC%12123\r\n This policy would replace the preceding header with the value ABC%str
TYPECAST_HTTP_ HOSTNAME_T	Provides operations for parsing an HTTP host name as it appears in HTTP for a host name is abc.def.com:8080.
TYPECAST_HTTP_ METHOD_T	Converts text to an HTTP method. For example, the following policy matches any HTTP request that contai with a value equal to POST: Add rewrite policy method_policy "http.req.header(\"Host\") .typecast_http_method_t.eq(POST)" act1
TYPECAST_DNS_ DOMAIN_T	Enables the designated text to be parsed like a DNS domain name in the

TYPECAST_HTTP_ HEADER_T("<name>")	Converts the designated text to a multi-line HTTP header that you specif argument. For example, the following expression converts “MyHeader” to “InHeade http.req.header("MyHeader").typcast_http_header_t("InHeader") Typically, text operations that you specify in this type of expression app line of this header, with some exceptions. For example, the CONTAINS o values in all the lines in instances of this header type.
TYPECAST_COOKIE_T	Treats the designated text as an HTTP cookie as it appears in a Set-Cook header. You can apply name-value list operations as well as text operati designated text. For example, you can designate equals (=) as the name- the semicolon (;) as the list element delimiter. If you apply name-value list operations, the list is parsed as if IGNORE_E were in effect. Each cookie begins with a `cookie-name=cookie-value` pair, optiona attribute-value pairs that are separated by a semicolon, as follows: `cookie1=value1;version=n.n;value;domain=value;path=valu` If the same attribute appears more than once in a cookie, the value for t the attribute is returned.
>.TYPECAST_DOUBLE_AT	Transforms the number to a value of data type double.
>.TYPECAST_IP_ADDRESS_AT	Converts the number to an IP address.
>.TYPECAST_TIME_AT	Converts the number to time format.

>.TYPECAST_TIME_AT.BETWEEN(<time1>, <time2>)	Returns a Boolean value (TRUE or FALSE) that indicates whether the time by <number> is between the lower and upper time value arguments <tim The following are prerequisites for this function: · Both the lower and upper time arguments must be fully specified. Fo 1995 Jan is fully specified. But GMT Jan, GMT 1995 20 and GMT Jan / specified. · Both arguments must be either GMT or Local. · The day of the week must not be present in either argument. Howev month can be specified as the first, second, third, or fourth weekday (example Wed_3 is the third Wednesday of the month). · The upper time argument, <time2>, must be bigger than the lower t <time1>. The following examples assume that the current time value is GMT 2005 and that the day is the first Sunday of the month of May in 2005. The res is given after each example. BETWEEN(GMT 2004, GMT 2006): TRUE BETWEEN(GMT 2004 Jan, GMT 2006 Nov): TRUE BETWEEN(GMT 2004 Jan, GMT 2006): TRUE BETWEEN(GMT 2005 May Sun_1, GMT 2005 May Sun_3): TRUE BETWEEN(GMT 2005 May 1, GMT May 2005 1): TRUE BETWEEN(LOCAL 2005 May 1, LOCAL May 2005 1): The result depends on the NetScaler system's timezone. Parameters: <time1> - Lower time value <time2> - Upper time value
>.TYPECAST_TIME_AT.DAY	Extracts the day of the month from the current system time and returns number that corresponds to the day of the month. The returned value ra

>.TYPECAST_TIME_AT.EQ(<t>)	Returns a Boolean value (TRUE or FALSE) that indicates whether the tim by <number> is equal to the time value argument <t>. The following examples assume that the current time value is GMT 2005 and that the day is the 1st Sunday of the month of May in 2005. The resu is given after each example. EQ(GMT 2005): TRUE EQ(GMT 2005 Dec): FALSE EQ(Local 2005 May): TRUE or FALSE, depending on the time zone. EQ(GMT 10h): TRUE EQ(GMT 10h 30s): TRUE EQ(GMT May 10h): TRUE EQ(GMT Sun): TRUE EQ(GMT May Sun_1): TRUE Parameters: <t> - Time
>.TYPECAST_TIME_AT.GE(<t>)	Returns a Boolean value (TRUE or FALSE) that indicates whether the tim by <number> is greater than or equal to the time value argument <t>. The following examples assume that the current time value is GMT 2005 and that the day is the 1st Sunday of the month of May in 2005. The resu is given after each example. GE(GMT 2004): TRUE GE(GMT 2005 Jan): TRUE GE(Local 2005 May): TRUE or FALSE, depending on the time zone. GE(GMT 8h): TRUE GE(GMT 30m): FALSE GE(GMT May 10h): TRUE GE(GMT May 10h 0m): TRUE GE(GMT Sun): TRUE GE(GMT May Sun_1): TRUE Parameters: <t> - Time

>.TYPECAST_TIME_AT.GT(<t>)	Returns a Boolean value (TRUE or FALSE) that indicates whether the tim by <number> is greater than the time value argument <t>. The following examples assume that the current time value is GMT 2005 and that the day is the 1st Sunday of the month of May in 2005. The resu is given after each example. GT(GMT 2004): TRUE GT(GMT 2005 Jan): TRUE GT(Local 2005 May): TRUE or FALSE, depending on the time zone. GT(GMT 8h): TRUE GT(GMT 30m): FALSE GT(GMT May 10h): FALSE GT(GMT May 10h 0m): TRUE GT(GMT Sun): FALSE GT(GMT May Sun_1): FALSE Parameters: <t> - Time
>.TYPECAST_TIME_AT.HOURS	Extracts the hour from the current system time and returns the correspo integer that can range from 0 to 23.
>.TYPECAST_TIME_AT.LE(<t>)	Returns a Boolean value (TRUE or FALSE) that indicates whether the tim by <number> is lesser than or equal to the time value argument <t>. The following examples assume that the current time value is GMT 2005 and that the day is the 1st Sunday of the month of May in 2005. The resu is given after each example. LE(GMT 2006): TRUE LE(GMT 2005 Dec): TRUE LE(Local 2005 May): TRUE or FALSE, depending on the time zone. LE(GMT 8h): FALSE LE(GMT 30m): TRUE LE(GMT May 10h): TRUE LE(GMT Jun 11h): TRUE LE(GMT Wed): TRUE LE(GMT May Sun_1): TRUE Parameters: <t> - Time

>.TYPECAST_TIME_AT.LT(<t>)	Returns a Boolean value (TRUE or FALSE) that indicates whether the time by <number> is lesser than the time value argument <t>. The following examples assume that the current time value is GMT 2005 and that the day is the 1st Sunday of the month of May in 2005. The resu is given after each example. LT(GMT 2006): TRUE LT(GMT 2005 Dec): TRUE LT(Local 2005 May): TRUE or FALSE, depending on the time zone. LT(GMT 8h): FALSE LT(GMT 30m): TRUE LT(GMT May 10h): FALSE LT(GMT Jun 11h): TRUE LT(GMT Wed): TRUE LT(GMT May Sun_1): FALSE Parameters: <t> - Time
>.TYPECAST_TIME_AT.MINUTES	Extracts the minute from the current system time and returns the value can range from 0 to 59.
>.TYPECAST_TIME_AT.MONTH	Extracts the month from the current system time and returns the value a can range from 1 (January) to 12 (December).
>.TYPECAST_TIME_AT.RELATIVE_BOOT	Calculates the number of seconds that have elapsed after the most recen number of seconds to the next scheduled reboot, depending on which is time, and returns an integer. If the closest boot time is in the past, the If the closest boot time is in the future (scheduled reboot time), the inte
>.TYPECAST_TIME_AT.RELATIVE_NOW	Calculates the number of seconds between the current system time and and returns the value as an integer. If the designated time is in the past negative. If it is in the future, the integer is positive.
>.TYPECAST_TIME_AT.SECONDS	Extracts the seconds from the current system time and returns the value can range from 0 to 59.
>.TYPECAST_TIME_AT.WEEKDAY	Returns an integer that corresponds to the day of the week; 0 for Sunday

>.TYPECAST_TIME_AT.WITHIN(<time1>, <time2>)	Returns a Boolean value (TRUE or FALSE) that indicates whether the tim by <number> lies within all the ranges defined by lower and upper time <time1> and <time2>. If an element of time such as the day or the hour is left unspecified in th <time1>, then it is assumed to have the lowest value possible for its rang If an element is left unspecified in the upper argument , <time2>, then i the highest value possible for its range. If the year is specified in one of the arguments, then it must be specifie argument as well. Following are the ranges for different elements of time: · month: 1-12 · day: 1-31 · weekday: 0-6 · hour: 0-23 · minutes: 0-59 · seconds: 0-59. Each element of time in the lower time value argument defines a range the corresponding element in the upper time value argument. For the re each element of time in the time value designated by <number> must lie corresponding range specified by the lower and upper arguments. The following examples assume that the current time value is GMT 2005 30s.and that the day is the second Tuesday of the month. The result of t given after each example. WITHIN(GMT 2004, GMT 2006): TRUE WITHIN(GMT 2004 Jan, GMT 2006 Mar): FALSE (May doesn't fall in the Jan WITHIN(GMT Feb, GMT): TRUE (May falls in the Feb-Dec range.) WITHIN(GMT Sun_1, GMT Sun_3): TRUE (2nd Tuesday lies within 1st Sund and the 3rd Sunday.) WITHIN(GMT 2005 May 1 10h, GMT May 2005 1 17h): TRUE WITHIN(LOCAL 2005 May 1, LOCAL May 2005 1): The result depends on the NetScaler system's timezone. Parameters: <time1> - Lower time value <time2> - Upper time value
>.TYPECAST_TIME_AT.YEAR	Extracts the year from the current system time and returns the value as

>.TYPECAST_NUM_T(<type>)	Casts numeric string data to a signed 32-bit number. The argument <typ the following: · DECIMAL. Treat the string as a decimal number and cast to a signed · HEX. Treat the string as a hexadecimal number and cast to a signed · DECIMAL_PREFIX. Consider the part of the string up to the first occ character that is not a valid decimal character and cast to a signed 3 · HEX_PREFIX. Consider the part of the string up to the first occurrer that is not a valid hexadecimal character and cast to a signed 32-bit For example, the following policy extracts a numeric portion of a query s number, and inserts an HTTP header named Company with the resulting add rewrite action myadd_action insert_http_header Company "http.req.url.query.typecast_num_t(decimal).add(4)" add rewrite policy myadd_policy true myadd_action bind rewrite global myadd_policy 300 END -type RES_DEFAULT For example, this policy would extract "4444" from the following URL st /test/file.html?4444 The action that is associated with the policy would insert the following H header: Company: 4448\r\n
>.TYPECAST_NUM_AT	Casts a number of any data type to a number of data type integer.
>.TYPECAST_DOUBLE_AT	Casts a number of any data type to a number of data type double.
>.TYPECAST_UNSIGNED_LONG_AT	Casts a number of any data type to a number of data type unsigned long
>.TYPECAST_NUM_T(<type>,<default>)	Casts string data to a signed 32-bit number. If the typecasting operation (UNDEF) condition, the function returns the value specified for default. takes the values specified for TYPECAST_NUM_T(<type>).
>.TYPECAST_UNSIGNED_LONG_T(<type>)	Casts string data to data of type unsigned long. The argument can be on · DECIMAL. Treat the string as a decimal number and cast to unsigned · HEX. Treat the string as a hexadecimal number and cast to unsigned · DECIMAL_PREFIX. Consider the part of the string up to the first occ character that is not a valid decimal character and cast to unsigned · HEX_PREFIX. Consider the part of the string up to the first occurrer that is not a valid hexadecimal character and cast to unsigned long.

>.TYPECAST_UNSIGNED_LONG_T(<type>,<default>)	Casts string data to data of type unsigned long. If the typecasting operat undefined (UNDEF) condition, the function returns the value specified fo argument takes the values specified for TYPECAST_UNSIGNED_LONG_T

Regular Expressions

When you want to perform string matching operations that are more complex than the operations that you perform with the CONTAINS(“<string>”) or EQ(“<string>“) operators, you use regular expressions. The policy infrastructure on the Citrix® NetScaler® appliance includes operators to which you can pass regular expressions as arguments for text matching. The names of the operators that work with regular expressions include the string REGEX. The regular expressions that you pass as arguments must conform to the regular expression syntax that is described in "http://www.pcre.org/pcre.txt." You can learn more about regular expressions at "http://www.regular-expressions.info/quickstart.html" and at "http://www.silverstones.com/thebat/Regex.html."

The target text for an operator that works with regular expressions can be either text or the value of an HTTP header. Following is the format of a default syntax expression that uses a regular expression operator to operate on text:

```
<text>.<regex_operator>(re<delimiter><regex_pattern><delimiter>)
```

The string <text> represents the default syntax expression prefix that identifies a text string in a packet (for example, HTTP.REQ.URL). The string <regex_operator> represents the regular expression operator. The regular expression always begins with the string re. A pair of matching delimiters, represented by <delimiter>, enclose the string <regex_pattern>, which represents the regular expression.

The following example expression checks whether the URL in an HTTP packet contains the string *.jpeg (where * is a wildcard) and returns a Boolean TRUE or FALSE to indicate the result. The regular expression is enclosed within a pair of slash marks (/), which act as delimiters.

```
http.req.url.regex_match(re/*.jpeg/)
```

Regular expression operators can be combined to define or refine the scope of a search. For example, `<text>.AFTER_REGEX(re/regex_pattern1/).BEFORE_REGEX(re/regex_pattern2/)` specifies that the target for string matching is the text between the patterns regex_pattern1 and regex_pattern2. You can use a text operator on the scope that is defined by the regular expression operators. For example, you can use the CONTAINS(“<string>”) operator to check whether the defined scope contains the string abc:

```
<text>.AFTER_REGEX(re/regex_pattern1/).BEFORE_REGEX(re/regex_pattern2
/).CONTAINS(“abc”)
```

Note: The process of evaluating a regular expression inherently takes more time than that for an operator such as CONTAINS(“<string>”) or EQ(“<string>”), which work with simple string arguments. You should use regular expressions only if your requirement is beyond the scope of other operators.

Basic Characteristics of Regular Expressions

Following are notable characteristics of regular expressions as defined on the NetScaler appliance:

- A regular expression always begins with the string “re” followed by a pair of delimiting characters (called delimiters) that enclose the regular expression that you want to use.

  For example, `re#<regex_pattern>#` uses the number sign (#) as a delimiter.

- A regular expression cannot exceed 1499 characters.
- Digit matching can be done by using the string \d (a backslash followed by d).
- White space can be represented by using \s (a backslash followed by s).
- A regular expression can contain white spaces.

Following are the differences between the NetScaler syntax and the PCRE syntax:

- The NetScaler does not allow back references in regular expressions.
- You should not use recursive regular expressions.
- The dot meta-character also matches the newline character.
- Unicode is not supported.
- The operation SET_TEXT_MODE(IGNORECASE) overrides the (?i) internal option in the regular expression.

Operations for Regular Expressions

The following table describes the operators that work with regular expressions. The operation performed by a regular expression operator in a given default syntax expression depends on whether the expression prefix identifies text or HTTP headers. Operations that evaluate headers override any text-based operations for all instances of the specified header type. When you use an operator, replace <text> with the default syntax expression prefix that you want to configure for identifying text.

Table 1. Default Syntax Expression Operators That Work with Regular Expressions

sion Operation	Description
RE_REGEX(<regular)	Selects the text that precedes the string that matches the <regular expression> argument. If the regular exp any data in the target, the expression returns a text object of length 0. The following expression selects the string "text" from "text/plain". `http.res.header("content-type").before_regex(re#/#)`
R_REGEX(<regular)	Selects the text that follows the string that matches the <regular expression> argument. If the regular expre text in the target, the expression returns a text object of length 0. The following expression extracts "Example" from "myExample": `http.req.header("etag").after_regex(re/my/)`
X_SELECT(<regular)	Selects a string that matches the <regular expression> argument. If the regular expression does not match t of length 0 is returned. The following example extracts the string "NS-CACHE-9.0: 90" from a Via header: `http.req.header("via").regex_select(re!NS-CACHE-\d\.\d:\s*\d{1,3}!)`

X_MATCH(<regular
)
	Returns TRUE if the target matches a <regular expression> argument of up to 1499 characters.
	
	The regular expression must be of the following format:
	
	`re<delimiter>regular expression< delimiter>`
	
	Both delimiters must be the same. Additionally, the regular expression must conform to the Perl-compatible expression library syntax. For more information, go tohttp://www.pcre.org/pcre.txt. In particular, see the However, note the following:
	
	· Back-references are not allowed.
	
	· Recursive regular expressions are not recommended.
	
	· The dot metacharacter also matches the newline character.
	
	· The Unicode character set is not supported.
	
	· SET_TEXT_MODE(IGNORECASE) overrides the (?i) internal option specified in the regular expression.
	
	The following are examples:
	
	http.req.hostname.regex_match(re/[[:alpha:]]+(abc){2,3}/)
	http.req.url.set_text_mode(urlencoded).regex_match(re#(a*b+c*)#)
	
	The following example matches ab and aB:
	
	`http.req.url.regex_match(re/a(?i)b/)`
	
	The following example matches ab, aB, Ab and AB:
	
	`http.req.url.set_text_mode(ignorecase).regex_match(re/ab/)`
	
	The following example performs a case-insensitive, multiline match in which the dot meta-character also m character:
	
	`http.req.body.regex_match(re/(?ixm) (^ab (.*) cd$) /)`

Configuring Classic Policies and Expressions

Some NetScaler features use classic policies and classic expressions. As with default syntax policies, classic policies can be either global or specific to a virtual server. However, to a certain extent, the configuration method and bind points for classic policies are different from those of default syntax policies. As with default syntax expressions, you can configure named expressions and use a named expression in multiple classic policies.

Where Classic Policies Are Used

The following table summarizes NetScaler features that can be configured by using classic policies.

Table 1. Policy Type and Bind Points for Policies in Features That Use Classic Policies

ature	Virtual Servers	Supported Policies	Policy Bind Points	How Y Policie
stem features, thentication	None	Authentication policies	Global	For th Authe featur contai authe schem differ authe metho examp config certifi authe schem
L	None	SSL policies	· Global · Load Balancing virtual server	To de to app encryp and ac inform clear To pro end-to securi messa decryp featur clear SSL to comm back-e server

ntent itching an use either assic or default ntax policies, t not both)	Content Switching virtual server	Content Switching policies	· Content Switching virtual server · Cache Redirection virtual server	To de server server respon servin based charac an inc reque Reque charac includ type, cookie metho type a associ server
mpression	None	HTTP Compression policies	· Global · Content Switching virtual server · Load Balancing virtual server · SSL Offload virtual server · Service	To de type o traffic compr
otection atures, Filter	None	Content Filtering policies	· Global · Content Switching virtual server · Load Balancing virtual server · SSL Offload virtual server · Service	To co behav filter
otection atures, reConnect	None	SureConnect policies	· Load Balancing virtual server · SSL Offload virtual server · Service	To co behav SureC functi
otection atures, Priority ueuing	None	Priority Queuing policies	· Load Balancing virtual server · SSL Offload virtual server	To co behav Priorit functi
TML Injection	None	HTML Injection Policies	· Global · Load Balancing virtual server · Content Switching virtual server · SSL Offload virtual server	To ena NetSc text o an HT that it client

AA - Traffic anagement	None	Authentication, Authorization, Auditing, and Session policies	· Authentication virtual server (authentication, session, and auditing policies) · Load Balancing or Content Switching virtual server (authorization and auditing policies) · Global (session and audit policies) · AAA group or user (session, auditing, and authorization policies)	To co for us specif and au user a
che edirection	Cache Redirection virtual server	Cache Redirection policies Map policies	Cache Redirection virtual server	To de wheth respon served cache server
pplication ewall	None	Application firewall policies	Global	To ide charac traffic that s should admit the fi

cess Gateway	VPN server	Pre-Authentication policies	· AAA Global · VPN vserver	To de the Ac Gatew authe autho auditi functi define rules f Web a the Ac Gatew
		Authentication policies	· System Global · AAA Global · VPN vserver	
		Auditing policies	· User · User group · VPN vserver	
		Session policies	· VPN Global · User · User Group · VPN vserver	
		Authorization policies	· User · User Group	
		Traffic policies	· VPN Global · User · User Group · VPN vserver	
		TCP Compression policies	VPN Global	

Configuring a Classic Policy

You can configure classic policies and classic expressions by using either the configuration utility or the command-line interface. A policy rule cannot exceed 1,499 characters. When configuring the policy rule, you can use named classic expressions. For more information about named expressions, see "Creating Named Classic Expressions." After configuring the policy, you bind it either globally or to a virtual server.

Note that there are small variations in the policy configuration methods for various NetScaler features.

Note: You can embed a classic expression in a default syntax expression by using the syntax SYS.EVAL_CLASSIC_EXPR***(classic_expression)***, specifying the *classic_expression* as the argument.

To create a classic policy by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- add cmp policy <name> -rule <expression> -action <action>
- show cmp policy [<policyName>]

Example

The following commands first create a compression action and then create a compression policy that applies the action:

```
> add cmp action cmp-act-compress compress
 Done
> show cmp action cmp-act-compress
1)      Name: cmp-act-compress  Compression Type: compress
 Done
> add cmp pol cmp-pol-compress -rule ExpCheckIp -resAction cmp-act-compress
 Done
> show cmp pol cmp-pol-compress
1)      Name: cmp-pol-compress  Rule: ExpCheckIp
        Response action: cmp-act-compress       Hits: 0
 Done
>
```

Parameters for configuring a classic policy

featureName

The feature for which you are creating the policy. For example, for Access Gateway policies, type `accessgw`. For application firewall policies, type `appfw`. For SSL policies, type `ssl`.

name

A name for the policy. You must begin a policy name with a letter or underscore. A policy name can consist of 1 to 31 characters, including letters, numbers, hyphen (-), period (.), pound sign (#), space ( ), and underscore (_).

expression

The expression, as described in "Configuring a Classic Expression."

action

The name of the action that you want to associate with this policy. For Access Gateway and application firewall policies, you substitute the appropriate profile instead of an action.

To create a policy with classic expressions by using the configuration utility

1. In the navigation pane, expand the feature for which you want to configure a policy and, depending on the feature, do the following:
   - For Content Switching, Cache Redirection, and the application firewall, click Policies.
   - For SSL, click Policies, and then in the details pane, click the Policies tab.
   - For System Authentication, click Authentication, and then in the details pane, click the Policies tab.
   - For Filter, SureConnect, and Priority Queuing, expand Protection Features, select the desired function, and then in the details pane, click the Policies tab.
   - For the Access Gateway, expand Access Gateway, expand Policies, select the desired function, and then in the details pane, click the Policies tab.
2. For most features, click the Add button.
3. In the Create <feature name> Policy dialog box, in the Name* text box, enter a name for the policy.

   Note: Note: You must begin a policy name with a letter or underscore. A policy name can consist of 1 to 31 characters, including letters, numbers, hyphen (-), period (.), pound sign (#), space ( ), and underscore (_).
4. For most features, you associate an action or a profile. For example, you may be required to select an action, or, in the case of an Access Gateway or application firewall policy, you select a profile to associate with the policy. A profile is a set of configuration options that operate as a set of actions that are applied when the data being analyzed matches the policy rule.
5. Create an expression that describes the type of data that you want this policy to match.

   Depending on the type of policy you want to create, you can choose a predefined expression, or you can create a new expression. For instructions on how to create an expression for most types of classic policies, see "Configuring a Classic Expression."

   Named expressions are predefined expressions that you can reference by name in a policy rule. For more information about named expressions, see "Creating Named Classic Expressions." For a list of all the default named expressions and a definition of each, see "Expressions Reference."
6. Click Create to create your new policy.
7. Click Close to return to the Policies screen for the type of policy you were creating.

Configuring a Classic Expression

Classic expressions consist of the following expression elements, listed in hierarchical order:

- **Flow Type.** Specifies whether the connection is incoming or outgoing. The flow type is REQ for incoming connections and RES for outgoing connections.
- **Protocol.** Specifies the protocol, the choices for which are HTTP, SSL, TCP, and IP.
- **Qualifier.** The protocol attribute, which depends on the selected protocol.
- **Operator.** The type of test you want to perform on the connection data. Your choice of operator depends upon the connection information you are testing. If the connection information you are testing is text, you use text operators. If it is a number, you use standard numeric operators.
- **Value.** The string or number against which the connection data element—defined by the flow type, protocol, and qualifier—is tested. The value can be either a literal or an expression. The literal or expression must match the data type of the connection data element.

In a policy, classic expressions can be combined to create more complex expressions using Boolean and comparative operators.

Expression elements are parsed from left to right. The leftmost element is either REQ or RES and designates a request or a response, respectively. Successive terms define a specific connection type and a specific attribute for that connection type. Each term is separated from any preceding or following term by a period. Arguments appear in parentheses and follow the expression element to which they are passed.

The following classic expression fragment returns the client source IP for an incoming connection.

```
REQ.IP.SOURCEIP
```

The example identifies an IP address in a request. The expression element SOURCEIP designates the source IP address. This expression fragment may not be useful by itself. You can use an additional expression element, an operator, to determine whether the returned value meets specific criteria. The following expression tests whether the client IP is in the subnet 200.0.0.0/8 and returns a Boolean TRUE or FALSE:

```
REQ.IP.SOURCEIP == 200.0.0.0 -netmask 255.0.0.0
```

To create a classic policy expression by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- set appfw policy <name> -rule <expression> -action <action>
- show appfw policy <name>

Example

```
> set appfw policy GenericApplicationSSL_ 'HTTP.REQ.METHOD.EQ("get")' APPFW_DROP
 Done
> show appfw policy GenericApplicationSSL_
       Name: GenericApplicationSSL_    Rule: HTTP.REQ.METHOD.EQ("get")
       Profile: APPFW_DROP     Hits: 0
       Undef Hits: 0
       Policy is bound to following entities
       1) REQ VSERVER app_u_GenericApplicationSSLPortalPages   PRIORITY : 100
 Done
```

To add an expression for a classic policy by using the configuration utility

This procedure documents the Add Expression dialog box. Depending on the feature for which you are configuring a policy, the route by which you arrive at this dialog box may be different.

1. Perform steps 1-4 in "To create a policy with classic expressions by using the configuration utility."
2. In the Add Expression dialog box, in Expression Type, click the type of expression you want to create.
3. Under Flow Type, click the down arrow and choose a flow type.

   The flow type is typically REQ or RES. The REQ option specifies that the policy applies to all incoming connections or requests. The RES option applies the policy to all outgoing connections or responses.

   For Application Firewall policies, you should leave the expression type set to General Expression, and the flow type set to REQ. The Application Firewall treats each request and response as a single paired entity, so all Application Firewall policies begin with REQ.
4. Under Protocol, click the down arrow and choose the protocol you want for your policy expression. Your choices are:

- HTTP. Evaluates HTTP requests that are sent to a Web server. For classic expressions, HTTP includes HTTPS requests.
- SSL. Evaluates SSL data associated with the current connection.
- TCP. Evaluates the TCP data associated with the current connection.
- IP. Evaluates the IP addresses associated with the current connection.

5. Under Qualifier, click the down arrow and choose a qualifier for your policy.

   The qualifier defines the type of data to be evaluated. The list of qualifiers that appears depends on which protocol you selected in step 4.

   The following list describes the qualifier choices for the HTTP protocol. For a complete list of protocols and qualifiers, see "Classic Expressions."

   The following choices appear for the HTTP protocol:

   - METHOD. Filters HTTP requests that use a particular HTTP method.
   - URL. Filters HTTP requests for a specific Web page.
   - URLQUERY. Filters HTTP requests that contain a particular query string.
   - VERSION. Filters HTTP requests on the basis of the specified HTTP protocol version.
   - HEADER. Filters on the basis of a particular HTTP header.
   - URLLEN. Filters on the basis of the length of the URL.
   - URLQUERY. Filters on the basis of the query portion of the URL.
   - URLQUERYLEN. Filters on the basis of the length of the query portion of the URL only.

6. Under Operator, click the down arrow and choose the operator for your policy expression. For a complete list of choices see the “Operators” table in "Classic Expressions." Some common operators are:

Operator	Description
==	Matches the specified value exactly or is exactly equal to the specified value.
!=	Does not match the specified value.
>	Is greater than the specified value.
<	Is less than the specified value.
>=	Is greater than or equal to the specified value.
<=	Is less than or equal to the specified value.
CONTAINS	Contains the specified value.

CONTENTS	Returns the contents of the designated header, URL, or URL query.
EXISTS	The specified header or query exists.
NOTCONTAINS	Does not contain the specified value.
NOTEXISTS	The specified header or query does not exist.

7. If a Value text box appears, type a string or numeric value, as appropriate. For example, chose REQ as the Flow Type, HTTP as the Protocol, and HEADER as the qualifier, and then type the value of the header string in the Value field and the header type for which you want to match the string in the Header Name text box.

8. Click OK.

9. To create a compound expression, click Add. Note that the type of compounding that is done depends on the following choices in the Create Policy dialog box:

   - **Match Any Expression.** The expressions are in a logical OR relationship.

   - **Match All Expressions.** The expressions are in a logical AND relationship.

   - **Tabular Expressions.** Click the AND, OR, and parentheses buttons to control evaluation.

   - **Advanced Free-Form.** Enter the expressions components directly into the Expression field, and click the AND, OR, and parentheses buttons to control evaluation.

Binding a Classic Policy

Depending on the policy type, you can bind a classic policy either globally or to a virtual server. Policy bind points are described in the table, "Policy Type and Bind Points for Policies in Features That Use Classic Policies."

Note: You can bind a classic policy to multiple bind points.

To bind a classic policy globally by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- bind cmp global <policyName> [-priority <positive_integer>]
- show cmp global

Example

```
> bind cmp global cmp-pol-compress -priority 2
 Done
> show cmp global
1)      Policy Name: cmp-pol-compress   Priority: 2
2)      Policy Name: ns_nocmp_xml_ie    Priority: 8700
3)      Policy Name: ns_nocmp_mozilla_47        Priority: 8800
4)      Policy Name: ns_cmp_mscss       Priority: 8900
5)      Policy Name: ns_cmp_msapp       Priority: 9000
6)      Policy Name: ns_cmp_content_type        Priority: 10000
 Done
>
```

To bind a classic policy to a virtual server by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- bind lb vserver <name> [<targetVserver>] [-policyName <string> [-priority <positive_integer>]
- show lb vserver<name>

Example

```
> bind lb vserver lbtemp -policyName cmp-pol-compress -priority 1
 Done
> show lb vserver lbtemp
        lbtemp (10.102.29.101:80) - HTTP        Type: ADDRESS
        State: UP
        Last state change was at Tue Oct 27 06:40:38 2009 (+557 ms)
        Time since last state change: 0 days, 02:00:40.330
        Effective State: UP
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  1 (Total)       1 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: Bound service's state changed to UP
        Group: vserver-grp
        Mode: IP
        Persistence: COOKIEINSERT (version 0)   Persistence Backup: SOURCEIP   Persistence Mask: 255.255.255
        Persistence Timeout: 2 min      Backup Persistence Timeout: 2 min
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none
1) http-one (10.102.29.252: 80) - HTTP State: UP        Weight: 1
        Persistence Cookie Value : NSC_wtfswfs-hsq=ffffffff096e03ed45525d5f4f58455e445a4a423660
1)      Policy : cmp-pol-compress Priority:1
 Done
>
```

Parameters for binding a classic policy

featureName

The name of the feature for which you are creating a policy. For application firewall policies, type `appfw`. For Access Gateway policies, type `accessgw`. For SSL policies, type `ssl`.

policyName

The name of the policy that you want to bind.

name

The name of the virtual server to which you bind the policy.

priority

The priority that you want to assign to the policy.

To bind a classic policy globally by using the configuration utility

Note: This procedure documents the Global Bindings dialog box. Depending on the feature for which you want to globally bind a policy, the route by which you arrive at this dialog box may be different.

1. In the navigation pane, expand the feature for which you want to globally bind a classic policy, and then locate the policy that you want to bind globally.

   Note: You cannot globally bind policies for Content Switching, Cache Redirection, SureConnect, Priority Queuing, or Access Gateway Authorization.

2. In the details pane, click Global Bindings.

3. In the Bind/Unbind <feature name> Policy(s) to Global dialog box, click Insert Policy.

4. In the Policy Name column, click the name of an existing policy that you want to globally bind, or click New Policy to open the Create <feature name> Policy dialog box.

5. After you have selected the policy or created a new policy, in the Priority column, type the priority value.

   The lower the number, the sooner this policy is applied relative to other policies. For example, a policy assigned a priority of 10 is applied before a policy with a priority of 100. You can use the same priority for different policies. All features that use classic policies implement only the first policy that a connection matches, so policy priority is important for getting the results you intend.

   As a best practice, leave room to add policies by setting priorities with intervals of 50 (or 100) between each policy.

6. Click OK.

To bind a classic policy to a virtual server by using the configuration utility

1. In the navigation pane, expand the feature that contains the virtual server to which you want to bind a classic policy (for example, if you want to bind a classic policy to a content switching virtual server, expand Content Switching), and then click Virtual Servers.

2. In the details pane, select the virtual server, and then click Open.

3. In the Configure <Feature> Virtual Server dialog box, on the Policies tab, click the feature icon for the type policy that you want, and then click Insert Policy.

4. In the Policy Name column, click the name of an existing policy that you want to bind to a virtual server, or click A to open the Create <feature name> Policy dialog box.

5. After you have selected the policy or created a new policy, in the Priority column, set the priority.

   If you are binding a policy to a content switching virtual server, in the Target column, select a load balancing virtual server to which traffic that matches the policy should be sent.

6. Click OK.

Viewing Classic Policies

You can view classic policies by using either the configuration utility or the command line. You can view details such as the policy's name, expression, and bindings.

To view a classic policy and its binding information by using the command line interface

At the command prompt, type the following commands to view a classic policy and its binding information:

show <featureName> policy [policyName]

Example

```
> show appfw policy GenericApplicationSSL_
      Name: GenericApplicationSSL_    Rule: ns_only_get_adv
      Profile: GenericApplicationSSL_Prof1    Hits: 0
      Undef Hits: 0
      Policy is bound to following entities
      1) REQ VSERVER app_u_GenericApplicationSSLPortalPages   PRIORITY : 100
 Done
```

Note: If you omit the policy name, all policies are listed without the binding details.

Parameters for viewing a classic policy

featureName

The name of the feature with which the policy is associated.

policyName

The name of the policy that you want to view.

To view classic policies and policy bindings by using the configuration utility

1. In the navigation pane, expand the feature whose policies you want to view, (for example, if you want to view application firewall policies, expand Application Firewall), and then click Policies.

2. In the details pane, do one or more of the following:

   - To view details for a specific policy, click the policy. Details appear in the Details area of the configuration pane.

   - To view bindings for a specific policy, click the policy, and then click Show Bindings.

   - To view global bindings, click the policy, and then click Global Bindings. Note that you cannot bind a Content Switching, Cache Redirection, SureConnect, Priority Queuing, or Access Gateway Authorization policy globally.

Creating Named Classic Expressions

A named classic expression is a classic expression that can be referenced through an assigned name. Often, you need to configure classic expressions that are large or complex and form a part of a larger compound expression. You might also configure classic expressions that you need to use frequently and in multiple compound expressions or classic policies. In these scenarios, you can create the classic expression you want, save it with a name of your choice, and then reference the expression from compound expressions or policies through its name. This saves configuration time and improves the readability of complex compound expressions. Additionally, any modifications to a named classic expression need to be made only once.

Some named expressions are built-in, and a subset of these are read-only. Built-in named expressions are divided into four categories: General, Anti-Virus, Personal Firewall, and Internet Security. General named expressions have a wide variety of uses. For example, from the General category, you can use the expressions `ns_true` and `ns_false` to specify a value of TRUE or FALSE, respectively, to be returned for all traffic. You can also identify data of a particular type (for example, HTM, DOC, or GIF files), determine whether caching headers are present, or determine whether the round trip time for packets between a client and the NetScaler is high (over 80 milliseconds).

Anti-Virus, Personal Firewall, and Internet Security named expressions test clients for the presence of a particular program and version and are used primarily in Access Gateway policies.

For descriptions of the built-in named expressions, see "Classic Expressions."

Note: You cannot modify or delete built-in named expressions.

To create a named classic expression by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- add expression <name> <value> [-comment <string>] [-clientSecurityMessage <string>]
- show expression [<name> | -type CLASSIC

Example

```
> add expression classic_ne "REQ.HTTP.URL CONTAINS www.example1.com" -comment "Checking the URL for
 Done
> show expression classic_ne
1)     Name: classic_ne  Expr: REQ.HTTP.URL CONTAINS www.example1.com  Hits: 0 Type : CLASSIC
       Comment: "Checking the URL for www.example1.com"
 Done
```

>

Parameters for creating a named classic expression

name

The name of the expression that will be created. This is a required argument. The maximum length of the expression is 63 characters.

value

The expression string. This is a required argument. The maximum length is 1499 characters.

comment

Any comments that you may want to associate with the expression. The maximum length is 255 characters.

clientSecurityMessage

The client security message that must be displayed if the expression evaluates to false. This parameter is valid for expressions that perform endpoint checks only. The maximum length is 127 characters.

To create a named classic expression by using the configuration utility

1. In the navigation pane, expand AppExpert, expand Expressions, and then click Classic Expressions.
2. In the details pane, click Add.

   Note: Some of the built-in expressions in the Expressions list are read-only.
3. In the Create Policy Expression dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for creating a named classic expression" as shown:

   - Expression Name*—name
   - Client Security Message—clientSecurityMessage
   - Comments—comment

   * A required parameter
4. To create the expression, do one of the following:

   - You can choose inputs to this expression from the Named Expressions drop-down list.
   - You can create a new expression, as described in "To add an expression for a classic policy by using the configuration utility."
5. When you are done, click Close. Verify that your new expression was created by scrolling to the bottom of the Classic Expressions list to view it.

Expressions Reference

The following tables list expressions and expression elements that you can use to identify specific types of data. The first table applies to default syntax expressions, in alphabetic order. The remaining tables cover the different types of classic expressions.

Default Syntax Expressions

The following table is a listing of default syntax expression prefixes, with cross-references to descriptions of these prefixes and the operators that you can specify for them. Note that some prefixes can work with multiple types of operators. For example, a cookie can be parsed by using operators for text or operators for HTTP headers.

You can use any element in the following tables as a complete expression on its own, or you can use various operators to combine these expression elements with others to form more complex expressions.

Note: The Description column in the following table contains cross-references to additional information about prefix usage and applicable operators for the prefix.

Expression Prefix	Links to Relevant Information, with Applicable Notes and Operator Descriptions
`CLIENT.ETHER`	"Prefixes for MAC Addresses." "Operations for MAC Addresses."
`CLIENT.ETHER.[DSTMAC | SRCMAC]`	"Prefixes for MAC Addresses." "Operations for MAC Addresses."
`CLIENT.INTERFACE`	Designates an expression that refers to the ID of the network interface through which the current packet entered the Application Switch. See the other `CLIENT.INTERFACE` prefix descriptions in this table.
`CLIENT.INTERFACE.ID`	Extracts the ID of the network interface that received the current packet of data. See the other `CLIENT.INTERFACE` prefix descriptions in this table.
`CLIENT.INTERFACE.ID.EQ("id")`	Returns Boolean TRUE if the interface's ID matches the ID that is passed as the argument. For example: `CLIENT.INTERFACE.ID.EQ("1/1")` See "Booleans in Compound Expressions."
`CLIENT.INTERFACE.[RXTHROU GHPUT | RXTXTHROUGHPUT | TXTHROUGHPUT]`	"Expressions for Numeric Client and Server Data." "Compound Operations for Numbers."
`CLIENT.IP`	Operates on the IP protocol data associated with the current packet. See the other `CLIENT.IP` prefixes in this table.

`CLIENT.IP.DST`	"Prefixes for IPV4 Addresses and IP Subnets." "Operations for IPV4 Addresses." "Compound Operations for Numbers."
`CLIENT.IP.SRC`	"Prefixes for IPV4 Addresses and IP Subnets." "Operations for IPV4 Addresses." "Compound Operations for Numbers."
`CLIENT.IPV6`	Operates on IPv6 protocol data. See the other `CLIENT.IPV6` prefixes in this table.
`CLIENT.IPV6.DST`	"Expression Prefixes for IPv6 Addresses." "Operations for IPV6 Prefixes."
`CLIENT.IPV6.SRC`	"Expression Prefixes for IPv6 Addresses." "Operations for IPV6 Prefixes."
`CLIENT.SSL`	Operates on the SSL protocol data for the current packet. See the other `CLIENT.SSL` prefixes in this table.
`CLIENT.SSL.CIPHER_BITS`	"Prefixes for Numeric Data in SSL Certificates." "Compound Operations for Numbers."
`CLIENT.SSL.CIPHER_EXPORTA BLE`	"Prefixes for Text-Based SSL and Certificate Data." "Booleans in Compound Expressions.
`CLIENT.SSL.CLIENT_CERT`	"Expressions for SSL Certificates." "Expressions for SSL Certificate Dates."
`CLIENT.SSL.IS_SSL`	"Prefixes for Text-Based SSL and Certificate Data." "Booleans in Compound Expressions."
`CLIENT.SSL.VERSION`	"Prefixes for Numeric Data in SSL Certificates." "Compound Operations for Numbers."
`CLIENT.TCP`	Operates on TCP protocol data. See the other `CLIENT.TCP` prefixes in this table.
`CLIENT.TCP.[DSTPORT | MSS | SRCPORT]`	"Expressions for TCP, UDP, and VLAN Data." "Compound Operations for Numbers."
`CLIENT.TCP.PAYLOAD( integer )`	"Expressions for TCP, UDP, and VLAN Data." "Default Syntax Expressions: Evaluating Text."

`CLIENT.UDP`	Operates on the UDP protocol data associated with the current packet. See the other `CLIENT.UDP` prefixes in this table.
`CLIENT.UDP.DNS.DOMAIN`	"Expressions for TCP, UDP, and VLAN Data." "Default Syntax Expressions: Evaluating Text."
`CLIENT.UDP.DNS.DOMAIN.EQ("`*`hostname`*`")`	"Expressions for TCP, UDP, and VLAN Data." "Booleans in Compound Expressions."
`CLIENT.UDP.DNS. [IS_AAAAREC | IS_ANYREC | IS_AREC | IS_CNAMEREC | IS_MXREC | IS_NSREC | IS_PTRREC | IS_SOAREC | IS_SRVREC]`	"Expressions for TCP, UDP, and VLAN Data." "Booleans in Compound Expressions."
`CLIENT.UDP.[DSTPORT | SRCPORT]`	"Expressions for TCP, UDP, and VLAN Data." "Compound Operations for Numbers."
`CLIENT.VLAN`	Operates on the VLAN through which the current packet entered the NetScaler. See the other `CLIENT.VLAN` prefixes in this table.
`CLIENT.VLAN.ID`	"Expressions for TCP, UDP, and VLAN Data." "Compound Operations for Numbers."
`HTTP.REQ`	Operates on HTTP requests. See the other `HTTP.REQ` prefixes in this table.
`HTTP.REQ.BODY(`*`integer`*`)`	"Expression Prefixes for Text in HTTP Requests and Responses." "Basic Operations on Text."
`HTTP.REQ.CACHE_CONTROL`	"Prefixes for Cache-Control Headers." "Operations for Cache-Control Headers."
`HTTP.REQ.CONTENT_LENGTH`	"Expressions for Numeric HTTP Payload Data Other Than Dates." "Compound Operations for Numbers."
`HTTP.REQ.COOKIE`	"Prefixes for HTTP Headers." "Operations for HTTP Headers." "Default Syntax Expressions: Evaluating Text."

`HTTP.REQ.DATE`	"Format of Dates and Times in an Expression." "Expressions for HTTP Request and Response Dates." "Default Syntax Expressions: Evaluating Text." "Compound Operations for Numbers." "Operations for HTTP Headers."
`HTTP.REQ.HEADER("`*`header_name`*`")`	"Expression Prefixes for Text in HTTP Requests and Responses." "Prefixes for HTTP Headers." "Operations for HTTP Headers."
`HTTP.REQ.FULL_HEADER("`*`header_name`*`")`	"Prefixes for HTTP Headers." "Operations for HTTP Headers."
`HTTP.REQ.HOSTNAME`	"Expression Prefixes for Text in HTTP Requests and Responses."
`HTTP.REQ.HOSTNAME.[DOMAIN | Server]`	"Expression Prefixes for Text in HTTP Requests and Responses." "Basic Operations on Text."
`HTTP.REQ.HOSTNAME.EQ("`*`hostname`*`")`	"Expression Prefixes for Text in HTTP Requests and Responses." "Booleans in Compound Expressions." "“Basic Operations on Expression Prefixes”."
`HTTP.REQ.HOSTNAME.PORT`	"Expression Prefixes for Text in HTTP Requests and Responses." "Compound Operations for Numbers."
`HTTP.REQ.IS_VALID`	Returns TRUE if the HTTP request is properly formed. See "Booleans in Compound Expressions."
`HTTP.REQ.METHOD`	"Expression Prefixes for Text in HTTP Requests and Responses." "Basic Operations on Text." "Complex Operations on Text."
`HTTP.REQ.TRACKING`	Returns the HTTP body tracking mechanism. See the descriptions of other `HTTP.REQ.TRACKING` prefixes in this table.

HTTP.REQ.TRACKING.EQ("*tracking_ method name*")	Returns TRUE or FALSE. See "Booleans in Compound Expressions."
HTTP.REQ.URL	Obtains the HTTP URL object from the request and sets the text mode to URLENCODED by default. See "Expression Prefixes for Text in HTTP Requests and Responses."
HTTP.REQ.URL.[CVPN_ENCODE | HOSTNAME | HOSTNAME.DOMAIN | SERVER | PATH | PATH_AND_QUERY | PROTOCOL | QUERY | SUFFIX | VERSION]	"Expression Prefixes for Text in HTTP Requests and Responses." "Basic Operations on Text." "Complex Operations on Text."
HTTP.REQ.URL.HOSTNAME.EQ("*hostn ame*")	"Expression Prefixes for Text in HTTP Requests and Responses. "Booleans in Compound Expressions."
HTTP.REQ.URL.HOSTNAME.PORT	"Expression Prefixes for Text in HTTP Requests and Responses. "Compound Operations for Numbers."
HTTP.REQ.URL.PATH.IGNORE_ EMPTY_ELEMENTS	Ignores spaces in the data. See the table "HTTP Expression Prefixes that Return Text."
HTTP.REQ.URL.QUERY.IGNORE _EMPTY_ELEMENTS	Ignores spaces in the data. See the table "HTTP Expression Prefixes that Return Text."
HTTP.REQ.USER.IS_MEMBER_OF	"HTTP Expression Prefixes that Return Text."
HTTP.REQ.USER.NAME	"HTTP Expression Prefixes that Return Text."
HTTP.REQ.VERSION	"Expression Prefixes for Text in HTTP Requests and Responses."
HTTP.REQ.VERSION.[MAJOR | MINOR]	Operates on the major or minor HTTP version string. See "Expression Prefixes for Text in HTTP Requests and Responses" and "Compound Operations for Numbers."
HTTP.RES	Operates on HTTP responses.
HTTP.RES.BODY(*integer*)	"Expression Prefixes for Text in HTTP Requests and Responses." "Basic Operations on Text." "Complex Operations on Text."
HTTP.RES.CACHE_CONTROL	"Prefixes for Cache-Control Headers." "Operations for Cache-Control Headers."

HTTP.RES.CONTENT_LENGTH	"Expression Prefixes for Text in HTTP Requests and Responses." "Operations for HTTP Headers." "Compound Operations for Numbers."
HTTP.RES.DATE	"Format of Dates and Times in an Expression." "Expressions for HTTP Request and Response Dates." "Expression Prefixes for Text in HTTP Requests and Responses." "Compound Operations for Numbers." "Operations for HTTP Headers."
HTTP.RES.HEADER("*header_name*")	"Expression Prefixes for Text in HTTP Requests and Responses." "Prefixes for HTTP Headers." "Operations for HTTP Headers."
HTTP.REQ.FULL_HEADER("*header_name*")	"Prefixes for HTTP Headers." "Operations for HTTP Headers."
HTTP.REQ.TXID	"Prefixes for HTTP Headers." "Operations for HTTP Headers."
HTTP.RES.IS_VALID	Returns TRUE if the HTTP response is properly formed. See "Booleans in Compound Expressions."
HTTP.RES.SET_COOKIE	"Prefixes for HTTP Headers." "Operations for HTTP Headers." "Default Syntax Expressions: Evaluating Text."
HTTP.RES.SET_COOKIE.COOKIE("*name*")	"Prefixes for HTTP Headers." "Operations for HTTP Headers." "Default Syntax Expressions: Evaluating Text."
HTTP.RES.SET_COOKIE.COOKIE.[DOMAIN | PATH | PORT]	"Prefixes for HTTP Headers." "Operations for HTTP Headers." "Default Syntax Expressions: Evaluating Text."

HTTP.RES.SET_COOKIE.COOKIE.EXPIRES	Obtains the Expires field of the cookie as a date string. The value of the Expires attribute can be operated upon as a time object. If multiple Expires fields are present, this expression operates on the first one. If the Expires attribute is absent, a string of length zero is returned. Also see: "Prefixes for HTTP Headers." "Operations for HTTP Headers." "Default Syntax Expressions: Evaluating Text." "Compound Operations for Numbers."
HTTP.RES.SET_COOKIE.COOKIE.PATH.IGNORE_EMPTY_ELEMENTS	Ignores spaces in the data. For an example, see the table "Expression Prefixes for Text in HTTP Requests and Responses."
HTTP.RES.SET_COOKIE.COOKIE.PORT.IGNORE_EMPTY_ELEMENTS	Ignores spaces in the data. For an example, see the table "HTTP Expression Prefixes that Return Text."
HTTP.RES.SET_COOKIE.COOKIE.VERSION	"Prefixes for HTTP Headers." "Compound Operations for Numbers."
HTTP.RES.SET_COOKIE.COOKIE("*name*"[,*integer*])[.PORT | .PATH | DOMAIN | VERSION | EXPIRES]	"Prefixes for HTTP Headers." "Default Syntax Expressions: Evaluating Text."
HTTP.RES.SET_COOKIE.COOKIE.EXPIRES	"Prefixes for HTTP Headers." "Operations for HTTP Headers." "Default Syntax Expressions: Evaluating Text." "Compound Operations for Numbers."
HTTP.RES.SET_COOKIE.EXISTS("*name*")	"Prefixes for HTTP Headers." "Booleans in Compound Expressions."
HTTP.RES.SET_COOKIE2	"Prefixes for HTTP Headers." "Operations for HTTP Headers." "Default Syntax Expressions: Evaluating Text."

HTTP.RES.SET_COOKIE2.COOKIE("*name*")	"Prefixes for HTTP Headers." "Operations for HTTP Headers." "Default Syntax Expressions: Evaluating Text."
HTTP.RES.SET_COOKIE2.COOKIE.[DOMAIN | PATH | PORT]	"Prefixes for HTTP Headers." "Operations for HTTP Headers." "Default Syntax Expressions: Evaluating Text."
HTTP.RES.SET_COOKIE2.COOKIE.EXPIRES	"Prefixes for HTTP Headers." "Operations for HTTP Headers." "Default Syntax Expressions: Evaluating Text." "Compound Operations for Numbers."
HTTP.RES.SET_COOKIE2.COOKIE.PATH.IGNORE_EMPTY_ ELEMENTS	Ignores spaces in the data. For an example, see the table HTTP Expression Prefixes that Return Text."
HTTP.RES.SET_COOKIE2.COOKIE.PORT.IGNORE_EMPTY_ ELEMENTS	Ignores spaces in the data. For an example, see the table "HTTP Expression Prefixes that Return Text." See also "Default Syntax Expressions: Evaluating Text" and "Compound Operations for Numbers."
HTTP.RES.SET_COOKIE2.COOKIE("*name*")[.integer].[PORT | PATH | DOMAIN | VERSION | EXPIRES]	"Prefixes for HTTP Headers." "Operations for HTTP Headers." "Default Syntax Expressions: Evaluating Text."
HTTP.RES.SET_COOKIE2.COOKIE.DOMAIN	"Prefixes for HTTP Headers." "Operations for HTTP Headers." "Default Syntax Expressions: Evaluating Text."
HTTP.RES.SET_COOKIE2.COOKIE.EXPIRES	"Prefixes for HTTP Headers." "Operations for HTTP Headers." "Default Syntax Expressions: Evaluating Text." "Compound Operations for Numbers."

HTTP.RES.SET_COOKIE2.COOKIE.VERSION	"Prefixes for HTTP Headers." "Operations for HTTP Headers." "Default Syntax Expressions: Evaluating Text." "Compound Operations for Numbers."
HTTP.RES.SET_COOKIE2.EXISTS("*name*")	"Prefixes for HTTP Headers." "Operations for HTTP Headers." "Booleans in Compound Expressions."
HTTP.RES.STATUS	"Expression Prefixes for Text in HTTP Requests and Responses." "Compound Operations for Numbers."
HTTP.RES.STATUS_MSG	"Expression Prefixes for Text in HTTP Requests and Responses."
HTTP.RES.TRACKING	Returns the HTTP body tracking mechanism. See the descriptions of other HTTP.REQ.TRACKING prefixes in this table.
HTTP.RES.TRACKING.EQ("*tracking_method*")	Returns TRUE or FALSE. See "Booleans in Compound Expressions."
HTTP.RES.TXID	" Prefixes for HTTP Headers." "Operations for HTTP Headers."
HTTP.RES.VERSION	"Expression Prefixes for Text in HTTP Requests and Responses."
HTTP.RES.VERSION.[MAJOR | MINOR]	Operates on the major or minor HTTP version string. See "Expression Prefixes for Text in HTTP Requests and Responses" and "Compound Operations for Numbers."
SERVER	Designates an expression that refers to the server. This is the starting point for access into parameters such as Ether and SSL. See the other SERVER prefixes in this table.
SERVER.ETHER	Operates on the ethernet protocol data associated with the current packet. See the other SERVER prefixes in this table.
SERVER.ETHER.DSTMAC	"Prefixes for MAC Addresses." "Prefixes for MAC Addresses."
SERVER.INTERFACE	Designates an expression that refers to the ID of the network interface that received the current packet of data. See the other SERVER.INTERFACE prefixes in this table.

SERVER.INTERFACE.ID.EQ("*id*")	Returns Boolean TRUE if the interface's ID matches the ID that is passed as the argument. For example: SERVER.INTERFACE.ID.EQ("LA/1") See "Booleans in Compound Expressions."
SERVER.INTERFACE.[RXTHROUGHPUT | RXTXTHROUGHPUT | TXTHROUGHPUT]	"Expressions for Numeric Client and Server Data." "Compound Operations for Numbers."
SERVER.IP	Operates on the IP protocol data associated with the current packet. See the other SERVER.IP prefixes in this table.
SERVER.IP.[DST | SRC]	"Prefixes for IPV4 Addresses and IP Subnets." "Operations for IPV4 Addresses." "Compound Operations for Numbers."
SERVER.IPV6	Operates on IPv6 protocol data. See the other SERVER.IPV6 prefixes in this table.
SERVER.IPV6.DST	"Expression Prefixes for IPv6 Addresses." "Operations for IPV6 Prefixes."
SERVER.IPV6.SRC	"Expression Prefixes for IPv6 Addresses." "Operations for IPV6 Prefixes."
SERVER.TCP	Operates on TCP protocol data. See the other CLIENT.TCP prefixes in this table.
SERVER.TCP.[DSTPORT | MSS | SRCPORT]	"Expressions for TCP, UDP, and VLAN Data." "Compound Operations for Numbers."
SERVER.VLAN	Operates on the VLAN through which the current packet entered the NetScaler. See the other SERVER.VLAN prefixes in this table.
SERVER.VLAN.ID	"Expressions for TCP, UDP, and VLAN Data." "Compound Operations for Numbers."
SYS	Designates an expression that refers to the NetScaler itself, not to the client or server.. See the other SYS prefixes in this table.
SYS.EVAL_CLASSIC_EXPR(*classic_expression*)	"Classic Expressions in Default Syntax Expressions." "Booleans in Compound Expressions."
SYS.HTTP_CALLOUT(*http_callout*)	"HTTP Callouts."
SYS.CHECK_LIMIT	"Rate Limiting."

SYS.TIME	"Expressions for the NetScaler System Time." "Compound Operations for Numbers."
SYS.TIME.[BETWEEN(*time1, time2*) | EQ(*time*) | GE(*time*) | GT(*time*) | LE(*time*) | LT(*time*) | WITHIN(*time1, time2*)]	"Expressions for the NetScaler System Time." "Booleans in Compound Expressions." "Compound Operations for Numbers."
SYS.TIME.[DAY | HOURS | MINUTES | MONTH | RELATIVE_BOOT | RELATIVE_NOW SECONDS | WEEKDAY | YEAR]	"Expressions for the NetScaler System Time." "Compound Operations for Numbers."
SYS.RANDOM	Returns a random number between 0 and 1, inclusive of 0 but exclusive of 1.
VPN.BASEURL.[CVPN_DECODE | CVPN_ENCODE | HOSTNAME | HOSTNAME.DOMAIN | HOSTNAME.SERVER | PATH | PATH_AND_QUERY | PROTOCOL | QUERY | SUFFIX]	"Expression Prefixes for VPNs and Clientless VPNs."
VPN.BASEURL.HOSTNAME.EQ("*hostna me*")	"Expression Prefixes for VPNs and Clientless VPNs." "Booleans in Compound Expressions."
VPN.BASEURL.HOSTNAME.PORT	"Expression Prefixes for VPNs and Clientless VPNs." "Compound Operations for Numbers."
VPN.BASEURL.PATH.IGNORE_EMPTY_ELEMENTS	Ignores spaces in the data. For an example, see the table "HTTP Expression Prefixes that Return Text."
VPN.BASEURL.QUERY.IGNORE_EMPTY_ELEMENTS	Ignores spaces in the data. For an example, see the table "HTTP Expression Prefixes that Return Text."
VPN.CLIENTLESS_BASEURL	" Expression Prefixes for VPNs and Clientless VPNs."
VPN.CLIENTLESS_BASEURL.[CVPN_DECODE | CVPN_ENCODE | HOSTNAME | HOSTNAME.DOMAIN | HOSTNAME.SERVER | PATH | PATH_AND_QUERY | PROTOCOL | QUERY | SUFFIX]	"Expression Prefixes for VPNs and Clientless VPNs."
VPN.CLIENTLESS_BASEURL.HOSTNAME.EQ("*hostname*")	"Expression Prefixes for VPNs and Clientless VPNs." "Booleans in Compound Expressions."

VPN.CLIENTLESS_BASEURL.HOSTNAME .PORT	"Expression Prefixes for VPNs and Clientless VPNs." "Compound Operations for Numbers."
VPN.CLIENTLESS_BASEURL.PATH.IGN ORE_EMPTY_ELEMENTS	Ignores spaces in the data. For an example, see the table "HTTP Expression Prefixes that Return Text."
VPN.CLIENTLESS_BASEURL.QUERY.IG NORE_EMPTY_ELEMENTS	Ignores spaces in the data. For an example, see the table "HTTP Expression Prefixes that Return Text."
VPN.CLIENTLESS_HOSTURL	" Expression Prefixes for VPNs and Clientless VPNs."
VPN.CLIENTLESS_HOSTURL.[CVPN_DE CODE | CVPN_ENCODE | HOSTNAME | HOSTNAME.DOMAIN | HOSTNAME.SERVER | PATH | PATH_AND_QUERY | PROTOCOL | QUERY | SUFFIX]	"Expression Prefixes for VPNs and Clientless VPNs."
VPN.CLIENTLESS_HOSTURL.HOSTNAME .EQ("*hostname*")	"Expression Prefixes for VPNs and Clientless VPNs." "Booleans in Compound Expressions.
VPN.CLIENTLESS_HOSTURL.HOSTNAME .PORT	"Expression Prefixes for VPNs and Clientless VPNs." "Compound Operations for Numbers."
VPN.CLIENTLESS_HOSTURL.PATH.IGN ORE_EMPTY_ELEMENTS	Ignores spaces in the data. For an example, see the table "HTTP Expression Prefixes that Return Text."
VPN.CLIENTLESS_HOSTURL.QUERY.IG NORE_EMPTY_ELEMENTS	Ignores spaces in the data. For an example, see the table "HTTP Expression Prefixes that Return Text."
VPN.HOST	" Expression Prefixes for VPNs and Clientless VPNs."
VPN.HOST.[DOMAIN | Server]	"Expression Prefixes for VPNs and Clientless VPNs."
VPN.HOST.EQ("*hostname*")	"Expression Prefixes for VPNs and Clientless VPNs." "Booleans in Compound Expressions.
VPN.HOST.PORT	"Expression Prefixes for VPNs and Clientless VPNs." "Default Syntax Expressions: Evaluating Text." "Compound Operations for Numbers."

Classic Expressions

The subtopics listed in the table of contents on the left side of your screen contain tables listing the NetScaler classic expressions.

In the table of operators, the result type of each operator is shown at the beginning of the description. In the other tables, the level of each expression is shown at the beginning of the description. For named expressions, each expression is shown as a whole.

Operators

Expression Element	Definition
==	Boolean. Returns TRUE if the current expression equals the argument. For text operations, the items being compared must exactly match one another. For numeric operations, the items must evaluate to the same number.
!=	Boolean. Returns TRUE if the current expression does not equal the argument. For text operations, the items being compared must not exactly match one another. For numeric operations, the items must not evaluate to the same number.
CONTAINS	Boolean. Returns TRUE if the current expression contains the string that is designated in the argument.
NOTCONTAINS	Boolean. Returns TRUE if the current expression does not contain the string that is designated in the argument.
CONTENTS	Text. Returns the contents of the current expression.
EXISTS	Boolean. Returns TRUE if the item designated by the current expression exists.
NOTEXISTS	Boolean. Returns TRUE if the item designated by the current expression does not exist.
>	Boolean. Returns TRUE if the current expression evaluates to a number that is greater than the argument.

<	Boolean. Returns TRUE if the current expression evaluates to a number that is less than the argument.
>=	Boolean. Returns TRUE if the current expression evaluates to a number that is greater than or equal to the argument.
<=	Boolean. Returns TRUE if the current expression evaluates to a number that is less than or equal to the argument.

General Expressions

Expression Element	Definition
REQ	Flow Type. Operates on incoming (or request) packets.
REQ.HTTP	Protocol Operates on HTTP requests.
REQ.HTTP.METHOD	Qualifier Designates the HTTP method.
REQ.HTTP.URL	Qualifier Designates the URL.
REQ.HTTP.URLTOKENS	Qualifier Designates the URL token.
REQ.HTTP.VERSION	Qualifier Designates the HTTP version.
REQ.HTTP.HEADER	Qualifier Designates the HTTP header.
REQ.HTTP.URLLEN	Qualifier Designates the number of characters in the URL.
REQ.HTTP.URLQUERY	Qualifier Designates the query portion of the URL.
REQ.HTTP.URLQUERYLEN	Qualifier Designates the length of the query portion of the URL.
REQ.SSL	Protocol Operates on SSL requests.
REQ.SSL.CLIENT.CERT	Qualifier Designates the entire client certificate.

REQ.SSL.CLIENT.CERT.SUBJECT	Qualifier Designates the client certificate subject.
REQ.SSL.CLIENT.CERT.ISSUER	Qualifier Designates the issuer of the client certificate.
REQ.SSL.CLIENT.CERT.SIGALGO	Qualifier Designates the validation algorithm used by the client certificate.
REQ.SSL.CLIENT.CERT.VERSION	Qualifier Designates the client certificate version.
REQ.SSL.CLIENT.CERT.VALIDFROM	Qualifier Designates the date before which the client certificate is not valid.
REQ.SSL.CLIENT.CERT.VALIDTO	Qualifier Designates the date after which the client certificate is not valid.
REQ.SSL.CLIENT.CERT.SERIALNUMBER	Qualifier Designates the serial number of the client certificate.
REQ.SSL.CLIENT.CIPHER.TYPE	Qualifier Designates the encryption protocol used by the client.
REQ.SSL.CLIENT.CIPHER.BITS	Qualifier Designates the number of bits used by the client's SSL key.
REQ.SSL.CLIENT.SSL.VERSION	Qualifier Designates the SSL version that the client is using.
REQ.TCP	Protocol Operates on incoming TCP packets.
REQ.TCP.SOURCEPORT	Qualifier Designates the source port of the incoming packet.
REQ.TCP.DESTPORT	Qualifier Designates the destination port of the incoming packet.

REQ.IP	Protocol Operates on incoming IP packets.
REQ.IP.SOURCEIP	Qualifier Designates the source IP of the incoming packet.
REQ.IP.DESTIP	Qualifier Designates the destination IP of the incoming packet.
RES	Flow Type Operates on outgoing (or response) packets.
RES.HTTP	Protocol Operates on HTTP responses.
RES.HTTP.VERSION	Qualifier Designates the HTTP version.
RES.HTTP.HEADER	Qualifier Designates the HTTP header.
RES.HTTP.STATUSCODE	Qualifier Designates the status code of the HTTP response.
RES.TCP	Protocol Operates on incoming TCP packets.
RES.TCP.SOURCEPORT	Qualifier Designates the source port of the outgoing packet.
RES.TCP.DESTPORT	Qualifier Designates the destination port of the outgoing packet.
RES.IP	Protocol Operates on outgoing IP packets.

RES.IP.SOURCEIP	Qualifier Designates the source IP of the outgoing packet. This can be in IPv4 or IPv6 format. For example: `add expr exp3 “sourceip == 10.102.32.123 –netmask 255.255.255.0 && destip == 2001::23/120”.`
RES.IP.DESTIP	Qualifier Designates the destination IP of the outgoing packet.

Client Security Expressions

The expressions to configure client settings on the Access Gateway with the following software:

- Antivirus
- Personal firewall
- Antispam
- Internet Security

For example usage, see http://support.citrix.com/article/CTX112599.

Actual Expression	Definition
`CLIENT.APPLICATION.AV(<NAME>.VERSION == <VERSION>)`	Checks whether the client is running the designated anti-virus program and version.
`CLIENT.APPLICATION.AV(<NAME>.VERSION != <VERSION>)`	Checks whether the client is not running the designated anti-virus program and version.
`CLIENT.APPLICATION.PF(<NAME>.VERSION == <VERSION>)`	Checks whether the client is running the designated personal firewall program and version.
`CLIENT.APPLICATION.PF(<NAME>.VERSION != <VERSION>)`	Checks whether the client is not running the designated personal firewall program and version.
`CLIENT.APPLICATION.IS(<NAME>.VERSION == <VERSION>)`	Checks whether the client is running the designated internet security program and version.
`CLIENT.APPLICATION.IS(<NAME>.VERSION != <VERSION>)`	Checks whether the client is not running the designated internet security program and version.
`CLIENT.APPLICATION.AS(<NAME>.VERSION == <VERSION>)`	Checks whether the client is running the designated anti-spam program and version.
`CLIENT.APPLICATION.AS(<NAME>.VERSION != <VERSION>)`	Checks whether the client is not running the designated anti-spam program and version.

Network-Based Expressions

Expression	Definition
REQ	Flow Type. Operates on incoming, or request, packets.
REQ.VLANID	Qualifier. Operates on the virtual LAN (VLAN) ID.
REQ.INTERFACE.ID	Qualifier. Operates on the ID of the designated NetScaler interface.
REQ.INTERFACE.RXTHROUGHPUT	Qualifier. Operates on the raw received packet throughput of the designated NetScaler interface.
REQ.INTERFACE.TXTHROUGHPUT	Qualifier. Operates on the raw transmitted packet throughput of the designated NetScaler interface.
REQ.INTERFACE.RXTXTHROUGHPUT	Qualifier. Operates on the raw received and transmitted packet throughput of the designated NetScaler interface.
REQ.ETHER.SOURCEMAC	Qualifier. Operates on the source MAC address.
REQ.ETHER.DESTMAC	Qualifier. Operates on the destination MAC address.
RES	Flow Type. Operates on outgoing (or response) packets.
RES.VLANID	Qualifier. Operates on the virtual LAN (VLAN) ID.
RES.INTERFACE.ID	Qualifier. Operates on the ID of the designated NetScaler interface.

RES.INTERFACE.RXTHROUGHPUT	Qualifier. Operates on the raw received packet throughput of the designated NetScaler interface.
RES.INTERFACE.TXTHROUGHPUT	Qualifier. Operates on the raw transmitted packet throughput of the designated NetScaler interface.
RES.INTERFACE.RXTXTHROUGHPUT	Qualifier. Operates on the raw received and transmitted packet throughput of the designated NetScaler interface.
RES.ETHER.SOURCEMAC	Qualifier. Operates on the source MAC address.
RES.ETHER.DESTMAC	Qualifier. Operates on the destination MAC address.

Date/Time Expressions

Expression	Definition
TIME	Qualifier. Operates on the date and time of day, GMT.
DATE	Qualifier. Operates on the date, GMT.
DAYOFWEEK	Operates on the specified day in the week, GMT.

File System Expressions

You can specify file system expressions in authorization policies for users and groups who access file sharing through the Access Gateway file transfer utility (the VPN portal). These expressions work with the Access Gateway file transfer authorization feature to control user access to file servers, folders, and files. For example, you can use these expressions in authorization policies to control access based on file type and size.

Expression	Definition
`FS.COMMAND`	Qualifier. Operates on a file system command. The user can issue multiple commands on a file transfer portal. (For example, ls to list files or mkdir to create a directory). This expression returns the current action that the user is taking. Possible values: Neighbor, login, ls, get, put, rename, mkdir, rmdir, del, logout, any. Following is an example: `Add authorization policy pol1 “fs.command eq login && (fs.user eq administrator || fs.serverip eq 10.102.88.221 –netmask 255.255.255.252)” allow`
`FS.USER`	Returns the user who is logged on to the file system.
`FS.SERVER`	Returns the host name of the target server. In the following example, the string `win2k3-88-22` is the server name: `fs.server eq win2k3-88-221`
`FS.SERVERIP`	Returns the IP address of the target server.

FS.SERVICE	Returns a shared root directory on the file server. If a particular folder is exposed as shared, a user can directly log on to the specified first level folder. This first level folder is called a service. For example, in the path \\hostname\SERVICEX\ETC, SERVICEX is the service. As another example, if a user accesses the file \\hostname\service1\dir1\file1.doc, FS.SERVICE will return service1. Following is an example: `fs.service notcontains New`
FS.DOMAIN	Returns the domain name of the target server.
FS.PATH	Returns the complete path of the file being accessed. For example, if a user accesses the file \\hostname\service1\dir1\file1.doc, FS.PATH will return \service\dir1\file1.doc. Following is an example: `fs.path notcontains SSL`
FS.FILE	Returns the name of the file being accessed. For example, if a user accesses the file \\hostname\service1\dir1\file1.doc, FS.FILE will return file1.doc.
FS.DIR	Returns the directory being accessed. For example, if a user accesses the file \\hostname\service1\dir1\file1.doc, FS.DIR will return \service\dir1.
FS.FILE.ACCESSTIME	Returns the time at which the file was last accessed. This is one of several options that provide you with granular control over actions that the user performs. (See the following entries in this table.)
FS.FILE.CREATETIME	Returns the time at which the file was created.
FS.FILE.MODIFYTIME	Returns the time at which the file was edited.
FS.FILE.WRITETIME	Returns the time of the most recent change in the status of the file.
FS.FILE.SIZE	Returns the file size.
FS.DIR.ACCESSTIME	Returns the time at which the directory was last accessed.
FS.DIR.CREATETIME	Returns the time at which the directory was created.

FS.DIR.MODIFYTIME	Returns the time at which the directory was last modified.
FS.DIR.WRITETIME	Returns the time at which the directory status last changed.

Note: File system expressions do not support regular expressions.

Built-In Named Expressions (General)

Expression	Definition
ns_all_apps_ncomp	Tests for connections with destination ports between 0 and 65535. In other words, tests for all applications.
ns_cachecontrol_nocache	Tests for connections with an HTTP Cache-Control header that contains the value “no-cache”.
ns_cachecontrol_nostore	Tests for connections with an HTTP Cache-Control header that contains the value “no-store”.
ns_cmpclient	Tests the client to determine if it accepts compressed content.
ns_content_type	Tests for connections with an HTTP Content-Type header that contains “text”.
ns_css	Tests for connections with an HTTP Content-Type header that contains “text/css”.
ns_ext_asp	Tests for HTTP connections to any URL that contains the string .asp—in other words, any connection to an active server page (ASP).
ns_ext_cfm	Tests for HTTP connections to any URL that contains the string .cfm
ns_ext_cgi	Tests for HTTP connections to any URL that contains the string .cgi—in other words, any connection to a common gateway interface (CGI) script.
ns_ext_ex	Tests for HTTP connections to any URL that contains the string .ex
ns_ext_exe	Tests for HTTP connections to any URL that contains the string .exe—in other words, any connection to a executable file.
ns_ext_htx	Tests for HTTP connections to any URL that contains the string .htx
ns_ext_not_gif	Tests for HTTP connections to any URL that does not contain the string .gif—in other words, any connection to a URL that is not a GIF image.
ns_ext_not_jpeg	Tests for HTTP connections to any URL that does not contain the string .jpeg—in other words, any connection to a URL that is not a JPEG image.

ns_ext_shtml	Tests for HTTP connections to any URL that contains the string .shtml—in other words, any connection to a server-parsed HTML page.
ns_false	Always returns a value of FALSE.
ns_farclient	Client is in a different geographical region from the NetScaler, as determined by the geographical region in the client's IP address. The following regions are predefined: 192.0.0.0 – 193.255.255.255: Multi-regional 194.0.0.0 – 195.255.255.255: European Union 196.0.0.0 – 197.255.255.255: Other1 198.0.0.0 – 199.255.255.255: North America 200.0.0.0 – 201.255.255.255: Central and South America 202.0.0.0 – 203.255.255.255: Pacific Rim 204.0.0.0 – 205.255.255.255: Other2 206.0.0.0 – 207.255.255.255: Other3
ns_header_cookie	Tests for HTTP connections that contain a Cookie header
ns_header_pragma	Tests for HTTP connections that contain a Pragma: no-cache header.
ns_mozilla_47	Tests for HTTP connections whose User-Agent header contains the string Mozilla/4.7—in other words, any connection from a client using the Mozilla 4.7 Web browser.
ns_msexcel	Tests for HTTP connections whose Content-Type header contains the string application/vnd.msexcel—in other words, any connection transmitting a Microsoft Excel spreadsheet.
ns_msie	Tests for HTTP connections whose User-Agent header contains the string MSIE—in other words, any connection from a client using any version of the Internet Explorer Web browser.

ns_msppt	Tests for HTTP connections whose Content-Type header contains the string application/vnd.ms-powerpoint—in other words, any connection transmitting a Microsoft PowerPoint file.
ns_msword	Tests for HTTP connections whose Content-Type header contains the string application/vnd.msword—in other words, any connection transmitting a Microsoft Word file.
ns_non_get	Tests for HTTP connections that use any HTTP method except for GET.
ns_slowclient	Returns TRUE if the average round trip time between the client and the NetScaler is more than 80 milliseconds.
ns_true	Returns TRUE for all traffic.
ns_url_path_bin	Tests the URL path to see if it points to the /bin/ directory.
ns_url_path_cgibin	Tests the URL path to see if it points to the CGI-BIN directory.
ns_url_path_exec	Tests the URL path to see if it points to the /exec/ directory.
ns_url_tokens	Tests for the presence of URL tokens.
ns_xmldata	Tests for the presence of XML data.

Built-In Named Expressions (Anti-Virus)

Expression	Definition
McAfee Virus Scan 11	Tests to determine whether the client is running the latest version of McAfee VirusScan.
McAfee Antivirus	Tests to determine whether the client is running any version of McAfee Antivirus.
Symantec AntiVirus 10 (with Updated Definition File)	Tests to determine whether the client is running the most current version of Symantec AntiVirus.
Symantec AntiVirus 6.0	Tests to determine whether the client is running Symantec AntiVirus 6.0.
Symantec AntiVirus 7.5	Tests to determine whether the client is running Symantec AntiVirus 7.5.
TrendMicro OfficeScan 7.3	Tests to determine whether the client is running Trend Microsystems' OfficeScan, version 7.3.
TrendMicro AntiVirus 11.25	Tests to determine whether the client is running Trend Microsystems' AntiVirus, version 11.25.
Sophos Antivirus 4	Tests to determine whether the client is running Sophos Antivirus, version 4.
Sophos Antivirus 5	Tests to determine whether the client is running Sophos Antivirus, version 5.
Sophos Antivirus 6	Tests to determine whether the client is running Sophos Antivirus, version 6.

Built-In Named Expressions (Personal Firewall)

Expression	Definition
TrendMicro OfficeScan 7.3	Tests to determine whether the client is running Trend Microsystems' OfficeScan, version 7.3.
Sygate Personal Firewall 5.6	Tests to determine whether the client is running the Sygate Personal Firewall, version 5.6.
ZoneAlarm Personal Firewall 6.5	Tests to determine whether the client is running the ZoneAlarm Personal Firewall, version 6.5.

Built-In Named Expressions (Client Security)

Expression	Definition
Norton Internet Security	Tests to determine whether the client is running any version of Norton Internet Security.

Summary Examples of Default Syntax Expressions and Policies

The following table provides examples of default syntax expressions that you can use as the basis for your own default syntax expressions.

Table 1. Examples of Default Syntax Expressions

Expression Type	Sample Expressions

Look at the method used in the HTTP request.	`http.req.method.eq(post)`
	
	`http.req.method.eq(get)`

Check the Cache-Control or Pragma header value in an HTTP request (`req`) or response (`res`).	`http.req.header("Cache-Control").contains("no-store")`
	
	`http.req.header("Cache-Control").contains("no-cache")`
	
	`http.req.header("Pragma").contains("no-cache")`
	
	`http.res.header("Cache-Control").contains("private")`
	
	`http.res.header("Cache-Control").contains("public")`
	
	`http.res.header("Cache-Control").contains("must-revalidate")`
	
	`http.res.header("Cache-Control").contains("proxy-revalidate")`
	
	`http.res.header("Cache-Control").contains("max-age")`

Check for the presence of a header in a request (`req`) or response (`res`).	`http.req.header("myHeader").exists`
	
	`http.res.header("myHeader").exists`

Look for a particular file type in an HTTP request based on the file extension.	`http.req.url.contains(".html")`
	
	`http.req.url.contains(".cgi")`
	
	`http.req.url.contains(".asp")`
	
	`http.req.url.contains(".exe")`
	
	`http.req.url.contains(".cfm")`
	
	`http.req.url.contains(".ex")`
	
	`http.req.url.contains(".shtml")`
	
	`http.req.url.contains(".htx")`
	
	`http.req.url.contains("/cgi-bin/")`
	
	`http.req.url.contains("/exec/")`
	
	`http.req.url.contains("/bin/")`

Look for anything that is other than a particular file type in an HTTP request.	`http.req.url.contains(".gif").not`
	
	`http.req.url.contains(".jpeg").not`

Check the type of file that is being sent in an HTTP response based on the Content-Type header.	`http.res.header("Content-Type").contains("text")`
	
	`http.res.header("Content-Type").contains("application/msword")`
	
	`http.res.header("Content-Type").contains("vnd.ms-excel")`
	
	`http.res.header("Content-Type").contains("application/vnd.ms-powerpoint")`
	
	`http.res.header("Content-Type").contains("text/css")`
	
	`http.res.header("Content-Type").contains("text/xml")`
	
	`http.res.header("Content-Type").contains("image/")`

Check whether this response contains an expiration header.	`http.res.header("Expires").exists`
Check for a Set-Cookie header in a response.	`http.res.header("Set-Cookie").exists`

Check the agent that sent the response.	`http.res.header("User-Agent").contains("Mozilla/4.7")`
	
	`http.res.header("User-Agent").contains("MSIE")`

Check if the first 1024 bytes of the body of a request starts with the string “some text”.	`http.req.body(1024).contains("some text")`

The following table shows examples of policy configurations and bindings for commonly used functions.

Table 2. Examples of Default Syntax Expressions and Policies

Purpose	Example

Use the rewrite feature to replace occurrences of `http:// with https://` in the body of an HTTP response.	`add rewrite action httpRewriteAction replace_all http.res.body(50000) "\"https://\"" -pattern http://`
	
	`add rewrite policy demo_rep34312 "http.res.body(50000).contains(\"http://\")" httpRewriteAction`

Replace all occurrences of “abcd” with “1234” in the first 1000 bytes of the HTTP body.	`add rewrite action abcdTo1234Action replace_all "http.req.body(1000)" "\"1234\"" -pattern abcd`
	
	`add rewrite policy abcdTo1234Policy "http.req.body(1000).contains(\"abcd\")" abcdTo1234Action`
	
	`bind rewrite global abcdTo1234Policy 100 END -type REQ_OVERRIDE`

Downgrade the HTTP version to 1.0 to prevent the server from chunking HTTP responses.	`add rewrite action downgradeTo1.0Action replace http.req.version.minor "\"0\""`
	
	`add rewrite policy downgradeTo1.0Policy "http.req.version.minor.eq(1)" downgradeTo1.0Action`
	
	`bind lb vserver myLBVserver -policyName downgradeTo1.0Policy -priority 100 -gotoPriorityExpression NEXT -type REQUEST`

Remove references to the HTTP or HTTPS protocol in all responses, so that if the user's connection is HTTP, the link is opened by using HTTP, and if the user's connection is HTTPS, the link is opened by using HTTPS.	`add rewrite action remove_http_https replace_all "http.res.body(1000000).set_text_mode(ignorecase)" "\"//\"" -pattern "re~https?://|HTTPS?://~"`
	
	`add rewrite policy remove_http_https true remove_http_https`
	
	`bind lb vserver test_vsvr -policyName remove_http_https -priority 20 -gotoPriorityExpression NEXT -type RESPONSE`

Rewrite instances of `http:// to https://` in all URLs.
 	
This policy uses the responder functionality.
	`add responder action httpToHttpsAction redirect "\"https://\" + http.req.hostname + http.req.url" -bypassSafetyCheck YES`
	
	`add responder policy httpToHttpsPolicy "!CLIENT.SSL.IS_SSL" httpToHttpsAction`
	
	`bind responder global httpToHttpsPolicy 1 END -type OVERRIDE`

Modify a URL to redirect from URL A to URL B. In this example, “file5.html” is appended to the path.
 	
This policy uses the responder functionality.
	`add responder action appendFile5Action redirect "\"http://\" + http.req.hostname + http.req.url + \"/file5.html\"" -bypassSafetyCheck YES`
	
	`add responder policy appendFile5Policy "http.req.url.eq(\"/testsite\")" appendFile5Action`
	
	`bind responder global appendFile5Policy 1 END -type OVERRIDE`

Redirect an external URL to an internal URL.	`add rewrite action act_external_to_internal REPLACE 'http.req.hostname.server' '"www.my.host.com"'`
	
	`add rewrite policy pol_external_to_internal 'http.req.hostname.server.eq("www.external.host.com")' act_external_to_internal`
	
	`bind rewrite global pol_external_to_internal 100 END -type REQ_OVERRIDE`

Redirect requests to www.example.com that have a query string to www.Web*n*.example.com. The value *n* is derived from a server parameter in the query string, for example, `server=5`.	`add rewrite action act_redirect_query REPLACE q#http.req.header("Host").before_str(".example.com")' '"Web" + http.req.url.query.value("server")#`
	
	`add rewrite policy pol_redirect_query q#http.req.header("Host").eq("www.example.com") && http.req.url.contains("?")' act_redirect_query#`

Limit the number of requests per second from a URL.	`add ns limitSelector ip_limit_selector http.req.url "client.ip.src"`
	
	`add ns limitIdentifier ip_limit_identifier -threshold 4 -timeSlice 3600 -mode request_rate -limitType smooth -selectorName ip_limit_selector`
	
	`add responder action my_Web_site_redirect_action redirect "\"http://www.mycompany.com/\""`
	
	`add responder policy ip_limit_responder_policy "http.req.url.contains(\"myasp.asp\") && sys.check_limit(\"ip_limit_identifier\")" my_Web_site_redirect_action`
	
	`bind responder global ip_limit_responder_policy 100 END -type default`

Check the client IP address but pass the request without modifying the request.	`add rewrite policy check_client_ip_policy 'HTTP.REQ.HEADER("x-forwarded-for").EXISTS || HTTP.REQ.HEADER("client-ip").EXISTS' NOREWRITE`
	
	`bind rewrite global check_client_ip_policy 100 END`

Remove old headers from a request and insert an NS-Client header.	`add rewrite action del_x_forwarded_for delete_http_header x-forwarded-for`
	
	`add rewrite action del_client_ip delete_http_header client-ip`
	
	`add rewrite policy check_x_forwarded_for_policy 'HTTP.REQ.HEADER("x-forwarded-for").EXISTS' del_x_forwarded_for`
	
	`add rewrite policy check_client_ip_policy 'HTTP.REQ.HEADER("client-ip").EXISTS' del_client_ip`
	
	`add rewrite action insert_ns_client_header insert_http_header NS-Client 'CLIENT.IP.SRC'`
	
	`add rewrite policy insert_ns_client_policy 'HTTP.REQ.HEADER("x-forwarded-for").EXISTS || HTTP.REQ.HEADER("client-ip").EXISTS' insert_ns_client_header`
	
	`bind rewrite global check_x_forwarded_for_policy 100 200`
	
	`bind rewrite global check_client_ip_policy 200 300`
	
	`bind rewrite global insert_ns_client_policy 300 END`

Remove old headers from a request, insert an NS-Client header, and then modify the “insert header” action so that the value of the inserted header contains the client IP values from the old headers and the NetScaler appliance's connection IP address.
 	
Note that this example repeats the previous example, with the exception of the final set `rewrite action`.
	`add rewrite action del_x_forwarded_for delete_http_header x-forwarded-for`
	
	`add rewrite action del_client_ip delete_http_header client-ip`
	
	`add rewrite policy check_x_forwarded_for_policy 'HTTP.REQ.HEADER("x-forwarded-for").EXISTS' del_x_forwarded_for`
	
	`add rewrite policy check_client_ip_policy 'HTTP.REQ.HEADER("client-ip").EXISTS' del_client_ip`
	
	`add rewrite action insert_ns_client_header insert_http_header NS-Client 'CLIENT.IP.SRC'`
	
	`add rewrite policy insert_ns_client_policy 'HTTP.REQ.HEADER("x-forwarded-for").EXISTS || HTTP.REQ.HEADER("client-ip").EXISTS' insert_ns_client_header`
	
	`bind rewrite global check_x_forwarded_for_policy 100 200`
	
	`bind rewrite global check_client_ip_policy 200 300`
	
	`bind rewrite global insert_ns_client_policy 300 END`
	
	`set rewrite action insert_ns_client_header -stringBuilderExpr 'HTTP.REQ.HEADER("x-forwarded-for").VALUE(0) + " " + HTTP.REQ.HEADER("client-ip").VALUE(0) + " " + CLIENT.IP.SRC' -bypassSafetyCheck YES`

Tutorial Examples of Default Syntax Policies for Rewrite

With the rewrite feature, you can modify any part of an HTTP header, and, for responses, you can modify the HTTP body. You can use this feature to accomplish a number of useful tasks, such as removing unnecessary HTTP headers, masking internal URLs, redirecting Web pages, and redirecting queries or keywords.

In the examples listed in the table of contents on the left side of your screen, you first create a rewrite action and a rewrite policy. Then you bind the policy globally.

Redirecting an External URL to an Internal URL

This example describes how to create a rewrite action and rewrite policy that redirects an external URL to an internal URL. You create an action, called act_external_to_internal, that performs the rewrite. Then you create a policy called pol_external_to_internal.

To redirect an external URL to an internal URL by using the command line interface

- To create the rewrite action, at the command prompt, type:

  add rewrite action act_external_to_internal REPLACE 'http.req.hostname.server' '"host_name_of_internal_Web_server"

- To create the rewrite policy, at the NetScaler command prompt, type:

  add rewrite policy pol_external_to_internal 'http.req.hostname.server.eq("host_name_of_external_Web_server")' act_external_to_internal

- Bind the policy globally.

To redirect an external URL to an internal URL by using the configuration utility

1. In the navigation pane, expand Rewrite, and then click Actions.
2. In the details pane, click Add.
3. In the Create Rewrite Action dialog box, enter the name act_external_to_internal.
4. To replace the HTTP server host name with the internal server name, choose Replace from the Type list box.
5. In the Header Name field, type Host.
6. In the String expression for replacement text field, type the internal host name of your Web server.
7. Click Create and then click Close.
8. In the navigation pane, click Policies.
9. In the details pane, click Add.
10. In the Name field, type pol_external_to_internal. This policy will detect connections to the Web server.
11. In the Action drop-down menu, choose the action act_external_to_internal.
12. In the Expression editor, construct the following expression:

    HTTP.REQ.HOSTNAME.SERVER.EQ("www.example.com")

13. Bind your new policy globally.

Redirecting a Query

This example describes how to create a rewrite action and rewrite policy that redirects a query to the proper URL. The example assumes that the request contains a Host header set to **`www.example.com`** and a GET method with the **`string /query.cgi?server=5`**. The redirect extracts the domain name from the host header and the number from the query string, and redirects the user's query to the server **`Web5.example.com`**, where the rest of the user's query is processed.

Note: Although the following commands appears on multiple lines, you should enter them on a single line without line breaks.

To redirect a query to the appropriate URL using the command line

- To create a rewrite action named act_redirect_query that replaces the HTTP server host name with the internal server name, type:

  add rewrite action act_redirect_query REPLACE q#http.req.header("Host").before_str(".example.com")' '"Web" + http.req.url.query.value("server")#

- To create a rewrite policy named pol_redirect_query, type the following commands at the NetScaler command prompt.. This policy detects connections, to the Web server, that contain a query string. Do not apply this policy to connections that do not contain a query string:

  add rewrite policy pol_redirect_query q#http.req.header("Host").eq("www.example.com") && http.req.url.contains("?")' act_redirect_query#

- Bind your new policy globally.

Because this rewrite policy is highly specific and should be run before any other rewrite policies, it is advisable to assign it a high priority. If you assign it a priority of 1, it will be evaluated first.

Rewriting HTTP to HTTPS

This example describes how to rewrite Web server responses to find all URLs that begin with the string “http” and replace that string with “https.” You can use this to avoid having to update Web pages after moving a server from HTTP to HTTPS.

To redirect HTTP URLs to HTTPS by using the command line interface

- To create a rewrite action named act_replace_http_with_https that replaces all instances of the string “http” with the string “https,” enter the following command:

  add rewrite action act_replace_http_with_https replace_all 'http.res.body(100)' '"https"' -pattern http

- To create a rewrite policy named pol_replace_http_with_https that detects connections to the Web server, enter the following command:

  add rewrite policy pol_replace_http_with_https TRUE act_replace_http_with_https NOREWRITE

- Bind your new policy globally.

To troubleshoot this rewrite operation, see "Case Study: Rewrite Policy for Converting HTTP Links to HTTPS not Working."

Removing Unwanted Headers

This example explains how to use a Rewrite policy to remove unwanted headers. Specifically, the example shows how to remove the following headers:

- **Accept Encoding header.** Removing the Accept Encoding header from HTTP responses prevents compression of the response.
- **Content Location header.** Removing the Content Location header from HTTP responses prevents your server from providing a hacker with information that might allow a security breach.

To delete headers from HTTP responses, you create a rewrite action and a rewrite policy, and you bind the policy globally.

To create the appropriate Rewrite action by using the command line interface

At the command prompt, type one of the following commands to either remove the Accept Encoding header and prevent response compression or remove the Content Location header:

- add rewrite action "act_remove-ae" delete_http_header "Accept-Encoding"
- add rewrite action "act_remove-cl" delete_http_header "Content-Location"

To create the appropriate Rewrite policy by using the command line interface

At the command prompt, type one of the following commands to remove either the Accept Encoding header or the Content Location header:

- add rewrite policy "pol_remove-ae" true "act_remove-ae"
- add rewrite policy "pol_remove-cl" true "act_remove-cl"

To bind the policy globally by using the command line interface

At the command prompt, type one of the following commands, as appropriate, to globally bind the policy that you have created:

- bind rewrite global pol_remove_ae 100

- bind rewrite global pol_remove_cl 200

Reducing Web Server Redirects

This example explains how to use a Rewrite policy to modify connections to your home page and other URLs that end with a forward slash (/) to the default index page for your server, preventing redirects and reducing load on your server.

To modify directory-level HTTP requests to include the default home page by using the command line

- To create a Rewrite action named action-default-homepage that modifies URLs that end in a forward slash to include the default home page index.html, type:

  add rewrite action "action-default-homepage" replace q#http.req.url.path "/" "/index.html"#

- To create a Rewrite policy named policy-default-homepage that detects connections to your home page and applies your new action, type:

  add rewrite policy "policy-default-homepage" q#http.req.url.path.EQ("/") "action-default-homepage"#

- Globally bind your new policy to put it into effect.

Masking the Server Header

This example explains how to use a Rewrite policy to mask the information in the Server header in HTTP responses from your Web server. That header contains information that hackers can use to compromise your Web site. While masking the header will not prevent a skilled hacker from finding out information about your server, it will make hacking your Web server more difficult and encourage hackers to choose less well protected targets.

To mask the Server header in responses from the command line

1. To create a Rewrite action named act_mask-server that replaces the contents of the Server header with an uninformative string, type:

   add rewrite action "act_mask-server" replace "http.RES.HEADER(\"Server\")" "\"Web Server 1.0\""

2. To create a Rewrite policy named pol_mask-server that detects all connections, type:

   add rewrite policy "pol_mask-server" true "act_mask-server"

3. Globally bind your new policy to put it into effect.

Tutorial Examples of Classic Policies

The subtopics listed in the table of contents on the left side of your screen describe useful examples of classic policy configuration for certain NetScaler features such as Access Gateway, application firewall, and SSL.

Access Gateway Policy to Check for a Valid Client Certificate

The following policies enable the NetScaler to ensure that a client presents a valid certificate before establishing a connection to a company's SSL VPN.

To check for a valid client certificate by using the command line interface

- Add an action to perform client certificate authentication.

  add ssl action act1 -clientAuth DOCLIENTAUTH

- Create an SSL policy to evaluate the client requests.

  add ssl policy pol1 -rule "REQ.HTTP.METHOD == GET" -action act1

- Add a rewrite action to insert the certificate issuer details into the HTTP header of the requests being sent to web server.

  add rewrite action act2 insert_http_header "CertDN" CLIENT.SSL.CLIENT_CERT.SUBJECT

- Create a rewrite policy to insert the certificate issuer details, if the client certificate exists.

  add rewrite policy pol2 "CLIENT.SSL.CLIENT_CERT.EXISTS" act2

  Bind these new policies to the NetScaler VIP to put them into effect.

Application Firewall Policy to Protect a Shopping Cart Application

Shopping cart applications handle sensitive customer information, for example, credit card numbers and expiration dates, and they access back-end database servers. Many shopping cart applications also use legacy CGI scripts, which can contain security flaws that were unknown at the time they were written, but are now known to hackers and identity thieves.

A shopping cart application is particularly vulnerable to the following attacks:

- **Cookie tampering.** If a shopping cart application uses cookies, and does not perform the appropriate checks on the cookies that users return to the application, an attacker could modify a cookie and gain access to the shopping cart application under another user's credentials. Once logged on as that user, the attacker could obtain sensitive private information about the legitimate user or place orders using the legitimate user’s account.

- **SQL injection.** A shopping cart application normally accesses a back-end database server. Unless the application performs the appropriate safety checks on the data users return in the form fields of its Web forms before it passes that information on to the SQL database, an attacker can use a Web form to inject unauthorized SQL commands into the database server. Attackers normally use this type of attack to obtain sensitive private information from the database or modify information in the database.

The following configuration will protect a shopping cart application against these and other attacks.

To protect a shopping cart application by using the configuration utility

1. In the navigation pane, expand Application Firewall, click Profiles, and then click Add.
2. In the Create Application Firewall Profile dialog box, in the Profile Name field, enter shopping_cart.
3. In the Profile Type drop-down list, select Web Application.
4. In the Configure Select Advanced defaults.
5. Click Create and then click Close.
6. In the details view, double-click the new profile.
7. In the Configure Web Application Profile dialog box, configure your new profile as described below:

   a. Click the Checks tab, double-click the Start URL check, and in the Modify Start URL Check dialog box, click the General tab and disable blocking, and enable learning, logging, statistics, and URL closure. Click OK and then click Close.

      Note that if you are using the command line, you configure these settings by typing the following at the prompt, and pressing ENTER:

      set appfw profile shopping_cart -startURLAction LEARN LOG STATS -startURLClosure ON

   b. For the Cookie Consistency check and Form Field Consistency checks, disable blocking, and enable learning, logging, statistics, using a similar method to the Modify Start URL Check configuration.

      If you are using the command line, you configure these settings by typing the following commands:

      set appfw profile shopping_cart -cookieConsistencyAction LEARN LOG STATS

      set appfw profile shopping_cart -fieldConsistencyAction LEARN LOG STATS

   c. For the SQL Injection check, disable blocking, and enable learning, logging, statistics, and transformation of special characters in the Modify SQL Injection Check dialog box, General tab, Check Actions section.

      If you are using the command line, you configure these settings by typing the following at the prompt, and pressing ENTER:

      set appfw profile shopping_cart -SQLInjectionAction LEARN LOG STATS -SQLInjectionTransformSpecialChars ON

d. For the Credit Card check, disable blocking; enable logging, statistics, and masking of credit card numbers; and enable protection for those credit cards you accept as forms of payment.

- If you are using the configuration utility, you configure blocking, logging, statistics, and masking (or *x-out*) in the Modify Credit Card Check dialog box, General tab, Check Actions section. You configure protection for specific credit cards in the Settings tab of the same dialog box.

- If you are using the command line, you configure these settings by typing the following at the prompt, and pressing ENTER:

set appfw profile shopping_cart -creditCardAction LOG STATS -creditCardXOut ON -creditCard <name> [<name>...]

For <name> you substitute the name of the credit card you want to protect. For Visa, you substitute VISA. For Master Card, you substitute MasterCard. For American Express, you substitute Amex. For Discover, you substitute Discover. For Diners Club, you substitute DinersClub. For JCB, you substitute JCB.

8. Create a policy named shopping_cart that detects connections to your shopping cart application and applies the shopping_cart profile to those connections.

To detect connections to the shopping cart, you examine the URL of incoming connections. If you host your shopping cart application on a separate host (a wise measure for security and other reasons), you can simply look for the presence of that host in the URL. If you host your shopping cart in a directory on a host that handles other traffic, as well, you must determine that the connection is going to the appropriate directory and/or HTML page.

The process for detecting either of these is the same; you create a policy based on the following expression, and substitute the proper host or URL for <string>.

REQ.HTTP.HEADER URL CONTAINS <string>

- If you are using the configuration utility, you navigate to the application firewall Policies page, click the Add... button to add a new policy, and follow the policy creation process described in “To create a policy with classic expressions using the configuration utility” beginning on page 201 and following.

- If you are using the command line, you type the following command at the prompt and press Enter:

  add appfw policy shopping_cart "REQ.HTTP.HEADER URL CONTAINS <string>" shopping_cart

9. Globally bind your new policy to put it into effect.

Because you want to ensure that this policy will match all connections to the shopping cart, and not be preempted by another more general policy, you should assign a high priority to it. If you assign one (1) as the priority, no other policy can preempt this one.

Application Firewall Policy to Protect Scripted Web Pages

Web pages with embedded scripts, especially legacy JavaScripts, often violate the “same origin rule,” which does not allow scripts to access or modify content on any server but the server where they are located. This security vulnerability is called *cross-site scripting*. The application firewall Cross-Site Scripting rule normally filters out requests that contain cross-site scripting.

Unfortunately, this can cause Web pages with older JavaScripts to stop functioning, even when your system administrator has checked those scripts and knows that they are safe. The example below explains how to configure the application firewall to allow cross-site scripting in Web pages from trusted sources without disabling this important filter for the rest of your Web sites.

To protect Web pages with cross-site scripting by using the command line interface

- At the command line, to create an advanced profile, type:

  add appfw profile pr_xssokay -defaults advanced

- To configure the profile, type:

  set appfw profile pr_xssokay -startURLAction NONE -startURLClosure OFF -cookieConsistencyAction LEARN LOG STATS -fieldConsistencyAction LEARN LOG STATS -crossSiteScriptingAction LEARN LOG STATS$"

- Create a policy that detects connections to your scripted Web pages and applies the pr_xssokay profile, type:

  add appfw policy pol_xssokay "REQ.HTTP.HEADER URL CONTAINS ^\.pl\?$ || REQ.HTTP.HEADER URL CONTAINS ^\.js$" pr_xssokay

- Globally bind the policy.

To protect Web pages with cross-site scripting by using the configuration utility

1. In the navigation pane, expand Application Firewall, and then click Profiles.
2. In the details view, click Add.
3. In the Create Application Firewall Profile dialog box, create a Web Application profile with advanced defaults and name it pr_xssokay. Click Create and then click Close.
4. In the details view, click the profile, click Open, and in the Configure Web Application Profile dialog box, configure the pr_xssokay profile as shown below.

   Start URL Check: Clear all actions.

   - Cookie Consistency Check: Disable blocking.
   - Form Field Consistency Check: Disable blocking.
   - Cross-Site Scripting Check: Disable blocking.

   This should prevent blocking of legitimate requests involving Web pages with cross-site scripting that you know are nonetheless safe.
5. Click Policies, and then click Add.
6. In the Create Application Firewall Policy dialog box, create a policy that detects connections to your scripted Web pages and applies the pr_xssokay profile:

   - Policy name: pol_xssokay
   - Associated profile: pr_xssokay

   Policy expression: `"REQ.HTTP.HEADER URL CONTAINS ^\.pl\?$ || REQ.HTTP.HEADER URL CONTAINS ^\.js$"`
7. Globally bind your new policy to put it into effect.

DNS Policy to Drop Packets from Specific IPs

The following example describes how to create a DNS action and DNS policy that detects connections from unwanted IPs or networks, such as those used in a DDOS attack, and drops all packets from those locations. The example shows networks within the IANA reserved IP block `192.168.0.0/16`. A hostile network will normally be on publicly routable IPs.

To drop packets from specific IPs by using the command line interface

- To create a DNS policy named pol_ddos_drop that detects connections from hostile networks and drops those packets, type:

  add dns policy pol_ddos_drop 'client.ip.src.in_subnet(192.168.253.128/25) || client.ip.src.in_subnet(192.168.254.32/27)' -drop YES'

  For the example networks in the `192.168.0.0/16` range, you substitute the IP and netmask in *###.###.###.###/##* format of each network you want to block. You can include as many networks as you want, separating each `CLIENT.IP.SRC.IN_SUBNET(###.###.###.###./##)` command with the OR operator.

- Globally bind your new policy to put it into effect.

SSL Policy to Require Valid Client Certificates

The following example shows an SSL policy that checks the user's client certificate validity before initiating an SSL connection with a client.

To block connections from users with expired client certificates

- Log on to the command line interface.

  If you are using the GUI, navigate to the SSL Policies page, then in the Data area, click the Actions tab.

- Create an SSL action named act_current_client_cert that requires that users have a current client certificate to establish an SSL connection with the NetScaler.

  add ssl action act_current_client_cert-clientAuth DOCLIENTAUTH -clientCert ENABLED -certHeader "clientCertificateHeader" -clientCertNotBefore ENABLED -certNotBeforeHeader "Mon, 01 Jan 2007 00:00:00 GMT"

- Create an SSL policy named pol_current_client_cert that detects connections to the Web server that contain a query string.

  add ssl policy pol_current_ client_cert 'REQ.SSL.CLIENT.CERT.VALIDFROM >= "Mon, 01 Jan 2007 00:00:00 GMT"' act_block_ssl

- Bind your new policy globally.

  Because this SSL policy should apply to any user’s SSL connection unless a more specific SSL policy applies, you may want to assign it a low priority. If you assign it a priority of one thousand (1000), that should ensure that other SSL policies are evaluated first, meaning that this policy will apply only to connections that do not match more specific policy criteria.

Migration of Apache mod_rewrite Rules to the Default Syntax

The Apache HTTP Server provides an engine known as mod_rewrite for rewriting HTTP request URLs. If you migrate the mod_rewrite rules from Apache to the NetScaler, you boost back-end server performance. In addition, because the NetScaler typically load balances multiple (sometimes thousands of) Web servers, after migrating the rules to the NetScaler you will have a single point of control for these rules.

The subtopic listed in the table of contents on the left side of your screen provide examples of mod_rewrite functions, and translations of these functions into Rewrite and Responder policies on the NetScaler.

Converting URL Variations into Canonical URLs

On some Web servers you can have multiple URLs for a resource. Although the canonical URLs should be used and distributed, other URLs can exist as shortcuts or internal URLs. You can make sure that users see the canonical URL regardless of the URL used to make an initial request.

In the following examples, the URL /~user is converted to /u/user.

Apache mod_rewrite solution for converting a URL

```
RewriteRule   ^/~([^/]+)/?(.*)    /u/$1/$2[R]
```

NetScaler solution for converting a URL

```
add responder action act1 redirect '"/u/"+HTTP.REQ.URL.AFTER_STR("/~")' -bypassSafetyCheck yes
add responder policy pol1 'HTTP.REQ.URL.STARTSWITH("/~") && HTTP.REQ.URL.LENGTH.GT(2)' act1
bind responder global pol1 100
```

Converting Host Name Variations to Canonical Host Names

You can enforce the use of a particular host name for reaching a site. For example, you can enforce the use of www.example.com instead of example.com.

Apache mod_rewrite solution for enforcing a particular host name for sites running on a port other than 80

```
RewriteCond %{HTTP_HOST}   !^www.example.com
RewriteCond %{HTTP_HOST}   !^$
RewriteCond %{SERVER_PORT} !^80$
RewriteRule ^/(.*)         http://www.example.com:%{SERVER_PORT}/$1 [L,R]
```

Apache mod_rewrite solution for enforcing a particular host name for sites running on port 80

```
RewriteCond %{HTTP_HOST}   !^www.example.com
RewriteCond %{HTTP_HOST}   !^$
RewriteRule ^/(.*)         http://www.example.com/$1 [L,R]
```

NetScaler solution for enforcing a particular host name for sites running on a port other than 80

```
add responder action act1 redirect '"http://www.example.com:"+CLIENT.TCP.DSTPORT+HTTP.REQ.URL' -byp
add responder policy pol1 '!HTTP.REQ.HOSTNAME.CONTAINS("www.example.com")&&!HTTP.REQ.HOSTNAME.
bind responder global pol1 100 END
```

NetScaler solution for enforcing a particular host name for sites running on port 80

```
add responder action act1 redirect '"http://www.example.com"+HTTP.REQ.URL' -bypassSafetyCheck yes
add responder policy pol1  '!HTTP.REQ.HOSTNAME.CONTAINS("www.example.com")&&!HTTP.REQ.HOSTNAME
bind responder global  pol1 100 END
```

Moving a Document Root

Usually the document root of a Web server is based on the URL “/”. However, the document root can be any directory. You can redirect traffic to the document root if it changes from the top-level “/” directory to another directory.

In the following examples, you change the document root from / to /e/www. The first two examples simply replace one string with another. The third example is more universal because, along with replacing the root directory, it preserves the rest of the URL (the path and query string), for example, redirecting /example/file.html to /e/www/example/file.html.

Apache mod_rewrite solution for moving the document root

```
RewriteEngine on
RewriteRule   ^/$  /e/www/  [R]
```

NetScaler solution for moving the document root

```
add responder action act1 redirect '"/e/www/"' -bypassSafetyCheck yes
add responder policy pol1 'HTTP.REQ.URL.EQ("/")' act1
bind responder global pol1 100
```

NetScaler solution for moving the document root and appending path information to the request

```
add responder action act1 redirect '"/e/www"+HTTP.REQ.URL' -bypassSafetyCheck yes
add responder policy pol1 '!HTTP.REQ.URL.STARTSWITH("/e/www/")' act1
bind responder global pol1 100 END
```

Moving Home Directories to a New Web Server

You may want to redirect requests that are sent to home directories on a Web server to a different Web server. For example, if a new Web server is replacing an old one over time, as you migrate home directories to the new location you need to redirect requests for the migrated home directories to the new Web server.

In the following examples, the host name for the new Web server is newserver.

Apache mod_rewrite solution for redirecting to another Web server

```
RewriteRule   ^/(.+)  http://newserver/$1     [R,L]
```

NetScaler solution for redirecting to another Web server (method 1)

```
add responder  action act1 redirect '"http://newserver"+HTTP.REQ.URL' -bypassSafetyCheck yes
add responder policy pol1 'HTTP.REQ.URL.REGEX_MATCH(re#^/(.+)#)'    act1
bind responder global pol1 100 END
```

NetScaler solution for redirecting to another Web server (method 2)

```
add responder  action act1 redirect '"http://newserver"+HTTP.REQ.URL' -bypassSafetyCheck yes
add responder policy pol1 'HTTP.REQ.URL.LENGTH.GT(1)' act1
bind responder global pol1 100 END
```

Working with Structured Home Directories

Typically, a site with thousands of users has a structured home directory layout. For example, each home directory may reside under a subdirectory that is named using the first character of the user name. For example, the home directory for jsmith (/~jsmith/anypath) might be /home/j/smith/.www/anypath, and the home directory for rvalveti (/~rvalveti/anypath) might be /home/r/rvalveti/.www/anypath.

The following examples redirect requests to the home directory.

Apache mod_rewrite solution for structured home directories

```
RewriteRule   ^/~(([a-z])[a-z0-9]+)(.*)  /home/$2/$1/.www$3
```

NetScaler solution for structured home directories

NetScaler solution for structured home directories

```
add rewrite action act1 replace 'HTTP.REQ.URL'  '"/home/"+ HTTP.REQ.URL.AFTER_STR("~").PREFIX(1)+"/"+ H
add rewrite policy pol1  'HTTP.REQ.URL.PATH.STARTSWITH("/~")' act1
bind rewrite global pol1 100
```

Redirecting Invalid URLs to Other Web Servers

If a URL is not valid, it should be redirected to another Web server. For example, you should redirect to another Web server if a file that is named in a URL does not exist on the server that is named in the URL.

On Apache, you can perform this check using mod_rewrite. On the NetScaler, an HTTP callout can check for a file on a server by running a script on the server. In the following NetScaler examples, a script named file_check.cgi processes the URL and uses this information to check for the presence of the target file on the server. The script returns TRUE or FALSE, and the NetScaler uses the value that the script returns to validate the policy.

In addition to performing the redirection, the NetScaler can add custom headers or, as in the second NetScaler example, it can add text in the response body.

Apache mod_rewrite solution for redirection if a URL is wrong

```
RewriteCond   /your/docroot/%{REQUEST_FILENAME} !-f
RewriteRule   ^(.+)      http://webserverB.com/$1 [R]
```

NetScaler solution for redirection if a URL is wrong (method 1)

```
add HTTPCallout Call
set policy httpCallout Call -IPAddress 10.102.59.101 -port 80 -hostExpr '"10.102.59.101"' -returnType BOOL -R
add responder action act1 redirect '"http://webserverB.com"+HTTP.REQ.URL' -bypassSafetyCheck yes
add responder policy pol1 '!HTTP.REQ.HEADER("Name").EXISTS  &&  !SYS.HTTP_CALLOUT(call)' act1
bind responder global pol1 100
```

NetScaler solution for redirection if a URL is wrong (method 2)

```
add HTTPCallout Call
set policy httpCallout Call -IPAddress 10.102.59.101 -port 80 -hostExpr '"10.102.59.101"' -returnType BOOL -R
add responder  action act1 respondwith  '"HTTP/1.1 302 Moved Temporarily\r\nLocation: http://webserverB.
add responder policy pol1 '!HTTP.REQ.HEADER("Name").EXISTS  &&  !SYS.HTTP_CALLOUT(call)' act1
bind responder global pol1 100
```

Rewriting a URL Based on Time

You can rewrite a URL based on the time. The following examples change a request for example.html to example.day.html or example.night.html, depending on the time of day.

Apache mod_rewrite solution for rewriting a URL based on the time

```
RewriteCond   %{TIME_HOUR}%{TIME_MIN} >0700
RewriteCond   %{TIME_HOUR}%{TIME_MIN} <1900
RewriteRule   ^example\.html$ example.day.html [L]
RewriteRule   ^example\.html$ example.night.html
```

NetScaler solution for rewriting a URL based on the time

```
add rewrite action act1 insert_before 'HTTP.REQ.URL.PATH.SUFFIX(\'.\',0)' '"day."'
add rewrite action act2  insert_before 'HTTP.REQ.URL.PATH.SUFFIX(\'.\',0)' '"night."'
add rewrite  policy pol1 'SYS.TIME.WITHIN(LOCAL 07h 00m,LOCAL 18h 59m)' act1
add rewrite policy pol2 'true'  act2
bind rewrite global pol1 101
bind rewrite global pol2 102
```

Redirecting to a New File Name (Invisible to the User)

If you rename a Web page, you can continue to support the old URL for backward compatibility while preventing users from recognizing that the page was renamed.

In the first two of the following examples, the base directory is /~quux/. The third example accommodates any base directory and the presence of query strings in the URL.

Apache mod_rewrite solution for managing a file name change in a fixed location

```
RewriteEngine  on
RewriteBase    /~quux/
RewriteRule    ^foo\.html$  bar.html
```

NetScaler solution for managing a file name change in a fixed location

```
add rewrite action act1 replace 'HTTP.REQ.URL.AFTER_STR("/~quux").SUBSTR("foo.html")' '"bar.html"'
add rewrite policy pol1 'HTTP.REQ.URL.ENDSWITH("/~quux/foo.html")' act1
bind rewrite global pol1 100
```

NetScaler solution for managing a file name change regardless of the base directory or query strings in the URL

```
add rewrite action act1 replace 'HTTP.REQ.URL.PATH.SUFFIX(\'/\',0)' '"bar.html"'
Add rewrite policy pol1 'HTTP.REQ.URL.PATH.CONTAINS("foo.html")' act1
Bind rewrite global pol1 100
```

Redirecting to New File Name (User-Visible URL)

If you rename a Web page, you may want to continue to support the old URL for backward compatibility and allow users to see that the page was renamed by changing the URL that is displayed in the browser.

In the first two of the following examples, redirection occurs when the base directory is /~quux/. The third example accommodates any base directory and the presence of query strings in the URL.

Apache mod_rewrite solution for changing the file name and the URL displayed in the browser

```
RewriteEngine on
RewriteBase    /~quux/
RewriteRule    ^old\.html$ new.html  [R]
```

NetScaler solution for changing the file name and the URL displayed in the browser

```
add responder action act1 redirect 'HTTP.REQ.URL.BEFORE_STR("foo.html")+"new.html"' -bypassSafetyCheck
add responder policy pol1 'HTTP.REQ.URL.ENDSWITH("/~quux/old.html")' act1
bind responder global pol1 100
```

NetScaler solution for changing the file name and the URL displayed in the browser regardless of the base directory or query strings in the URL

```
add responder action act1 redirect 'HTTP.REQ.URL.PATH.BEFORE_STR("old.html")+"new.html"+HTTP.REQ.URL
add responder policy pol1 'HTTP.REQ.URL.PATH.CONTAINS("old.html")' act1
bind responder global pol1 100
```

Accommodating Browser Dependent Content

To accommodate browser-specific limitations—at least for important top-level pages—it is sometimes necessary to set restrictions on the browser type and version. For example, you might want to set a maximum version for the latest Netscape variants, a minimum version for Lynx browsers, and an average feature version for all others.

The following examples act on the HTTP header "User-Agent", such that if this header begins with "Mozilla/3", the page MyPage.html is rewritten to MyPage.NS.html. If the browser is "Lynx" or "Mozilla" version 1 or 2, the URL becomes MyPage.20.html. All other browsers receive page MyPage.32.html.

Apache mod_rewrite solution for browser-specific settings

```
RewriteCond %{HTTP_USER_AGENT}  ^Mozilla/3.*
RewriteRule ^MyPage\.html$ MyPage.NS.html [L]
RewriteCond %{HTTP_USER_AGENT}  ^Lynx/.* [OR]
RewriteCond %{HTTP_USER_AGENT}  ^Mozilla/[12].*
RewriteRule ^MyPage\.html$ MyPage.20.html [L]
RewriteRule ^fMyPage\.html$ MyPage.32.html [L]
NetScaler solution for browser-specific settings
add patset pat1
bind patset pat1 Mozilla/1
bind Patset pat1 Mozilla/2
bind patset pat1 Lynx
bind Patset pat1 Mozilla/3
add rewrite action act1 insert_before 'HTTP.REQ.URL.SUFFIX' '".NS."'
add rewrite action act2 insert_before 'HTTP.REQ.URL.SUFFIX' '".20."'
add rewrite action act3 insert_before 'HTTP.REQ.URL.SUFFIX' '".32."'
add rewrite policy pol1 'HTTP.REQ.HEADER("User-Agent").STARTSWITH_INDEX("pat1").EQ(4)' act1
add rewrite policy pol2 'HTTP.REQ.HEADER("User-Agent").STARTSWITH_INDEX("pat1").BETWEEN(1,3)' act2
add rewrite policy pol3 '!HTTP.REQ.HEADER("User-Agent").STARTSWITH_ANY("pat1")' act3
bind rewrite global pol1 101 END
bind rewrite global pol2 102 END
bind rewrite global pol3 103 END
```

Blocking Access by Robots

You can block a robot from retrieving pages from a specific directory or a set of directories to ease up the traffic to and from these directories. You can restrict access based on the specific location or you can block requests based on information in User-Agent HTTP headers.

In the following examples, the Web location to be blocked is /~quux/foo/arc/, the IP addresses to be blocked are 123.45.67.8 and 123.45.67.9, and the robot's name is NameOfBadRobot.

Apache mod_rewrite solution for blocking a path and a User-Agent header

```
RewriteCond %{HTTP_USER_AGENT}   ^NameOfBadRobot.*
RewriteCond %{REMOTE_ADDR}       ^123\.45\.67\.[8-9]$
RewriteRule ^/~quux/foo/arc/.+   -   [F]
```

NetScaler solution for blocking a path and a User-Agent header

```
add responder action act1 respondwith "'HTTP/1.1 403 Forbidden\r\n\r\n'"
add responder policy pol1 'HTTP.REQ.HEADER("User_Agent").STARTSWITH("NameOfBadRobot")&&CLIENT.IP.S
bind responder global pol1 100
```

Blocking Access to Inline Images

If you find people frequently going to your server to copy inline graphics for their own use (and generating unnecessary traffic), you may want to restrict the browser's ability to send an HTTP Referer header.

In the following example, the graphics are located in http://www.quux-corp.de/~quux/.

Apache mod_rewrite solution for blocking access to an inline image

```
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://www.quux-corp.de/~quux/.*$
RewriteRule .*\.gif$ - [F]
```

NetScaler solution for blocking access to an inline image

```
add patset pat1
bind patset pat1 .gif
bind patset pat1 .jpeg
add responder action act1 respondwith "'HTTP/1.1 403 Forbidden\r\n\r\n'"
add responder policy pol1 '!HTTP.REQ.HEADER("Referer").EQ("") && !HTTP.REQ.HEADER("Referer").STARTSWI
bind responder global pol1 100
```

Creating Extensionless Links

To prevent users from knowing application or script details on the server side, you can hide file extensions from users. To do this, you may want to support extensionless links. You can achieve this behavior by using rewrite rules to add an extension to all requests, or to selectively add extensions to requests.

The first two of the following examples show adding an extension to all request URLs. In the last example, one of two file extensions is added. Note that in the last example, the mod_rewrite module can easily find the file extension because this module resides on the Web server. In contrast, the NetScaler must invoke an HTTP callout to check the extension of the requested file on the Web server. Based on the callout response, the NetScaler adds the .html or .php extension to the request URL.

Note: In the second NetScaler example, an HTTP callout is used to query a script named file_check.cgi hosted on the server. This script checks whether the argument that is provided in the callout is a valid file name.

Apache mod_rewrite solution for adding a .php extension to all requests

```
RewriteRule ^/?([a-z]+)$ $1.php [L]
```

NetScaler policy for adding a .php extension to all requests

```
add rewrite action act1 insert_after 'HTTP.REQ.URL' "".php""
add rewrite policy pol1 'HTTP.REQ.URL.PATH.REGEX_MATCH(re#^/([a-z]+)$#)' act1
bind rewrite global pol1 100
```

Apache mod_rewrite solution for adding either .html or .php extensions to requests

```
RewriteCond %{REQUEST_FILENAME}.php -f
RewriteRule ^/?([a-zA-Z0-9]+)$ $1.php [L]
RewriteCond %{REQUEST_FILENAME}.html –f
RewriteRule ^/?([a-zA-Z0-9]+)$ $1.html [L]
```

NetScaler policy for adding either .html or .php extensions to requests

```
add HTTPCallout Call_html
add HTTPCallout Call_php
set policy httpCallout Call_html -IPAddress 10.102.59.101 -port 80 -hostExpr ""10.102.59.101"" -returnType BO
set policy httpCallout Call_php -IPAddress 10.102.59.101 -port 80 -hostExpr ""10.102.59.101"" -returnType BO
add patset pat1
bind patset pat1 .html
bind patset pat1 .php
bind patset pat1 .asp
```

```
bind patset pat1 .cgi
add rewrite  action act1 insert_after 'HTTP.REQ.URL.PATH'  "".html""
add rewrite  action act2 insert_after "HTTP.REQ.URL.PATH"  "".php""
add rewrite policy pol1 '!HTTP.REQ.URL.CONTAINS_ANY("pat1") && SYS.HTTP_CALLOUT(Call_html)' act1
add rewrite policy pol2 '!HTTP.REQ.URL.CONTAINS_ANY("pat1") && SYS.HTTP_CALLOUT(Call_php)' act2
bind rewrite global pol1 100 END
bind rewrite global pol2 101 END
```

Redirecting a Working URI to a New Format

Suppose that you have a set of working URLs that resemble the following:

/index.php?id=nnnn

To change these URLs to /nnnn and make sure that search engines update their indexes to the new URI format, you need to do the following:

- Redirect the old URIs to the new ones so that search engines update their indexes.
- Rewrite the new URI back to the old one so that the index.php script runs correctly.

To accomplish this, you can insert marker code into the query string (making sure that the marker code is not seen by visitors), and then removing the marker code for the index.php script.

The following examples redirect from an old link to a new format only if a marker is not present in the query string. The link that uses the new format is re-written back to the old format, and a marker is added to the query string.

Apache mod_rewrite solution

```
RewriteCond %{QUERY_STRING} !marker
RewriteCond %{QUERY_STRING} id=([-a-zA-Z0-9_+]+)
RewriteRule ^/?index\.php$ %1? [R,L]
RewriteRule ^/?([-a-zA-Z0-9_+]+)$  index.php?marker&id=$1 [L]
NetScaler solution
add responder action act_redirect redirect 'HTTP.REQ.URL.PATH.BEFORE_STR("index.php")+HTTP.REQ.URL.C
add responder policy pol_redirect '!HTTP.REQ.URL.QUERY.CONTAINS("marker")&& HTTP.REQ.URL.QUERY.VA
bind responder global pol_redirect 100 END
add rewrite action act1 replace 'HTTP.REQ.URL.PATH.SUFFIX(\'/\',0)' '"index.phpmarker&id="+HTTP.REQ.URL
add rewrite policy pol1 '!HTTP.REQ.URL.QUERY.CONTAINS("marker")'  act1
bind rewrite global pol1 100 END
```

Ensuring That a Secure Server Is Used for Selected Pages

To make sure that only secure servers are used for selected Web pages, you can use the following Apache mod_rewrite code or NetScaler Responder policies.

Apache mod_rewrite solution

```
RewriteCond %{SERVER_PORT} !^443$
RewriteRule ^/?(page1|page2|page3|page4|page5)$  https://www.example.com/%1 [R,L]
```

NetScaler solution using regular expressions

```
add responder action res_redirect redirect  "'https://www.example.com"+HTTP.REQ.URL' -bypassSafetyChec
add responder policy pol_redirect '!CLIENT.TCP.DSTPORT.EQ(443)&&HTTP.REQ.URL.REGEX_MATCH(re/page[
bind responder global pol_redirect 100 END
```

NetScaler solution using pattern sets

```
add patset pat1
bind patset pat1 page1
bind patset pat1 page2
bind patset pat1 page3
bind patset pat1 page4
bind patset pat1 page5
add responder action res_redirect redirect  "'https://www.example.com"+HTTP.REQ.URL' -bypassSafetyChec
add responder policy pol_redirect '!CLIENT.TCP.DSTPORT.EQ(443)&&HTTP.REQ.URL.CONTAINS_ANY("pat1")'
bind responder global pol_redirect 100 END
```

Rate Limiting

The rate limiting feature enables you to define the maximum load for a given network entity or virtual entity on the Citrix NetScaler appliance. The feature enables you to configure the appliance to monitor the rate of traffic associated with the entity and take preventive action, in real time, based on the traffic rate. This feature is particularly useful when the network is under attack from a hostile client that is sending the appliance a flood of requests. You can mitigate the risks that affect the availability of resources to clients, and you can improve the reliability of the network and the resources that the appliance manages.

You can monitor and control the rate of traffic that is associated with virtual and user-defined entities, including virtual servers, URLs, domains, and combinations of URLs and domains. You can throttle the rate of traffic if it is too high, base information caching on the traffic rate, and redirect traffic to a given load balancing virtual server if the traffic rate exceeds a predefined limit. You can apply rate-based monitoring to HTTP, TCP, and DNS requests.

To monitor the rate of traffic for a given scenario, you configure a *rate limit identifier*. A rate limit identifier specifies numeric thresholds such as the maximum number of requests or connections (of a particular type) that are permitted in a specified time period called a *time slice*.

Optionally, you can configure filters, known as *stream selectors*, and associate them with rate limit identifiers when you configure the identifiers. After you configure the optional stream selector and the limit identifier, you must invoke the limit identifier from a default syntax policy. You can invoke identifiers from any feature in which the identifier may be useful, including rewrite, responder, DNS, and integrated caching.

You can globally enable and disable SNMP traps for rate limit identifiers. Each trap contains cumulative data for the rate limit identifier's configured data collection interval (time slice), unless you specified multiple traps to be generated per time slice. For more information about configuring SNMP traps and managers, see "SNMP."

Configuring a Stream Selector

A traffic stream selector is an optional filter for identifying an entity for which you want to throttle access. The selector is applied to a request or a response and selects data points (keys) that can be analyzed by a rate stream identifier. These data points can be based on almost any characteristic of the traffic, including IP addresses, subnets, domain names, TCP or UDP identifiers, and particular strings or extensions in URLs.

A stream selector consists of individual default syntax expressions called selectlets. Each selectlet is a non-compound default syntax expression. A traffic stream selector can contain up to five non-compound expressions called selectlets. Each selectlet is considered to be in an AND relationship with the other expressions. Following are some examples of selectlets:

http.req.url
http.res.body(1000>after_str(\"car_model\").before_str(\"made_in\")"
"client.ip.src.subnet(24)"

The order in which you specify parameters is significant. For example, if you configure an IP address and a domain (in that order) in one selector, and then specify the domain and the IP address (in the reverse order) in another selector, the NetScaler considers these values to be unique. This can lead to the same transaction being counted twice. Also, if multiple policies invoke the same selector, the NetScaler, again, can count the same transaction more than once.

Note: If you modify an expression in a stream selector, you may get an error if any policy that invokes it is bound to a new policy label or bind point. For example, suppose that you create a stream selector named myStreamSelector1, invoke it from myLimitID1, and invoke the identifier from a DNS policy named dnsRateLimit1. If you change the expression in myStreamSelector1, you might receive an error when binding dnsRateLimit1 to a new bind point. The workaround is to modify these expressions before creating the policies that invoke them.

To configure a traffic stream selector by using the command line interface

At the command prompt, type:

add stream selector <name> <rule> ...

Example

> add stream selector myStreamSel HTTP.REQ.URL CLIENT.IP.SRC

To configure a stream selector by using the configuration utility

Navigate to AppExpert > Rate Limiting > Selectors, click Add and specify the relevant details.

Configuring a Traffic Rate Limit Identifier

A rate limit identifier returns a Boolean TRUE if the amount of traffic exceeds a numeric limit within a particular time interval. The rate limit identifier definition can optionally include a stream selector. When you include a limit identifier in the compound default syntax expression in a policy rule, if you do not specify a stream selector, the limit identifier is applied to all the requests or responses that are identified by the compound expression.

Note: The maximum length for storing string results of selectors (for example, HTTP.REQ.URL) is 60 characters. If the string (for example, URL) is 1000 characters long, of which 50 characters are enough to uniquely identify a string, use an expression to extract only the required 50 characters.

To configure a traffic limit identifier from the command line interface

At the command prompt, type:

add ns limitIdentifier <limitIdentifier> -threshold <positive_integer> -timeSlice <positive_integer> -mode <mode> -limitType (BURSTY | SMOOTH) -selectorName <string> -maxBandwidth <positive_integer> -trapsInTimeSlice <positive_integer>

Example

Configuring traffic rate limit identifier in BURSTY mode:

```
> add ns limitIdentifier 100_request_limit -threshold 100 -timeSlice 1000 -mode REQUEST_RATE -limitType B
```

Configuring traffic rate limit identifier in SMOOTH mode:

```
> add ns limitidentifier limit_req -mode request_rate -limitType smooth -timeslice 1000 -Threshold 2000 -tra
```

To configure a traffic limit identifier by using the configuration utility

Navigate to AppExpert > Rate Limiting > Limit Identifiers, click Add and specify the relevant details.

Configuring and Binding a Traffic Rate Policy

You implement rate-based application behavior by configuring a policy in an appropriate NetScaler feature. The feature must support default syntax policies. The policy expression must contain the following expression prefix to enable the feature to analyze the traffic rate:

```
sys.check_limit(<limit_identifier>)
```

Where `limit_identifier` is the name of a limit identifier.

The policy expression must be a compound expression that contains at least two components:

- An expression that identifies traffic to which the rate limit identifier is applied. For example:

  ```
  http.req.url.contains("my_aspx.aspx").
  ```

- An expression that identifies a rate limit identifier, for example, `sys.check_limit("my_limit_identifier")`. This must be the last expression in the policy expression.

To configure a rate-based policy by using the command line interface

At the command prompt, type the following command to configure a rate-based policy and verify the configuration:

add cache|dns|rewrite|responder policy <policy_name> -rule expression && sys.check_limit("<LimitIdentifierName>") [<feature-specific information>]

Following is a complete example of a rate-based policy rule. Note that this example assumes that you have configured the responder action, send_direct_url, that is associated with the policy. Note that the sys.check_limit parameter must be the last element of the policy expression:

add responder policy responder_threshold_policy "http.req.url.contains(\"myindex.html\") && sys.check_limi

For information about binding a policy globally or to a virtual server, see "Binding Default Syntax Policies."

Rate Limiting Policy Parameters

Name

A name of up to 31 characters.

Expression

A default syntax expression that contains, at minimum, a component that identifies traffic to which the rate limit identifier should be applied and a sys.check_limit parameter.

Feature-specific information

Other required information for the policy definition, for example, actions or profiles to trigger if the policy evaluates to TRUE.

Note: You must specify sys.check_limit as the final expression element in the policy rule to ensure that the NetScaler updates the limit records only if the policy is true.

To configure a rate-based policy by using the configuration utility

1. In the navigation pane, expand the feature in which you want to configure a policy (for example, Integrated Caching, Rewrite, or Responder), and then click Policies.
2. In the details pane, click Add. In Name, enter a unique name for the policy.
3. Under Expression, enter the policy rule, and make sure that you include the `sys.check_limit` parameter as the final component of the expression. For example:

   ```
   http.req.url.contains("my_aspx.aspx") && sys.check_limit("my_limit_identifier")
   ```

4. Enter feature-specific information about the policy.

   For example, you may be required to associate the policy with an action or a profile. For more information, see the feature-specific documentation.
5. Click Create, and then click Close.
6. Click Save.

Viewing the Traffic Rate

If traffic through one or more virtual servers matches a rate-based policy, you can view the rate of this traffic. The rate statistics are maintained in the limit identifier that you named in the rule for the rate-based policy. If more than one policy uses the same limit identifier, you can view the traffic rate as defined by hits to all of the policies that use the particular limit identifier.

To view the traffic rate by using the command line interface

At the command prompt, type the following command to view the traffic rate:

show ns limitSessions <limitIdentifier>

Example

sh limitsession myLimitSession

Parameters for viewing the traffic rate

limitIdentifier

The name of the rate limit identifier. Maximum length: 31.

To view the traffic rate by using the configuration utility

1. Navigate to AppExpert > Rate Limiting > Limit Identifiers.
2. Select a limit identifier whose traffic rate you want to view.
3. Click the Show Sessions button. If traffic through one or more virtual servers has matched a rate limiting policy that uses this limit identifier (and the hits are within the configured time slice for this identifier), the Session Details dialog box appears. Otherwise, you receive a "`No session exists`" message.

Testing a Rate-Based Policy

To test a rate-based policy, you can send traffic to any virtual server to which a rate-based policy is bound.

Task overview: Testing a rate-based policy

1. Configure a stream selector (optional) and a rate limit identifier (required). For example:

   ```
   add stream selector sel_subnet Q.URL "CLIENT.IP.SRC.SUBNET(24)"
   add ns limitIdentifier k_subnet -Threshold 4 -timeSlice 3600 -mode REQUEST_RATE  -limittype smooth  -s
   ```

2. Configure the action that you want to associate with the policy that uses the rate limit identifier. For example:

   ```
   add responder action resp_redirect redirect "\"http://response_site.com/\""
   ```

3. Configure a policy that uses the sys.check_limit expression prefix to call the rate limit identifier. For example, the policy can apply a rate limit identifier to all requests arriving from a particular subnet, as follows:

   ```
   add responder policy resp_subnet "SYS.CHECK_LIMIT(\"k_subnet\")" resp_redirect
   ```

4. Bind the policy globally or to a virtual server. For example:

   ```
   bind responder global resp_subnet 6 END -type DEFAULT
   ```

5. In a browser address bar, send a test HTTP query to a virtual server. For example:

   ```
   http://<IP of a vserver>/testsite/test.txt
   ```

6. At the NetScaler command prompt, type:

   ```
   show ns limitSessions <limitIdentifier>
   ```

   Example

   ```
   > sh limitsession k_subnet
   1)      Time Remaining:       98 secs  Hits: 2                    Action Taken: 0
          Total Hash:    1718618  Hash String: /test.txt
          IPs gathered:
                 1) 10.217.253.0
          Active Transactions: 0
    Done
   >
   ```

7. Repeat the query and check the limit identifier statistics again to verify that the statistics are being updated correctly.

Examples of Rate-Based Policies

The following table shows examples of rate-based policies.

Table 1. Examples of Rate-Based Policies

Purpose	Example
Limit the number of requests per second from a URL	add stream selector ipStreamSelector http.req.url "client.ip.src" add ns limitIdentifier ipLimitIdentifier -threshold 4 -timeSlice 1000 -mode request_rate -limitType smooth -selectorName ipStreamSelecto add responder action myWebSiteRedirectAction redirect "\"http://www.mycompany.com/\"" add responder policy ipLimitResponderPolicy "http.req.url.contains(\"m && sys.check_limit(\"ipLimitIdentifier\")" myWebSiteRedirectAction bind responder global ipLimitResponderPolicy 100 END -type default
Cache a response if the request URL rate exceeds 5 per 20000 milliseconds	add stream selector cacheStreamSelector http.req.url add ns limitidentifier cacheRateLimitIdentifier -threshold 5 -timeSlice 2 -selectorName cacheStreamSelector add cache policy cacheRateLimitPolicy -rule "http.req.method.eq(get) && sys.check_limit(\"cacheRateLimitIdentifier\")" -action cache bind cache global cacheRateLimitPolicy -priority 10
Drop a connection on the basis of cookies received in requests from www.yourcompany.com if the requests exceed the rate limit	add stream selector reqCookieStreamSelector "http.req.cookie .value(\"mycookie\")" "client.ip.src.subnet(24)" add ns limitIdentifier myLimitIdentifier -Threshold 2 -timeSlice 3000 -selectorName reqCookieStreamSelector add responder action sendRedirectUrl redirect '\"http://www.mycompa + http.req.url' -bypassSafetyCheck YES add responder policy rateLimitCookiePolicy "http.req.url.contains(\"www.yourcompany.com\") && sys.check_limit(\"myLimitIdentifier\")" sendRedirectUrl

Drop a DNS packet if the requests from a particular client IP address and DNS domain exceed the rate limit	add stream selector dropDNSStreamSelector client.udp.dns.domain clie add ns limitIdentifier dropDNSRateIdentifier -timeslice 20000 -mode req -selectorName dropDNSStreamSelector -maxBandwidth 1 -trapsintimesl add dns policy dnsDropOnClientRatePolicy "sys.check_limit (\"dropDNSRateIdentifier\")" -drop yes
Limit the number of HTTP requests that arrive from the same subnet (with a subnet mask of 32) and that have the same destination IP address.	add stream selector ipv6_sel "CLIENT.IPv6.src.subnet(32)" CLIENT.IPv6.d add ns limitIdentifier ipv6_id -imeSlice 20000 -selectorName ipv6_sel add lb vserver ipv6_vip HTTP 3ffe::209 80 -persistenceType NONE -cltTi add responder action redirect_page redirect "\"http://redirectpage.com add responder policy ipv6_resp_pol "SYS.CHECK_LIMIT(\"ipv6_id\")" redir bind responder global ipv6_resp_pol 5 END -type DEFAULT

Sample Use Cases for Rate-Based Policies

The following scenarios describe two uses of rate-based policies in global server load balancing (GSLB):

- The first scenario describes the use of a rate-based policy that sends traffic to a new data center if the rate of DNS requests exceed 1000 per second.
- In the second scenario, if more than five DNS requests arrive for a local DNS (LDNS) client within a particular period, the additional requests are dropped.

Redirecting Traffic on the Basis of Traffic Rate

In this scenario, you configure a proximity-based load balancing method, and a rate-limiting policy that identifies DNS requests for a particular region. In the rate-limiting policy, you specify a threshold of 1000 DNS requests per second. A DNS policy applies the rate limiting policy to DNS requests for the region "Europe.GB.17.London.UK-East.ISP-UK." In the DNS policy, DNS requests that exceed the rate limiting threshold, starting with request 1001 and continuing to the end of the one-second interval, are to be forwarded to the IP addresses that are associated with the region "North America.US.TX.Dallas.US-East.ISP-US."

The following configuration demonstrates this scenario:

```
add stream selector DNSSelector1 client.udp.dns.domain
add ns limitIdentifier DNSLimitIdentifier1 -threshold 5 -timeSlice 1000 -selectorName DNSSelector1
add dns policy DNSLimitPolicy1 "client.ip.src.matches_location(\"Europe.GB.17.London.*.*\") &&
sys.check_limit(\"DNSLimitIdentifier1\")" -preferredLocation "North America.US.TX.Dallas.*.*"
bind dns global DNSLimitPolicy1 5
```

Dropping DNS Requests on the Basis of Traffic Rate

In the following example of global server load balancing, you configure a rate limiting policy that permits a maximum of five DNS requests in a particular interval, per domain, to be directed to an LDNS client for resolution. Any requests that exceed this rate are dropped. This type of policy can help protect the NetScaler from resource exploitation. For example, in this scenario, if the time to live (TTL) for a connection is five seconds, this policy prevents the LDNS from requerying a domain. Instead, it uses data that is cached on the NetScaler.

```
add stream selector LDNSSelector1 client.udp.dns.domain client.ip.src
add ns limitIdentifier LDNSLimitIdentifier1 -threshold 5 -timeSlice 1000 -selectorName LDNSSelector1
add dns policy LDNSPolicy1 "client.udp.dns.domain.contains(\".\") && sys.check_limit(\"LDNSLimitIdentifier1\
```

```
bind dns global LDNSPolicy1 6
show gslb vserver gvip
gvip - HTTP     State: UP
Last state change was at Mon Sep  8 11:50:48 2008 (+711 ms)
Time since last state change: 1 days, 02:55:08.830
Configured Method: STATICPROXIMITY
BackupMethod: ROUNDROBIN
No. of Bound Services :  3 (Total)       3 (Active)
Persistence: NONE       Persistence ID: 100
Disable Primary Vserver on Down: DISABLED       Site Persistence: NONE
Backup Session Timeout: 0
Empty Down Response: DISABLED
Multi IP Response: DISABLED Dynamic Weights: DISABLED
Cname Flag: DISABLED
Effective State Considered: NONE
1)      site11_svc(10.100.00.00: 80)- HTTP State: UP    Weight: 1
Dynamic Weight: 0       Cumulative Weight: 1
Effective State: UP
Threshold : BELOW
Location: Europe.GB.17.London.UK-East.ISP-UK
2)      site12_svc(10.101.00.100: 80)- HTTP State: UP   Weight: 1
Dynamic Weight: 0       Cumulative Weight: 1
Effective State: UP
Threshold : BELOW
Location: North America.US.TX.Dallas.US-East.ISP-US
3)      site13_svc(10.102.00.200: 80)- HTTP State: UP   Weight: 1
Dynamic Weight: 0       Cumulative Weight: 1
Effective State: UP
Threshold : BELOW
Location: North America.US.NJ.Salem.US-Mid.ISP-US
1)      www.gslbindia.com        TTL: 5 secn
Cookie Timeout: 0 min   Site domain TTL: 3600 sec
Done
```

Responder

Today's complex Web configurations often require different responses to HTTP requests that appear, on the surface, to be similar. When users request a Web site's home page, you may want to provide a different home page depending on where each user is located, which browser the user is using, or which language(s) the browser accepts and the order of preference. You might want to break the connection immediately if the request is coming from an IP range that has been generating DDoS attacks or initiating hacking attempts.

With the Responder feature, responses can be based on who sends the request, where it is sent from, and other criteria with security and system management implications. The feature is simple and quick to use. By avoiding the invocation of more complex features, it reduces CPU cycles and time spent in handling requests that do not require complex processing.

For handling sensitive data such as financial information, if you want to ensure that the client uses a secure connection to browse a site, you can redirect the request to secure connection by using https:// instead of http://.

To use the Responder feature, do the following;

- Enable the Responder feature on the NetScaler.
- Configure responder actions. The action can be to generate a custom response, redirect a request to a different Web page, or reset a connection.
- Configure responder policies. The policy determines the requests (traffic) on which an action has to be taken.
- Bind each policy to a bind point put it into effect. A bind point refers to an entity at which NetScaler examines the traffic to see if it matches a policy. For example, a bind point can be a load balancing virtual server.

You can specify a default action for requests that do not match any policy, and you can bypass the safety check for actions that would otherwise generate error messages.

The Rewrite feature of NetScaler helps in rewriting some information in the requests or responses handled by NetScaler. The following section shows some differences between the two features.

Comparison between Rewrite and Responder options

The main difference between the rewrite feature and the responder feature is as follows:

Responder cannot be used for response or server-based expressions. Responder can be used only for the following scenarios depending on client parameters:

- Redirecting a http request to new Web sites or Web pages
- Responding with some custom response

- Dropping or resetting a connection at request level

In case of a responder policy, the NetScaler examines the request from the client, takes action according to the applicable policies, sends the response to the client, and closes the connection with the client.

In case of a rewrite policy, the NetScaler examines the request from the client or response from the server, takes action according to the applicable policies, and forwards the traffic to the client or the server.

In general, it is recommended to use responder if you want the NetScaler to reset or drop a connection based on a client or request-based parameter. Use responder to redirect traffic, or respond with custom messages. Use rewrite for manipulating data on HTTP requests and responses.

Enabling the Responder Feature

To use the Responder feature, you must first enable it.

To enable the responder feature by using the command line interface

At the command prompt, type the following commands to enable the responder feature and verify the configuration:

- enable ns feature<feature>
- show ns feature

Example

```
enable ns feature Responder
 Done
> show ns feature

      Feature                 Acronym           Status
      -------                 -------           ------
 1)   Web Logging               WL                ON
 2)   Surge Protection          SP                ON
.
.
.
 22)  Responder                 RESPONDER         ON
 23)  HTML Injection            HTMLInjection     ON
 24)  NetScaler Push            push              OFF
Done
>
```

To enable the responder feature by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features, click Change advanced features.
3. In the Configure Advanced Features dialog box, select the Responder check box, and then click OK.
4. In the Enable/Disable Feature(s)? dialog box, click YES. A message appears in the status bar, stating that the feature has been enabled.

Configuring a Responder Action

After enabling the responder feature, you must configure one or more actions for handling requests. The responder supports the following types of actions:

Respond with

Sends the response defined by the Target expression without forwarding the request to a web server. (The NetScaler appliance substitutes for and acts as a web server.) Use this type of action to manually define a simple HTML-based response. Normally the text for a Respond with action consists of a web server error code and brief HTML page.

Respond with SQL OK

Sends the designated SQL OK response defined by the Target expression. Use this type of action to send an SQL OK response to an SQL query.

Respond with SQL Error

Sends the designated SQL Error response defined by the Target expression. Use this type of action to send an SQL Error response to an SQL query.

Respond with HTML page

Sends the designated HTML page as the response. You can choose from a drop-down list of HTML pages that were previously uploaded, or upload a new HTML page. Use this type of action to send an imported HTML page as the response.

Redirect

Redirects the request to a different web page or web server. A Redirect action can redirect requests originally sent to a "dummy" web site that exists in DNS, but for which there is no actual web server, to an actual web site. It can also redirect search requests to an appropriate URL. Normally, the redirection target for a Redirect action consists of a complete URL.

To configure a responder action by using the command line interface

At the command prompt, type the following commands to configure a responder action and verify the configuration:

- add responder action <name> <type> <target> [-bypassSafetyCheck (YES | NO)]
- show responder action

Example

To create a responder action that displays a “Not Found” error page for URLs that do not exist:

```
add responder action act404Error respondWith "'HTTP/1.1 404 Not Found\r\n\r\n"+ "HTTP.REQ.URL.HTTP_URL
 Done
> show responder action

1)      Name: act404Error
        Operation: respondwith
        Target: "HTTP/1.1 404 Not Found

"+ "HTTP.REQ.URL.HTTP_URL_SAFE" + "does not exist on the web server."
        BypassSafetyCheck : NO
        Hits: 0
        Undef Hits: 0
        Action Reference Count: 0
 Done
```

To create a responder action that displays a “Not Found” error page for URLs that do not exist:

```
add responder action act404Error respondWith "'HTTP/1.1 404 Not Found\r\n\r\n"+ "HTTP.REQ.URL.HTTP_URL
 Done
> show responder action

1)      Name: act404Error
        Operation: respondwith
        Target: "HTTP/1.1 404 Not Found

"+ "HTTP.REQ.URL.HTTP_URL_SAFE" + "does not exist on the web server."
        BypassSafetyCheck : NO
        Hits: 0
        Undef Hits: 0
        Action Reference Count: 0
 Done
```

To modify an existing responder action by using the command line interface

At the command prompt, type the following command to modify an existing responder action and verify the configuration:

- set responder action <name> -target <string> [-bypassSafetyCheck (YES | NO)]
- show responder action

Example

```
set responder action act404Error  -target '"HTTP/1.1 404 Not Found\r\n\r\n"+ "HTTP.REQ.URL.HTTP_URL_SAF
 Done
> show responder action

1)      Name: act404Error
        Operation: respondwith
        Target: "HTTP/1.1 404 Not Found

"+ "HTTP.REQ.URL.HTTP_URL_SAFE" + "does not exist on the web server."
        BypassSafetyCheck : NO
        Hits: 0
        Undef Hits: 0
        Action Reference Count: 0
 Done
```

To remove a responder action by using the command line interface

At the command prompt, type the following command to remove a responder action and verify the configuration:

- rm responder action <name>
- show responder action

Example

```
rm responder action act404Error
 Done

> show responder action
 Done
```

Parameters for configuring a responder action

name

A name for your new action, or the name of the existing action that you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols.

type

The type of responder action. Possible values:

- *respondWith*: Sends the response specified in the target expression.
- *sqlresponse_ok*: Sends an SQL OK response as specified in the target expression.

- *sqlresponse_error*: Sends an SQL Error response as specified in the target expression.
- *respondwithhtmlpage*: Sends the uploaded HTML page specified as the target.
- *redirect*: Redirects the request to the URL specified as the target expression.

target

The HTTP or SQL string to be sent as a response, the name of the uploaded HTML page to be sent as a response, or the URL to which the request is redirected. For `respondWith`, `sqlresponse_ok`, and `sqlresponse_error` response types, the target must consist of one or more strings enclosed in straight double quotes, with the entire response enclosed in straight single quotes. Within a response, type a plus sign (+) between separate double-quoted strings. Type \r\n to begin a new line.

bypassSafetyCheck

Bypass the appliance's built-in safety checks when adding or modifying this action. Possible values: YES, NO

To configure a responder action by using the configuration utility

1. Navigate to AppExpert > Responder > Actions.
2. In the details pane, do one of the following:
   - To create a new action, click Add.
   - To modify an existing action, select the action, and then click Open.
3. In the Add Responder Action or Configure Responder Action dialog box, type or select values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring a responder action" as follows (asterisk indicates a required parameter):
   - Name*—name (Cannot be changed for a previously configured action)
   - Type*—type
   - Target*—target
   - Bypass Safety Check—byPassSafetyCheck

   If you want help creating the target for a new action, while the cursor is in the Target text box you can either hold down the Control key and press the space bar, or you can use the Add Expression dialog box as described in “To add an expression by using the Add Expression dialog box” below.
4. Click Create or OK, depending on whether you are creating a new action or modifying an existing action.
5. Click Close. A message appears in the status bar, stating that the feature has been enabled.
6. To delete a responder action, select the action, and then click Remove. A message appears in the status bar, stating that the feature has been disabled.

To add an expression by using the Add Expression dialog box

1. In the Create Responder Action or Configure Responder Action dialog box, click Add.
2. In the Add Expression dialog box, in the first list box choose the first term for your expression.

   HTTP

   The HTTP protocol. Choose this if you want to examine some aspect of the request that pertains to the HTTP protocol.

   SYS

   The protected web site(s). Choose this if you want to examine some aspect of the request that pertains to the recipient of the request.

   CLIENT

   The computer that sent the request. Choose this if you want to examine some aspect of the sender of the request.

   ANALYTICS

   The analytics data associated with the request. Choose this if you want to examine request metadata.

   SIP

   A SIP request. Choose this if you want to examine some aspect of a SIP request.

   When you make your choice, the rightmost list box lists appropriate terms for the next part of your expression.
3. In the second list box, choose the second term for your expression. The choices depend upon which choice you made in the previous step, and are appropriate to the context. After you make your second choice, the Help window below the Construct Expression window (which was blank) displays help describing the purpose and use of the term you just chose.
4. Continue choosing terms from the list boxes that appear to the right of the previous list box, or typing strings or numbers in the text boxes that appear to prompt you to enter a value, until your expression is finished.

Configuring the Global HTTP Action

You can configure the global HTTP action to invoke a responder action when an HTTP request times out. To configure this feature, you must first create the responder action that you want to invoke. Then, you configure the global HTTP timeout action to respond to a timeout with that responder action.

To configure the global HTTP action by using the command line interface

At the command prompt, type the following command:

- set ns httpProfile -reqTimeoutAction <responder action name>
- save ns config

For <responder action name>, substitute the name of the responder action.

Configuring a Responder Policy

After you configure a responder action, you must next configure a responder policy to select the requests to which the NetScaler appliance should respond. A responder policy is based on a rule, which consists of one or more expressions. The rule is associated with an action, which is performed if a request matches the rule.

Note: For creating and managing responder policies, the configuration utility provides assistance that is not available at the NetScaler command prompt.

To configure a responder policy by using the command line interface

At the command prompt, type the following command to add a new responder policy and verify the configuration:

- add responder policy <name> <expression> <action> [<undefaction>]-appFlowaction<actionName>
- show responder policy <name>

Example

```
> add responder policy policyThree "CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)" RESET
 Done
> show responder policy policyThree

      Name: policyThree
      Rule: CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)
      Responder Action: RESET
      UndefAction: Use Global
      Hits: 0
      Undef Hits: 0
 Done
```

To modify an existing responder policy by using the command line interface

At the command prompt, type the following command to modify an existing responder policy and verify the configuration:

- set responder policy <name> [-rule <expression>] [-action <string>] [-undefAction <string>]

- show responder policy <name>

To remove a responder policy by using the command line interface

At the command prompt, type the following command to remove a responder policy and verify the configuration:

- rm responder policy <name>
- show responder policy

Example

```
>rm responder policy pol404Error
 Done

> show responder policy
 Done
```

Parameters for configuring a responder policy

name

A name for the policy, or the name of the existing policy you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should choose a name that will make it easy for others to tell what type of request this policy was configured to match.

rule

The expression that defines the rule for this policy. The expression can be a simple expression or a complex expression that contains several expressions in structured relationship to one another. Expressions are written in the NetScaler Policy Infrastructure (PI) language. For more information about PI, see "AppExpert."

action

The name of the responder action associated with the policy. You can choose either the built-in ‘NOOP’ or ‘RESET’ actions, or a responder action you have configured.

appFlowaction

The name of the AppFlow action that sends the web-page performance data to the collectors in which you want to collect the web-page performance data.

undefaction

The action to use if the policy generates an UNDEF event. You can select either the NOOP, RESET, or DROP action, or configure the NetScaler appliance use the configured global undefined action.

Any responder-specific undefined action you configure will override the global undefined action.

To configure a responder policy by using the configuration utility

1. Navigate to Responder > Policies.
2. In the details pane, do one of the following:
   - To create a new policy, click Add.
   - To modify an existing policy, select the policy, and then click Open.
3. In the Create Responder Policy or Configure Responder Policy dialog box, type or select values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring a responder policy" as follows (asterisk indicates a required parameter):
   - Name*—name (Cannot be changed for a previously configured policy.)
   - Action*—action
   - Expression*—expression
   - Undefined-Result Action—undefaction
   - AppFlow Action—actionName

   If you want help creating an expression for a new policy, while your cursor is in the Expression text box you can either hold down the Control key and press the space bar, or you can use the Add Expression dialog box as described in “To add an expression by using the Add Expression dialog box.”
4. Click Create or OK, depending on whether you are creating a new policy or modifying an existing policy.
5. Click Close. A message appears in the status bar, stating that the feature has been configured.

Binding a Responder Policy

To put a policy into effect, you must bind it either globally, so that it applies to all traffic that flows through the NetScaler, or to a specific virtual server, so that the policy applies only to requests whose destination IP address is the VIP of that virtual server.

When you bind a policy, you assign a priority to it. The priority determines the order in which the policies you define are evaluated. You can set the priority to any positive integer.

In the NetScaler operating system, policy priorities work in reverse order—the higher the number, the lower the priority. For example, if you have three policies with priorities of 10, 100, and 1000, the policy assigned a priority of 10 is performed first, then the policy assigned a priority of 100, and finally the policy assigned an order of 1000. The responder feature implements only the first policy that a request matches, not any additional policies that it might also match, so policy priority is important for getting the results you intend.

You can leave yourself plenty of room to add other policies in any order, and still set them to evaluate in the order you want, by setting priorities with intervals of 50 or 100 between each policy when you globally bind it. You can then add additional policies at any time without having to reassign the priority of an existing policy.

For additional information about binding policies on the NetScaler, see "Policies and Expressions."

Note: Responder policies cannot be bound to TCP-based virtual servers.

To globally bind a responder policy by using the command line interface

At the command prompt, type the following command to globally bind a responder policy and verify the configuration:

- bind responder global <policyName> <priority> [<gotoPriorityExpression [-type <type>] [-invoke (<labelType> <labelName>)]
- show responder global

Example

```
> bind responder global poliError 100
 Done
> show responder global
1)      Global bindpoint: REQ_DEFAULT
        Number of bound policies: 1

 Done
```

To bind responder policy to a specific virtual server by using the command line interface

At the command prompt, type the following command to bind responder policy to a specific virtual server and verify the configuration:

bind lb vserver <name> -policyname <policy_name> -priority <priority>

Example

```
> bind lb vserver vs-loadbal -policyName policyTwo -priority 100
 Done
> show lb vserver
1)      vs-loadbal (10.102.29.20:80) - HTTP      Type: ADDRESS
        State: OUT OF SERVICE
        Last state change was at Wed Aug 19 09:05:47 2009 (+211 ms)
        Time since last state change: 2 days, 00:58:03.260
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none
2)      vs-cont-sw (0.0.0.0:0) - TCP     Type: ADDRESS
        State: DOWN
        Last state change was at Wed Aug 19 10:03:46 2009 (+213 ms)
        Time since last state change: 2 days, 00:00:04.260
        Effective State: DOWN
        Client Idle Timeout: 9000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Connection Failover: DISABLED
 Done
```

Parameters for binding a responder policy

name

The name of the virtual server to which you want to bind this policy.

policyname

The name of the responder policy you want to bind.

priority

The priority assigned to this responder policy.

type

Bindpoint, specifying where to bind the policy.

invoke

Invoke flag.

labelType

Type of policy label invocation.

labelName

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

To globally bind a responder policy by using the configuration utility

1. Navigate to Responder > Policies.
2. On the Responder Policies page, select a responder policy, and then click Policy Manager.
3. In the Responder Policy Manager dialog box Bind Points menu, select Default Global.
4. Click Insert Policy to insert a new row and display a drop-down list of all unbound responder policies.
5. Click one of the policies on the list. That policy is inserted into the list of globally bound responder policies.
6. Click Apply Changes.
7. Click Close. A message appears in the status bar, stating that the configuration has been successfully completed.

To bind a responder policy to a specific virtual server by using the configuration utility

1. Navigate to Load Balancing > Virtual Servers.
2. On the Load Balancing Virtual Servers page, select the virtual server to which you want to bind the responder policy, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, select the Policies tab, which displays a list of all policies configured on your NetScaler appliance.
4. Select the check box next to the name of the policy you want to bind to this virtual server.
5. Click OK. A message appears in the status bar, stating that the configuration has been successfully completed.

Setting the Responder Default Action

The NetScaler appliance generates an undefined event (UNDEF event) when a request does not match a responder policy, and then carries out the default action assigned to undefined events. By default, that action is to forward the request to the next feature without changing it. This default behavior is normally what you want; it ensures that requests that do not require special handling by a specific responder action are sent to your Web servers and clients receive access to the content that they requested.

If the Web site(s) your NetScaler appliance protects receive a significant number of invalid or malicious requests, however, you may want to change the default action to either reset the client connection or drop the request. In this type of configuration, you would write one or more responder policies that would match any legitimate requests, and simply redirect those requests to their original destinations. Your NetScaler appliance would then block any other requests as specified by the default action you configured.

You can assign any one of the following actions to an undefined event:

NOOP

The NOOP action aborts responder processing but does not alter the packet flow. This means that the appliance continues to process requests that do not match any responder policy, and eventually forwards them to the requested URL unless another feature intervenes and blocks or redirects the request. This action is appropriate for normal requests to your Web servers and is the default setting.

RESET

If the undefined action is set to RESET, the appliance resets the client connection, informing the client that it must re-establish its session with the Web server. This action is appropriate for repeat requests for Web pages that do not exist, or for connections that might be attempts to hack or probe your protected Web site(s).

DROP

If the undefined action is set to DROP, the appliance silently drops the request without responding to the client in any way. This action is appropriate for requests that appear to be part of a DDoS attack or other sustained attack on your servers.

Note: UNDEF events are triggered only for client requests. No UNDEF events are triggered for responses.

To set the undefined action by using the command line interface

At the command prompt, type the following command to set the undefined action and verify the configuration:

- set responder param -undefAction (RESET|DROP|NOOP)

- show responder param

Example

```
>set responder param -undefAction RESET
 Done
> show responder param
       Action Name: RESET
 Done
>
```

To set the undefined action by using the configuration utility

1. In the navigation pane, expand Responder, and then under Settings, click the Change Responder Settings link.
2. In the Set Responder Params dialog box, under Global Undefined-Result Action, select NOOP, RESET, or DROP.
3. Click OK. A message appears in the status bar, stating that the Responder Parameters have been configured.

Responder Action and Policy Examples

Responder actions and policies are powerful and complex, but you can get started with relatively simple applications. For typical examples, see "Example: Blocking Access from Specified IPs" and "Example: Redirecting a Client to a new URL."

Example: Blocking Access from Specified IPs

The following procedures block access to your protected Web site(s) by clients originating from the CIDR 222.222.0.0/16. The responder sends an error message stating that the client is not authorized to access the URL requested.

To block access by using the command line interface

At the command prompt, type the following commands to block access:

- add responder action act_unauthorized respondwith '"HTTP/1.1 200 OK\r\n\r\n" + "Client: " + CLIENT.IP.SRC + " is not authorized to access URL:" + "HTTP.REQ.URL.HTTP_URL_SAFE"'
- add responder policy pol_un "CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)" act_unauthorized
- bind responder global pol_un 10

To block access by using the configuration utility

1. In the navigation pane, expand Responder, and then click Actions.
2. In the details pane, click Add.
3. In the Create Responder Action dialog box, do the following:
   a. In the Name text box, type `act_unauthorized`.
   b. Under Type, select Respond with.
   c. In the Target text area, type the following string:
   ```
   "HTTP/1.1 200 OK\r\n\r\n"
   + "Client: " + CLIENT.IP.SRC + " is not authorized to access
   URL:" + HTTP.REQ.URL.HTTP_URL_SAFE
   ```
   d. Click Create, and then click Close.
   The responder action you configured, named `act_unauthorized`, now appears in the Responder Actions page.
4. In the navigation pane, click Policies.
5. In the details pane, click Add.
6. In the Create Responder Policy dialog box, do the following:
   a. In the Name text box, type `pol_unauthorized`.
   b. Under Action, select act_unauthorized.
   c. In the Expression window, type the following rule:
   `CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)`
   d. Click Create, then click Close.
   The responder policy you configured, named pol_unauthorized, now appears in the Responder Policies page.
7. Globally bind your new policy, `pol_unauthorized`, as described in "Binding a Responder Policy."

Example: Redirecting a Client to a new URL

The following procedures redirect clients who access your protected Web site(s) from within the CIDR 222.222.0.0/16 to a specified URL.

To redirect clients by using the command line interface

At the command prompt, type the following commands to redirect clients and verify the configuration:

- add responder action act_redirect redirect '"http://www.example.com/404.html"'
- show responder action act_redirect

- add responder policy pol_redirect "CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)" act_redirect
- show responder policy pol_redirect
- bind responder global pol_redirect 10

Example

> add responder action act_redirect redirect '" http ://www.example.com/404.html '"

> add responder policy pol_redirect "CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)" act_redirect

To redirect clients by using the configuration utility

1. Navigate to Responder > Actions.
2. In the details pane, click Add.
3. In the Create Responder Action dialog box, do the following:
   a. In the Name text box, type `act_redirect`.
   b. Under Type, select Redirect.
   c. In the Target text area, type the following string:
      `"http://www.example.com/404.html"`
   d. Click Create, then click Close.

   The responder action you configured, named act_redirect, now appears in the Responder Actions page.
4. In the navigation pane, click Policies.
5. In the details pane, click Add.
6. In the Create Responder Policy dialog box, do the following:
   a. In the Name text box, type `pol_redirect`.
   b. Under Action, select act_redirect.
   c. In the Expression window, type the following rule:
      `CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)`
   d. Click Create, then click Close.

   The responder policy you configured, named pol_redirect, now appears in the Responder Policies page.
7. Globally bind your new policy, pol_redirect, as described in "Binding a Responder Policy."

Diameter Support for Responder

The Responder feature now supports the Diameter protocol. You can configure Responder to respond to Diameter requests as it does HTTP and TCP requests. For example, you could configure Responder to respond to requests from a specific Diameter origin with a redirect to a web page enhanced for mobile devices. A number of NetScaler expressions have been added that support examination of the Diameter header and the attribute-value pairs (AVPs). These expressions support lookup of specific AVPs by index, ID or name, examine the information in each AVP, and send an appropriate response.

To configure Responder to respond to a Diameter request

To configure the Responder feature to send a response to a diameter request, at the command prompt, type the following commands:

- add responder action <actname> RESPONDWITH "DIAMETER.NEW_REDIRECT(\"aaa://host.example.com\")"
  For <actname>, substitute a name for your new action. The name can consist of from one to 127 characters in length, and can contain letters, numbers, and the hyphen (-) and underscore (_) symbols. For aaa://host.example.com, substitute the URL of the diameter host to which you want to redirect connections.

- add responder policy <polname> "diameter.req.avp(264).value.eq(\"host1.example.net\")" <actname>
  For <polname>, substitute a name for your new policy. As with <actname>, the name can consist of from one to 127 characters in length, and can contain letters, numbers, and the hyphen (-) and underscore (_) symbols. For host1.example.net, substitute the name of the originating host of the requests that you want to redirect. For <actname>, substitute the name of the action that you just created.

- bind lb vserver <vservername> -policyName <polname> -priority <priority> -type REQUEST
  For <vservername>, substitute the name of the load balancing virtual server to which you want to bind the policy. For <polname>, substitute the name of the policy you just created. For <priority>, substitute a priority for the policy.

Example

To create a Responder action and policy to respond to Diameter requests that originate from "host1.example.net" with a redirect to "host.example.com", you could add the following action and policy, and bind the policy as shown.

```
> add responder action act_resp-dm-redirect RESPONDWITH "DIAMETER.NEW_REDIRECT(\"aaa://host.exampl
> add responder pol_resp-dm-redirect "diameter.req.avp(264).value.eq(\"host1.example.net\")" act_resp-dm
> bind lb vserver vs1 -policyName pol_resp-dm-redirect -priority 10 -type REQUEST

Done
```

Rewrite

Rewrite refers to the rewriting of some information in the requests or responses handled by the NetScaler appliance. Rewriting can help in providing access to the requested content without exposing unnecessary details about the Web site's actual configuration. A few situations in which the rewrite feature is useful are described below:

- To improve security, the NetScaler can rewrite all the http:// links to https:// in the response body.
- In the SSL offload deployment, the insecure links in the response have to be converted into secure links. Using the rewrite option, you can rewrite all the *http://* links to *https://* for making sure that the outgoing responses from NetScaler to the client have the secured links.
- If a Web site has to show an error page, you can show a custom error page instead of the default 404 Error page. For example, if you show the home page or site map of the Web site instead of an error page, the visitor remains on the site instead of moving away from the Web site.
- If you want to launch a new Web site, but use the old URL, you can use the Rewrite option.
- When a topic in a site has a complicated URL, you can rewrite it with a simple, easy-to-remember URL (also referred to as 'cool URL').
- You can append the default page name to the URL of a Web site. For example, if the default page of a company's Web site is '*http://www.abc.com/index.php*', when the user types '*abc.com*' in the address bar of the browser, you can rewrite the URL to '*abc.com/index.php*'.

When you enable the rewrite feature, NetScaler can modify the headers and body of HTTP requests and responses.

To rewrite HTTP requests and responses, you can use protocol-aware NetScaler policy expressions in the rewrite policies you configure. The virtual servers that manage the HTTP requests and responses must be of type HTTP or SSL. In HTTP traffic, you can take the following actions:

- Modify the URL of a request
- Add, modify or delete headers
- Add, replace, or delete any specific string within the body or headers.

To rewrite TCP payloads, consider the payload as a raw stream of bytes. Each of the virtual servers that managing the TCP connections must be of type TCP or SSL_TCP. The term *TCP rewrite* is used to refer to the rewrite of TCP payloads that are not HTTP data. In TCP traffic, you can add, modify, or delete any part of the TCP payload.

For examples to use the rewrite feature, see "Rewrite Action and Policy Examples."

Comparison between Rewrite and Responder options

The main difference between the rewrite feature and the responder feature is as follows:

Responder cannot be used for response or server-based expressions. Responder can be used only for the following scenarios depending on client parameters:

- Redirecting a http request to new Web sites or Web pages
- Responding with some custom response
- Dropping or resetting a connection at request level

In case of a responder policy, the NetScaler examines the request from the client, takes action according to the applicable policies, sends the response to the client, and closes the connection with the client.

In case of a rewrite policy, the NetScaler examines the request from the client or response from the server, takes action according to the applicable policies, and forwards the traffic to the client or the server.

In general, it is recommended to use responder if you want the NetScaler to reset or drop a connection based on a client or request-based parameter. Use responder to redirect traffic, or respond with custom messages. Use rewrite for manipulating data on HTTP requests and responses.

How Rewrite Works

A rewrite policy consists of a rule and action. The rule determines the traffic on which rewrite is applied and the action determines the action to be taken by the NetScaler. You can define multiple rewrite policies. For each policy, specify the bind point and priority.

A *bind point* refers to a point in the traffic flow at which the NetScaler examines the traffic to verify whether any rewrite policy can be applied to it. You can bind a policy to a specific load balancing or content switching virtual server, or make the policy global if you want the policy to be applied to the entire traffic handled by the NetScaler. These policies are referred to as global policies.

In addition to the user-defined policies, the NetScaler has some default policies. You cannot modify or delete a default policy.

For evaluating the policies, NetScaler follows the order mentioned below:

- Global policies
- Policies bound to specific virtual servers
- Default policies

Note: NetScaler can apply a rewrite policy only when it is bound to a point.

NetScaler implements the rewrite feature in the following steps:

- The NetScaler appliance checks for global policies and then checks for policies at individual bind points.
- If multiple policies are bound to a bind point, the NetScaler evaluates the policies in the order of their priority. The policy with the highest priority is evaluated first. After evaluating each policy, if the policy is evaluated to TRUE (the traffic matches the rule), it adds the action associated with the policy to a list of actions to be performed. A match occurs when the characteristics specified in the policy rule match the characteristics of the request or response being evaluated.
- For any policy, in addition to the action, you can specify the policy that should be evaluated after the current policy is evaluated. This policy is referred to as the 'Go to Expression'. For any policy, if a Go to Expression (gotoPriorityExpr) is specified, the NetScaler evaluates the Go to Expression policy; it ignores policy with the next highest priority.

  You can specify the priority of the policy to indicate the Go to Expression policy; you cannot use the name of the policy. If you want the NetScaler to stop evaluating other policies after evaluating a particular policy, you can set the Go to Expression to 'END'.
- After all the policies are evaluated or when a policy has the Go to Expression set as END, the NetScaler starts performing the actions according to the list of actions.

For more information about configuring rewrite policies, see "Configuring a Rewrite Policy" and about binding rewrite policies, see "Binding a Rewrite Policy."

The following figure illustrates how NetScaler processes a request or response when the rewrite feature is used.

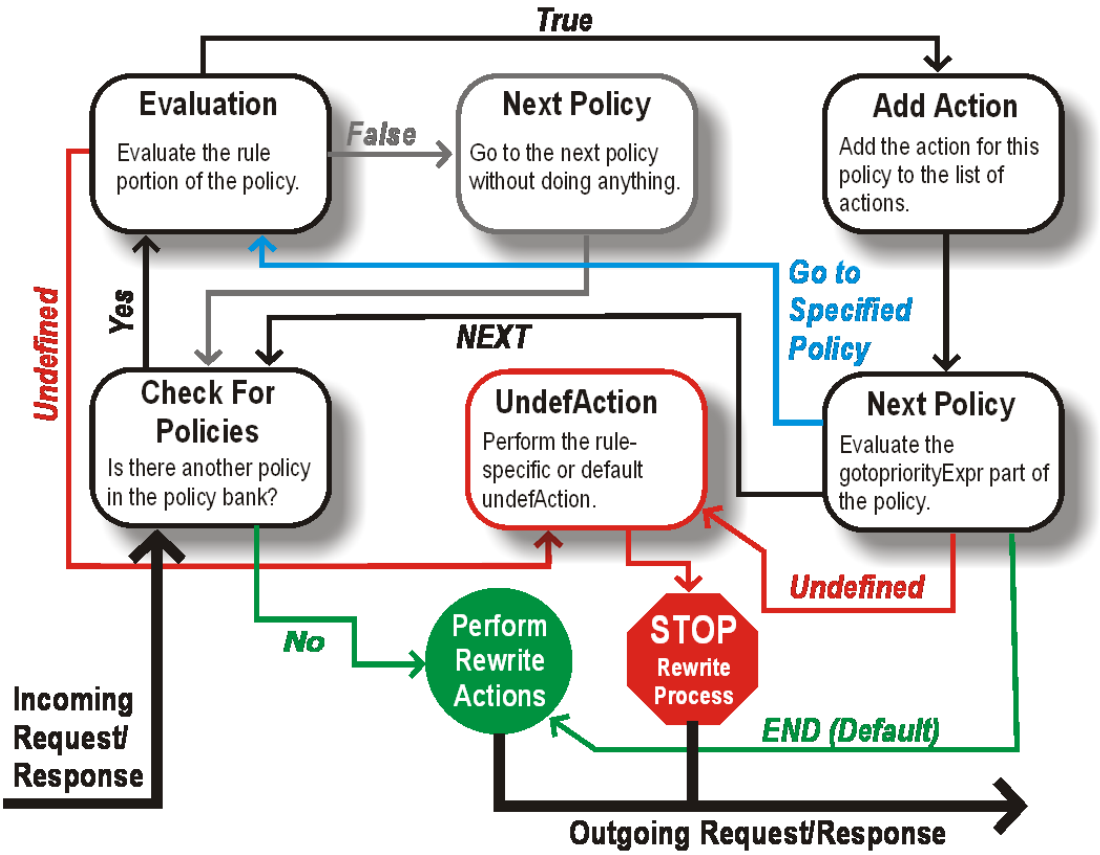


Figure 1. The Rewrite Process

Policy Evaluation

The policy with the highest priority is evaluated first. NetScaler does not stop the evaluation of rewrite policies when it finds a match; it evaluates all the rewrite policies configured on the NetScaler.

- If a policy evaluates to TRUE, the NetScaler follows the procedure below:
  - If the policy has the Go to Expression set to END, the NetScaler stops evaluating all the other policies and starts performing the rewrite.
  - The *gotoPriorityExpression* can be set to 'NEXT', 'END', some integer or 'INVOCATION_LIST'. The value determines the policy with the next priority. The following table shows the action taken by NetScaler for each value of the expression.

Value of the expression	Action
NEXT	Policy with the next priority gets evaluated.
END	Evaluation of policies stops.

<an integer>	Policy with specified priority gets evaluated.
INVOCATION_LIST	Goto NEXT or END is applied based on the result of the invocation list.

- If a policy evaluates to FALSE, the NetScaler continues the evaluation in the order of priority.
- If a policy evaluates to UNDEFINED (cannot be evaluated on the received traffic due to an error), the NetScaler performs the action assigned to the UNDEFINED condition (referred to as *undefAction*) and stops further evaluation of polices.

The NetScaler starts the actual rewriting only after the evaluation is complete. It refers to the list of actions identified by policies that are evaluated to TRUE, and starts the rewriting. After implementing all the actions in the list, the NetScaler forwards the traffic as required.

Note: Ensure that the policies do not specify conflicting or overlapping actions on the same part of the HTTP header or body, or TCP payload. When such a conflict occurs, the NetScaler encounters an undefined situation and aborts the rewrite.

Rewrite Actions

On the NetScaler appliance, specify the actions to be taken such as adding, replacing, or deleting text within the body, or adding, modifying or deleting headers, or any changes in the TCP payload as *rewrite actions*. For more information about rewrite actions, see "Configuring a Rewrite Action."

The following table describes the steps the NetScaler can take when a policy evaluates to TRUE.

Action	Result
Insert	The rewrite action specified for the policy is carried out.
NOREWRITE	The request or response is not rewritten. NetScaler forwards the traffic without rewriting any part of the message.
RESET	The connection is aborted at the TCP level.
DROP	The message is dropped.

Note: For any policy, you can configure the undefaction (action to be taken when the policy evaluates to UNDEFINED) as NOREWRITE, RESET, or DROP.

To use the Rewrite feature, take the following steps:

- Enable the feature on the NetScaler.
- Define rewrite actions.
- Define rewrite policies.
- Bind the policies to a bind point to bring a policy into effect.

Enabling the Rewrite Feature

Enable the rewrite feature on the NetScaler appliance if you want to rewrite the HTTP or TCP requests or responses. If the feature is enabled, NetScaler takes rewrite action according to the specified policies. For more information, see "How Rewrite Works."

To enable the rewrite feature by using the command line interface

At the command prompt, type the following commands to enable the rewrite feature and verify the configuration:

- enable ns feature REWRITE
- show ns feature

Example

```
> enable ns feature REWRITE
 Done
> show ns feature

      Feature                Acronym          Status
      -------                -------          ------
1)    Web Logging              WL               OFF
2)    Surge Protection         SP               ON
.
.
.
19)   Rewrite                  REWRITE          ON
.
.
24)   NetScaler Push           push             OFF
Done
```

To enable the rewrite feature by using the configuration utility

1. In the navigation pane, click System, and then click Settings.
2. In the details pane, under Modes and Features, click Configure basic features.
3. In the Configure Basic Features dialog box, select the Rewrite check box, and then click OK.
4. In the Enable/Disable Feature(s) dialog box, click Yes. A message appears in the status bar, stating that the selected feature was enabled.

Configuring a Rewrite Action

After enabling the rewrite feature, you need to configure one or more actions unless a built-in rewrite action is sufficient. All of the built-in actions have names beginning with the string ns_cvpn, followed by a string of letters and underscore characters. Built-in actions perform useful and complex tasks such as decoding parts of a clientless VPN request or response or modifying JavaScript or XML data. The built-in actions can be viewed, enabled, and disabled, but cannot be modified or deleted.

Target expressions in actions for TCP rewrite must begin with one of the following expression prefixes:

- **`CLIENT.TCP.PAYLOAD`.** For rewriting TCP payloads in client requests. For example, `CLIENT.TCP.PAYLOAD(10000).AFTER_STR("string1")`.
- **`SERVER.TCP.PAYLOAD`.** For rewriting TCP payloads in server responses. For example, `SERVER.TCP.PAYLOAD(1000).B64DECODE.BETWEEN("string1","string2")`.

You can use all types of existing string manipulation functions with these prefixes to identify the strings that you want to rewrite. To configure a rewrite action, you assign it a name, specify an action type, and add one or more arguments specifying additional data. The following table describes the action types and the arguments you use with them.

Note: Action types that can be used only for HTTP rewrite are identified in the **Rewrite Action Type** column.

Table 1. Rewrite Action Types and Their Arguments

Rewrite Action Type	Argument 1	Argument 2
INSERT_HTTP_HEADER: Inserts the HTTP header you specify into the HTTP request or response. This is the default choice. This action type can be used only with HTTP requests and responses.	The HTTP header you want to insert. For example, if you want to insert the client IP from which a request is sent, type `Client-IP`.	A string expression that describes the contents of the header you want to insert. For example, if you want to insert the Client IP from which a request is sent, type `CLIENT.IP.SRC`.

INSERT_BEFORE: Inserts a new string before the designated string.	A string expression that describes the string before which you want to insert a new string. For example, if you want to find the hostname www.example.com and insert a string before the example.com portion, type the following: `HTTP.REQ.HOSTNAME.BEFORE_STR ("example.com")`	A string expression that describes the new string you want to insert. For example, if you want to insert the new string en. before the string example in the hostname, type en followed by a period.
INSERT_AFTER: Inserts a new string after the designated string.	A string expression that describes the string after which you want to insert a new string. For example, if you want to find the hostname www.example.com, and insert a string after the www. portion, type the following: `HTTP.REQ.HOSTNAME.AFTER_STR ("www.")`	A string expression that describes the new string you want to insert. For example, if you want to insert the new string en. after the string www. in the hostname, type en followed by a period.
REPLACE: Replaces the designated string with a different string.	A string expression that describes the string you want to replace with a new string. For example, if you want to replace the entire hostname in the Host header, type `HTTP.REQ.HOSTNAME.SERVER`.	A string expression that describes the new string you want to insert. For example, if you want to replace the current host header with the string web01.example.net, type `web01.example.net`.
DELETE: Deletes the designated string.	A string expression that describes the string you want to delete. For example, if you want to find and delete the string .en in the hostname of HTTP response headers, type the following: `HTTP.RES.HEADER("Host").SUBSTR("en.")`	

DELETE_HTTP_HEADER: Deletes the designated HTTP header, including all header contents. This action type can be used only with HTTP requests and responses.	The name of the HTTP header you want to delete. For example, if you want to delete the cache-control header from HTTP responses, type `HTTP.RES.HEADER ("Cache-Control").`	
CORRUPT_HTTP_HEADER: Replaces the name of the given HTTP header with a corrupted name so that it will not be recognized by the receiver. This action type can be used only with HTTP requests and responses.	The name of the HTTP header that you want to corrupt. If the specified header occurs more than once in a request, all the occurrences are corrupted. For example, if you want to corrupt the `Host` header in an HTTP request, you can use the following rewrite action command: `add rewrite action corrupt_header_act CORRUPT_HTTP_HEADER Host.`	
REPLACE_HTTP_RES: Replace the http response with the value specified in the target field. This action type can be used only with HTTP requests and responses.	A string expression that describes the string you want to replace the HTTP response with. For example, type `HTTP 200 OK` You are not authorized to view this page to replace the entire HTTP response with this warning.	
REPLACE_ALL: Will replace all occurrences of a pattern in the target text reference with the value specified in the string builder expression.	The part of either the HTTP request or response where you want to carry out the replacement.	A string expression that describes the new string you want to insert.
DELETE_ALL: Delete every occurrence of the pattern specified in the target text reference.	The part of either the HTTP request or response where you want the deletion to occur.	A string pattern after which the deletion should occur.

INSERT_AFTER_ALL: Inserts the value specified by string builder expression after each occurrence of a specified pattern in the target text reference.	The part of either the HTTP request or response where you want the insertion to occur.	A string expression that describes the new string you want to insert.
INSERT_BEFORE_ALL: Inserts the value you specify before each occurrence of the pattern you specify.	The part of either the HTTP request or response that you want to delete.	A string expression that describes the new string you want to insert.
CLIENTLESS_VPN_ENCODE: Encodes the URL you specify in clientless VPN format.	The URL you want to encode.	
CLIENTLESS_VPN_ENCODE_ALL: Encodes all of the URLs you specify in clientless VPN format.	A pattern that matches the URLs you want to encode.	
CLIENTLESS_VPN_DECODE: Decodes the URL you specify from clientless VPN format and returns it as unencoded text.	The URL you want to decode.	
CLIENTLESS_VPN_DECODE_ALL: Decodes all of the URLs you specify from clientless VPN format and returns them as unencoded text.	A pattern that matches all of the URLs you want to decode.	

To create a new rewrite action by using the command line interface

At the command prompt, type the following commands to create a new rewrite action and verify the configuration:

- add rewrite action <name> <type> <target> [<stringBuilderExpr>] [(-pattern <expression> | -patset <string>)] [-bypassSafetyCheck (YES|NO)]
- show rewrite action <name>

Example 1: Inserting an HTTP Header With the Client IP

```
> add rewrite action insertact INSERT_HTTP_HEADER "client-IP" CLIENT.IP.SRC
Done

> show rewrite action insertact

    Name: insertact
    Operation: insert_http_header   Target:Client-IP
    Value:CLIENT.IP.SRC
```

```
        BypassSafetyCheck : NO
        Hits: 0
        Undef Hits: 0
        Action Reference Count: 0
 Done
```

Example 2: Replacing Strings in a TCP Payload (TCP Rewrite)

```
> add rewrite action client_tcp_payload_replace_all REPLACE_ALL
  'client.tcp.payload(1000)' '"new-string"' -search text("old-string")
 Done
> show rewrite action client_tcp_payload_replace_all

        Name: client_tcp_payload_replace_all
        Operation: replace_all
        Target:client.tcp.payload(1000)
        Value:"new-string"
        Search: text("old-string")
        BypassSafetyCheck : NO
        Hits: 0
        Undef Hits: 0
        Action Reference Count: 0
 Done
>
```

To modify an existing rewrite action by using the command line interface

At the command prompt, type the following commands to modify an existing rewrite action and verify the configuration:

- set rewrite action <name> [-target <string>] [-stringBuilderExpr <string>] [(-pattern <expression> | -patset <string>)] [-bypassSafetyCheck (YES|NO)]
- show rewrite action <name>

Example

```
> set rewrite action insertact -target "Client-IP"
 Done
> show rewrite action insertact

        Name: insertact
        Operation: insert_http_header   Target:Client-IP
        Value:CLIENT.IP.SRC
        BypassSafetyCheck : NO
        Hits: 0
        Undef Hits: 0
        Action Reference Count: 0
```

Done

To remove a rewrite action by using the command line interface

At the command prompt, type the following commands to remove a rewrite action :

rm rewrite action <name>

Example

```
> rm rewrite action insertact
Done
```

Parameters for configuring a rewrite action

name

A name for your new action, or the name of the existing action you want to modify or remove. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should choose a name that will make it easy for others to tell what this action is supposed to do. (Cannot be changed for an existing action.)

pattern

Pattern that is used to match multiple strings in the request or response. The pattern may be a string literal (without quotes) or a PCRE-format regular expression with a delimiter that consists of any printable ASCII non-alphanumeric character except for the underscore (_) and space ( ) that is not otherwise used in the expression. Example: re~https?://|HTTPS?://~ The preceding regular expression can use the tilde (~) as the delimiter because that character does not appear in the regular expression itself. Used in the INSERT_BEFORE_ALL, INSERT_AFTER_ALL, REPLACE_ALL, and DELETE_ALL action types.

bypassSafetyCheck

Whether to bypass the built-in safety checks when adding or modifying this action. Values: YES, NO. Default: NO. For more information, see "Bypassing the Safety Check."

target

A NetScaler default syntax expression that describes the text to be rewritten by the rewrite action. For TCP rewrite actions, the target expression must begin with either `CLIENT.TCP.PAYLOAD` or `SERVER.TCP.PAYLOAD`.

stringBuilderExpr

Expression specifying the new value of the rewritten packet. Maximum length of a string literal that can be used inside the expression is 255 characters. A string literal that contains more than 255 characters can be split into smaller chunks of 255 characters each. The chunks can then be concatenated with the + operator. Maximum length of the input expression is 8191.

search

Searches for the designated string or expression in the HTTP header or body. You can use a search expression with actions of the following types: delete_all, insert_after_all, insert_before_all, and replace_all. You can use any of the following argument types:

- **String (`-search text("<string>")`).** A literal text string. For example, the following expression searches an HTTP response for the string "Server: Apache", which indicates that the responding server is an Apache HTTPD server:

  -search text("Server: Apache")

- **Regular Expression (`-search regex(re/<regex>/)`).** A PCRE-format regular expression. For example, the following expression searches an HTTP response for a Location header, which indicates a redirect URL:

  -search regex(re/^Location:/)

- **XPath Expression (`-search xpath(xp%<xpathex>%)`).** An XPath expression that is used to search a standard XML file. For example, the following expression searches an XML request or response for the path "/a/b" :

  -search xpath(xp%/a/b%)

- **XPath JSON Expression (`-search xpath_json(xp%<xpathex>%)`).** An XPath expression that is used to search a JavaScript Object Notation (JSON) file. For example, the following expression searches a JSON request or response for the path "/a/b":

  -search xpath_json(xp%/a/b%)

- **Patset (`-search patset("<patset>")`).** A pattern set. For example, the following expression searches an HTTP request or response for a match with the `zipcodes` patset:

  -search patset("zipcodes")

refineSearch (-refineSearch "extend(#,#).<expression>)

A means of more efficiently searching and rewriting a lengthy response than with a simple search command. Instead of using the Search command to search for all occurrences of a regular expression and then rewriting the matched strings, refineSearch enables you to search for a simple string that appears within the text you want to rewrite, and then refine that search by including surrounding context, and then searching only the selected text and context for a regular expression match.

For example, assume that you want to search a response for all URLs at any host within the domain `example.net`. Instead of simply searching the entire response for the regular expression `#<https?://(^|[0-9A-Za-z][0-9A-Za-z]+\.example.net/[^>]*># `, you could use the following command:

```
add rewrite action <name> <type> 'http.res.body(10000)'
  -pattern "example.net" -refineSearch "extend(20,40).regex_select
   (re%<https?://(^|[0-9A-Za-z][0-9A-Za-z]+\.example.net/[^>]*>%)"
```

The refineSearch command does the same thing that the equivalent Search command would do, but is more efficient and runs faster. The difference may be negligible with a small response body, but can be significant when the response body is large.

To configure a rewrite action by using the configuration utility

1. Navigate to Rewrite > Actions.
2. In the details pane, do one of the following:
   - To create a new action, click Add.
   - To modify an existing action, select the action, and then click Open.
3. In the Add Rewrite Action or Configure Rewrite Action dialog box, specify values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring a rewrite action" as follows (asterisk indicates a required parameter):
   - Name*—name
   - Type*—type (When you select a type of action from the Type list, the names of the remaining text boxes in the Create Rewrite Action or Configure Rewrite Action dialog box change to indicate the kind of additional information to be entered. For all Expression and String Expression text boxes, be sure to enclose strings in double quotation marks. Alternatively, you can use the Add Expression dialog box, as described in the procedure that follows this one.)
     - Expression (Argument 1)
     - Expression (Argument 2) (Several types do not take a second argument, in which case this text area will be greyed out.)
   - Pattern—target (Several types have implied targets, in which case this text area is greyed out.)
   - Bypass Safety Check—bypassSafetyCheck
4. Click Create or OK. A message appears in the status bar, stating that the Action has been configured successfully.
5. Repeat steps 2 through 4 to create or modify as many rewrite actions as you wish.
6. Click Close.

To add an expression by using the Add Expression dialog box

1. In the Create Rewrite Action or Configure Rewrite Action dialog box, under the text area for the type argument you want to enter, click Add.

2. In the Add Expression dialog box, in the first list box choose the first term for your expression.

   HTTP

   The HTTP protocol. Choose this if you want to examine some aspect of the request that pertains to the HTTP protocol.

   SYS

   The protected Web site(s). Choose this if you want to examine some aspect of the request that pertains to the recipient of the request.

   CLIENT

   The computer that sent the request. Choose this if you want to examine some aspect of the sender of the request.

   When you make your choice, the rightmost list box lists appropriate terms for the next part of your expression.

3. In the second list box, choose the second term for your expression. The choices depend upon which choice you made in the previous step, and are appropriate to the context. After you make your second choice, the Help window below the Construct Expression window (which was blank) displays help describing the purpose and use of the term you just chose.

4. Continue choosing terms from the list boxes that appear to the right of the previous list box, or typing strings or numbers in the text boxes that appear to prompt you to enter a value, until your expression is finished.

   For more information about the PI expressions language and creating expressions for responder policies, see "Policies and Expressions."

   If you want to test the effect of a rewrite action when used on sample HTTP data, you can use the Rewrite Expression Evaluator.

   Note: The Rewrite Expression Evaluator is only available in the configuration utility. There is no NetScaler command line version.

To evaluate a rewrite action by using the Rewrite Action Evaluator dialog box

1. In the Rewrite Actions details pane, select the rewrite action that you want to evaluate, and then click Evaluate.

2. In the Rewrite Expression Evaluator dialog box, specify values for the following parameters. (An asterisk indicates a required parameter.)

   - Rewrite Action*—If the rewrite action you want to evaluate is not already selected, select it from the drop-down list. After you select a Rewrite action, the Details section displays the details of the selected Rewrite action.

   - New*—Select New to open the Create Rewrite Action dialog box and create a new rewrite action.

   - Modify*—Select Modify to open the Configure Rewrite Action dialog box and modify the selected rewrite action.

   - Flow Type*—Specifies whether to test the selected rewrite action with HTTP Request data or HTTP Response data. The default is Request. If you want to test with Response data, select Response.

   - HTTP Request/Response Data*—Provides a space for you to provide the HTTP data that the Rewrite Action Evaluator will use for testing. You can paste the data directly into the window, or click Sample to insert some sample HTTP headers.

   - Show end-of-line—Specifies whether to show UNIX-style end-of-line characters (\n) at the end of each line of sample HTTP data.

   - Sample—Inserts sample HTTP data into the HTTP Request/Response Data window. You can choose either GET or POST data.

   - Browse—Opens a local browse window so that you can choose a file containing sample HTTP data from a local or network location.

   - Clear—Clears the current sample HTTP data from the HTTP Request/Response Data window.

3. Click Evaluate. The Rewrite Action Evaluator evaluates the effect of the Rewrite action on the sample data that you chose, and displays the results as modified by the selected Rewrite action in the Results window. Additions and deletions are highlighted as indicated in the legend in the lower left-hand corner of the dialog box.

4. Continue evaluating Rewrite actions until you have determined that all of your actions have the effect that you wanted.

   - You can modify the selected rewrite action and test the modified version by clicking Modify to open the Configure Rewrite Action dialog box, making and saving your changes, and then clicking Evaluate again.

   - You can evaluate a different rewrite action using the same request or response data by selecting it from the Rewrite Action drop-down list, and then clicking Evaluate again.

5. Click Close to close the Rewrite Expression Evaluator and return to the Rewrite Actions pane.

To delete a rewrite action, select the rewrite action you want to delete, then click Remove and, when prompted, confirm your choice by clicking OK.

Configuring a Rewrite Policy

After you create any needed rewrite action(s), you must create at least one rewrite policy to select the requests that you want the NetScaler appliance to rewrite.

A rewrite policy consists of a rule, which itself consists of one or more expressions, and an associated action that is performed if a request or response matches the rule. Policy rules for evaluating HTTP requests and responses can be based on almost any part of a request or response.

Even though you cannot use TCP rewrite actions to rewrite data other than the TCP payload, you can base the policy rules for TCP rewrite policies on the information in the transport layer and the layers below the transport layer.

If a configured rule matches a request or response, the corresponding policy is triggered and the action associated with it is carried out.

Note: You can use either the command line interface or the configuration utility to create and configure rewrite policies. Users who are not thoroughly familiar with the command line interface and the NetScaler Policy expression language will usually find using the configuration utility much easier.

To add a new rewrite policy by using the command line interface

At the command prompt, type the following commands to add a new rewrite policy and verify the configuration:

- add rewrite policy <name> <expression> <action> [<undefaction>]
- show rewrite policy <name>

Example 1: Rewriting HTTP Content

```
> add rewrite policy policyNew "HTTP.RES.IS_VALID" insertact NOREWRITE
 Done
> show rewrite policy policyNew
      Name: policyNew
      Rule: HTTP.RES.IS_VALID
      RewriteAction: insertact
      UndefAction: NOREWRITE
      Hits: 0
      Undef Hits: 0

 Done
```

Example 2: Rewriting a TCP Payload (TCP Rewrite)

```
> add rewrite policy client_tcp_payload_policy CLIENT.IP.SRC.EQ(172.168.12.232) client_tcp_payload_replac
 Done
> show rewrite policy client_tcp_payload_policy
      Name: client_tcp_payload_policy
      Rule: CLIENT.IP.SRC.EQ(172.168.12.232)
      RewriteAction: client_tcp_payload_replace_all
      UndefAction: Use Global
      LogAction: Use Global
      Hits: 0
      Undef Hits: 0

 Done
>
```

To modify an existing rewrite policy by using the command line interface

At the command prompt, type the following commands to modify an existing rewrite policy and verify the configuration:

- set rewrite policy <name> -rule <expression> -action <action> [<undefaction>]
- show rewrite policy <name>

Example

```
> set rewrite policy policyNew -rule "HTTP.RES.IS_VALID" -action insertaction
 Done

> show rewrite policy policyNew
      Name: policyNew
      Rule: HTTP.RES.IS_VALID
      RewriteAction: insertaction
      UndefAction: NOREWRITE
      Hits: 0
      Undef Hits: 0

 Done
```

To remove a rewrite policy by using the command line interface

At the command prompt, type the following command to remove a rewrite policy:

rm rewrite policy <name>

Example

```
> rm rewrite policy policyNew
Done
```

Parameters for configuring a rewrite policy

name

A name for the policy, or the name of the existing policy you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should choose a name that will make it easy for others to tell what type of request this policy was created to match. (Cannot be changed for an existing policy.)

rule

The expression that defines the rule for this policy. The expression can be a simple expression or a complex expression that contains several expressions in structured relationship to one another. Expressions are written in the NetScaler default syntax.

Note: The rewrite feature does not support the use of stream selectors that include SIP-based expressions.

For more information about the default syntax, see "Policies and Expressions."

action

The name of the rewrite action associated with the policy. You can choose either one of the built-in rewrite actions, or a rewrite action you have configured. For a complete list of built-in rewrite actions, see "Policies and Expressions."

undefAction

The action to use if the policy generates an UNDEF event. You can select the NOREWRITE, RESET, or DROP action, or configure the NetScaler use the configured global undefined action.

Any rewrite-specific undefined action you configure will override the global undefined action.

To configure a rewrite policy by using the configuration utility

1. Navigate to Rewrite > Policies.
2. In the details pane, do one of the following:
   - To create a new policy, click Add.
   - To modify an existing policy, select the policy, and then click Open.
3. In the Create Rewrite Policy or Configure Rewrite Policy dialog box, specify values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring a rewrite policy" as follows (asterisk indicates a required parameter):
   - Name*—name
   - Action*—action
   - Undefined-Result Action—undefAction
   - Expression*—expression (You can add the expression in any of three ways. First, you can click Add and choose an existing expression in the Frequently Used Expressions drop-down list. Second, you can type the expression directly into the supplied text box. For brief help and prompts, while the cursor is in the text box, hold down the CTRL key and then press the Space bar. Third, you can use the Add Expression dialog box, as described in “To add an expression by using the Add Expression dialog box.”)
4. Click Create or OK. A message appears in the status bar, stating that the Policy has been configured successfully.
5. Repeat steps 2 through 4 to create or modify as many rewrite actions as you wish.
6. Click Close. To delete a rewrite policy, select the rewrite policy you want to delete, then click Remove and, when prompted, confirm your choice by clicking OK.

Binding a Rewrite Policy

After creating a rewrite policy, you must bind it to put it into effect. You can bind your policy to Global if you want to apply it to all traffic that passes through your NetScaler, or you can bind your policy to a specific virtual server or bind point to direct only that virtual server or bind point's incoming traffic to that policy. If an incoming request matches a rewrite policy, the action associated with that policy is carried out.

Rewrite policies for evaluating HTTP requests and responses can be bound to virtual servers of type HTTP or SSL, or they can be bound to the REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, and RES_DEFAULT bind points. Rewrite policies for TCP rewrite can be bound only to virtual servers of type TCP or SSL_TCP, or to the OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, OTHERTCP_RES_OVERRIDE, and OTHERTCP_RES_DEFAULT bind points.

Note: The term OTHERTCP is used in the context of the NetScaler appliance to refer to all TCP or SSL_TCP requests and responses that you want to treat as a raw stream of bytes regardless of the protocols that the TCP packets encapsulate.

When you bind a policy, you assign it a priority. The priority determines the order in which the policies you define are evaluated. You can set the priority to any positive integer.

In the NetScaler operating system, policy priorities work in reverse order - the higher the number, the lower the priority. For example, if you have three policies with priorities of 10, 100, and 1000, the policy assigned a priority of 10 is applied first, then the policy assigned a priority of 100, and finally the policy assigned an order of 1000.

Unlike most other features in the NetScaler operating system, the rewrite feature continues to evaluate and implement policies after a request matches a policy. However, the effect of a particular action policy on a request or response will often be different depending on whether it is performed before or after another action. Priority is important to get the results you intended.

You can leave yourself plenty of room to add other policies in any order, and still set them to evaluate in the order you want, by setting priorities with intervals of 50 or 100 between each policy when you bind it. If you do this, you can add additional policies at any time without having to reassign the priority of an existing policy.

When binding a rewrite policy, you also have the option of assigning a goto expression (gotoPriorityExpression) to the policy. A goto expression can be any positive integer that matches the priority assigned to a different policy that has a higher priority than the policy that contains the goto expression. If you assign a goto expression to a policy, and a request or response matches the policy, the NetScaler will immediately go to the policy whose priority matches the goto expression. It will skip over any policies with priority numbers that are lower than that of the current policy, but higher than the priority number of the goto expression, and not evaluate those policies.

For more information about binding policies on the NetScaler, see "Binding a Rewrite Policy."

To globally bind a rewrite policy by using the command line interface

At the command prompt, type the following commands to globally bind a rewrite policy and verify the configuration:

- bind rewrite global <policyName> <priority> [<gotoPriorityExpression>] [-type <type>] [-invoke (<labelType> <labelName>)]
- show rewrite global

Example

```
>bind rewrite global policyNew 10
 Done

> show rewrite global
1)      Global bindpoint: RES_DEFAULT
       Number of bound policies: 1

2)      Global bindpoint: REQ_OVERRIDE
       Number of bound policies: 1

 Done
```

To bind rewrite policy to a specific virtual server by using the command line interface

At the command prompt, type the following commands to bind rewrite policy to a specific virtual server and verify the configuration:

- bind lb vserver <name>@ (<serviceName>@ [-weight <positive_integer>]) | <serviceGroupName>@ | (-policyName <string>@ [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-type (REQUEST | RESPONSE)] [-invoke (<labelType> <labelName>)])
- show lb vserver <name>

Example

```
> bind lb vserver lbvip -policyName ns_cmp_msapp -priority 50
 Done
>
> show lb vserver lbvip
      lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
      State: DOWN
      Last state change was at Wed Jul 15 05:54:24 2009 (+226 ms)
      Time since last state change: 28 days, 01:57:26.350
```

```
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1)      Policy : ns_cmp_msapp Priority:50
2)      Policy : cf-pol Priority:1      Inherited
 Done
```

Parameters for binding a rewrite policy

name

If you are binding this rewrite policy to a specific virtual server, the name of that virtual server.

policyName

The name of the rewrite policy you want to bind. This parameter is mandatory.

priority

The priority assigned to this rewrite policy. The priority determines the order in which policies are evaluated, allowing the NetScaler to evaluate the most specific policy first, and more general policies in descending order, finishing with the most general policy. The lower the value for this parameter, the higher the priority. Assign the lowest priority value to the policy that is to be evaluated first. This parameter is mandatory.

gotoPriorityExpression

The priority of the next policy that should be evaluated if this policy matches. If set to END, this parameter halts the policy evaluation process after evaluation of the current policy. If you are careful to assign your policy priorities in the right order, you can use this parameter to skip over policies in the event that the current policy matches, and go directly to a specific policy.

type

Bindpoint, specifying where to bind the policy.

invoke

Type of policy label invocation.

labelType

Type of policy label invocation.

labelName

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

weight

Weight for this service. This weight is used when the system performs load balancing, giving greater priority to a specific service. It is useful when the services bound to a virtual server are of different capacity.

To bind a rewrite policy to a bind point by using the configuration utility

1. Navigate to Rewrite > Policies.
2. In the details pane, select the rewrite policy you want to globally bind, and then click Policy Manager.
3. In the Rewrite Policy Manager dialog box, in the Bind Points menu, do one of the following:
   a. If you want to configure bindings for HTTP rewrite policies, click HTTP, and then click either Request or Response, depending on whether you want to configure request-based rewrite policies or response-based rewrite policies.
   b. If you want to configure bindings for TCP rewrite policies, click TCP, and then click either Client or Server, depending on whether you want to configure client-side TCP rewrite policies or server-side TCP rewrite policies.
4. Click the bind point to which you want to bind the rewrite policy. The Rewrite Policy Manager dialog box displays all the rewrite policies that are bound to the selected bind point.
5. Click Insert Policy to insert a new row and display a drop-down list with all available, unbound rewrite policies.
6. Click the policy you want to bind to the bind point. The policy is inserted into the list of rewrite policies bound to the bind point.
7. In the Priority column, you can change the priority to any positive integer. For more information about this parameter, see `priority` in "Parameters for binding a rewrite policy."
8. If you want to skip over policies and go directly to a specific policy in the event that the current policy is matched, change the value in the Goto Expression column to equal the priority of the next policy to be applied.. For more information about this parameter, see `gotoPriorityExpression` in "Parameters for binding a rewrite policy."
9. To modify a policy, click the policy, and then click Modify Policy.
10. To unbind a policy, click the policy, and then click Unbind Policy.
11. To modify an action, in the Action column, click the action you want to modify, and then click Modify Action.
12. To modify an invoke label, in the Invoke column, click the invoke label you want to modify, and then click Modify Invoke Label.
13. To regenerate the priorities of all the policies that are bound to the bind point you are currently configuring, click Regenerate Priorities. The policies retain their existing priorities relative to the other policies, but the priorities are renumbered in multiples of ten.
14. Click Apply Changes.

15. Click Close. A message appears in the status bar, stating that the Policy has been configured successfully.

To bind a rewrite policy to a specific virtual server by using the configuration utility

1. Navigate to Load Balancing > Virtual Servers.
2. In the details pane list of virtual servers, select the virtual server to which you want to bind the rewrite policy, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, select the Policies tab. All policies configured on your NetScaler appear on the list.
4. Select the check box next to the name of the policy you want to bind to this virtual server.
5. Click OK. A message appears in the status bar, stating that the Policy has been configured successfully.

Configuring Rewrite Policy Labels

If you want to build a more complex policy structure than is supported by single policies, you can create policy labels and then bind them as you would policies. A policy label is a user-defined point to which policies are bound. When a policy label is invoked, all the policies bound to it are evaluated in the order of the priority you configured. A policy label can include one or multiple policies, each of which can be assigned its own result. A match on one policy in the policy label can result in proceeding to the next policy, invoking a different policy label or appropriate resource, or an immediate end to policy evaluation and return of control to the policy that invoked the policy label.

A rewrite policy label consists of a name, a transform name that describes the type of policy included in the policy label, and a list of policies bound to the policy label. Each policy that is bound to the policy label contains all of the elements described in "Configuring a Rewrite Policy."

Note: You can use either the command line interface or the configuration utility to create and configure rewrite policy labels. Users who are not thoroughly familiar with the command line interface and the NetScaler Policy Infrastructure (PI) language will usually find using the configuration utility much easier.

To configure a rewrite policy label by using the command line interface

To add a new rewrite policy label, at the command prompt, type the following command:

```
add rewrite policylabel <labelName> <transform>
```

For example, to add a rewrite policy label named `polLabelHTTPResponses` to group all policies that work on HTTP responses, you would type the following:

```
add rewrite policylabel polLabelHTTPResponses http_res
```

To modify an existing rewrite policy label, at the NetScaler command prompt, type the following command:

```
set rewrite policy <name> <transform>
```

Note: The set rewrite policy command takes the same options as the add rewrite policy command.

To remove a rewrite policy label, at the NetScaler command prompt, type the following command:

```
rm rewrite policy<name>
```

For example, to remove a rewrite policy label named `polLabelHTTPResponses`, you would type the following:

```
rm rewrite policy polLabelHTTPResponses
```

Parameters for rewrite policy labels

name

A name for the policy label, or the name of the existing policy label that you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should choose a name that will make it easy for others to tell what type of policy this policy label was created to contain. (Cannot be changed for an existing policy label.)

transform

The type of policy that this policy label contains. Your choices are:

- http_req. Groups rewrite policies that process HTTP requests.
- http_res. Groups rewrite policies that process HTTP responses.
- URL. Groups rewrite policies that process HTTP URLs.
- text. Groups rewrite policies that process text.
- clientless_vpn_req. Groups rewrite policies that process clientless VPN requests.
- clientless_vpn_res. Groups rewrite policies that process clientless VPN responses.
- othertcp_req. Groups request-based TCP rewrite policies.
- othertcp_res. Groups response-based TCP rewrite policies.

The default is http_req.

To configure a rewrite policy label by using the configuration utility

1. Navigate to Rewrite > Policy Labels.
2. In the details pane, do one of the following:
   - To create a new policy label, click Add.
   - To modify an existing policy label, select the policy, and then click Open.
3. In the Create Rewrite Policy or Configure Rewrite Policy dialog box, specify values for the following parameters. (An asterisk indicates a required parameter. For a term in parentheses, see the corresponding parameter in the table above.)
   - Name* (name)
   - Transform* (transform)
4. Add or remove policies from the list that is bound to the policy label.
   - To add a policy to the list, click Insert Policy, and choose a policy from the drop-down list. You can create a new policy and add it to the list by choosing New Policy in the list, and following the instructions in "Configuring a Rewrite Policy."
   - To remove a policy from the list, select that policy, and then click Unbind Policy.
5. Modify the priority of each policy by editing the number in the Priority column.

   You can also automatically renumber policies by clicking Regenerate Priorities.

6. Click Create or OK, and then click Close.

   To remove a policy label, select it, and then click Remove. To rename a policy label, select it and then click Rename. Edit the name of the policy, and then click OK to save your changes.

Configuring the Default Rewrite Action

An undefined event is triggered when the NetScaler cannot evaluate a policy, usually because it detects a logical or other error in the policy or an error condition on the NetScaler. When the rewrite policy evaluation results in an error, the specified undefined action is carried out. Undefined actions configured at the rewrite policy level are carried out before a globally configured undefined action.

The NetScaler supports following three types of undefined actions:

undefAction NOREWRITE

Aborts rewrite processing, but does not alter the packet flow. This means that the NetScaler continues to process requests and responses that do not match any rewrite policy, and eventually forwards them to the requested URL unless another feature intervenes and blocks or redirects the request. This action is appropriate for normal requests to your Web servers, and is the default setting.

undefAction RESET

Resets the client connection. This means that the NetScaler tells the client that it must re-establish its session with the Web server. This action is appropriate for repeat requests for Web pages that do not exist, or for connections that might be attempts to hack or probe your protected Web site(s).

undefAction DROP

Silently drops the request without responding to the client in any way. This means that the NetScaler simply discards the connection without responding to the client. This action is appropriate for requests that appear to be part of a DDoS attack or another sustained attack on your servers.

Note: Undefined events can be triggered for both request and response flow specific policies.

To configure the default action by using the command line interface

At the command prompt, type the following commands to configure the default action and verify the configuration:

- set rewrite param -undefAction (NOREWRITE | RESET | DROP)
- show rewrite param

Example

```
> set rewrite param -undefAction NOREWRITE
 Done
> show rewrite param
       Action Name: NOREWRITE
 Done
```

To configure the default action by using the configuration utility

1. In the navigation pane, expand Rewrite.
2. In the details pane, under Rewrite Overview, click the Change Rewrite Settings link. The Set Rewrite Params dialog box appears.
3. Under Global Undefined-Result Action, select an option as follows:
   - NoRewrite—NOREWRITE
   - Reset—RESET
   - Drop—DROP
4. Click OK. The global undefined action is set to the value you chose.

Bypassing the Safety Check

When you create a rewrite action, the NetScaler verifies that the expression you used to create the action is safe. Expressions created by the NetScaler from run-time data, such as URLs contained in HTTP requests, can cause unexpected errors. The NetScaler reports expressions that cause such errors as unsafe expressions.

In some cases, the expressions may be safe. For example, the NetScaler cannot validate an expression that contains a URL that does not resolve, even if the URL does not resolve because the Web server is temporarily unavailable. You can manually bypass the Safety Check to allow these expressions.

To bypass the safety check by using the command line interface

At the command prompt, type the following commands to bypass the safety check and verify the configuration:

- set rewrite action <name> -bypassSafetyCheck YES
- show rewrite action <name>

Example

```
> set rewrite action insertact -bypassSafetyCheck YES
 Done
> show rewrite action insertact

      Name: insertact
      Operation: insert_http_header   Target:Client-IP
      Value:CLIENT.IP.SRC
      BypassSafetyCheck : YES
      Hits: 0
      Undef Hits: 0
      Action Reference Count: 2
 Done
```

To bypass safety check by using the configuration utility

1. In the navigation pane, expand Rewrite > Actions.
2. In the details pane, select the rewrite action to be exempted from the safety check, and then click Open.
3. In the Configure Rewrite Action dialog box, select the Bypass Safety Check check box.
4. Click OK.

Rewrite Action and Policy Examples

The examples in this section demonstrate how to configure rewrite to perform various useful tasks. The examples occur in the server room of Example Manufacturing Inc., a mid-sized manufacturing company that uses its Web site to manage a considerable portion of its sales, deliveries, and customer support.

Example Manufacturing has two domains: example.com for its Web site and email to customers, and example.net for its intranet. Customers use the Example Web site to place orders, request quotes, research products, and contact customer service and technical support.

As an important part of Example's revenue stream, the Web site must respond quickly and keep customer data confidential. Example therefore has several Web servers and uses Citrix NetScaler appliances to balance the Web site load and manage traffic to and from its Web servers.

The Example system administrators use the rewrite features to perform the following tasks:

Example 1: Delete old X-Forwarded-For and Client-IP Headers.

Example Inc. removes old X-Forwarded-For and Client-IP HTTP headers from incoming requests.

Example 2: Adding a Local Client-IP Header.

Example Inc. adds a new, local Client-IP header to incoming requests.

Example 3: Tagging Secure and Insecure Connections.

Example Inc. tags incoming requests with a header that indicates whether the connection is a secure connection.

Example 4: Mask the HTTP Server Type.

Example Inc. modifies the HTTP Server: header so that unauthorized users and malicious code cannot use that header to determine the HTTP server software it uses.

Example 5: Redirect an External URL to an Internal URL.

Example Inc. hides information about the actual names of its Web servers and the configuration of its server room from users, to make URLs on its Web site shorter and easier to remember, and to improve security on its site.

Example 6: Migrating Apache Rewrite Module Rules.

Example Inc. moved its Apache rewrite rules to a NetScaler appliance, translating the Apache PERL-based script syntax to the NetScaler rewrite rule syntax.

Example 7: Marketing Keyword Redirection.

The marketing department at Example Inc. sets up simplified URLs for certain predefined keyword searches on the company's Web site.

Example 8: Redirect Queries to the Queried Server.

Example Inc. redirects certain query requests to the appropriate server.

Example 9: Home Page Redirection.

Example Inc. recently acquired a smaller competitor, and it now redirects requests for the acquired company's home page to a page on its own Web site.

Each of these tasks requires that the system administrators create rewrite actions and policies and bind them to a valid bind point on the NetScaler.

Example 1: Delete Old X-Forwarded-For and Client-IP Headers

Example Inc. wants to remove old X-Forwarded-For and Client-IP HTTP headers from incoming requests, so that the only X-Forwarded-For headers that appear are the ones added by the local server. This configuration can be done through the NetScaler command line or the configuration utility. The Example Inc. system administrator is an old-school networking engineer and prefers to use a CLI where possible, but wants to be sure he understands the configuration utility interface so that he can show new system administrators on the team how to use it.

The examples below demonstrate how to perform each configuration with both the CLI and the configuration utility. The procedures are abbreviated on the assumption that users will already know the basics of creating rewrite actions, creating rewrite policies, and binding policies.

- For more detailed information about creating rewrite actions, see "Configuring a Rewrite Action."
- For more detailed information about creating rewrite policies, see "Configuring a Rewrite Policy."
- For more detailed information about binding rewrite policies, see "Binding a Rewrite Policy."

To delete old X-Forwarded and Client-IP headers from a request by using the command line interface

At the command prompt, type the following commands in the order shown:

```
add rewrite action act_del_xfor delete_http_header x-forwarded-for
add rewrite action act_del_cip delete_http_header client-ip
add rewrite policy pol_check_xfor 'HTTP.REQ.HEADER("x-forwarded-for").EXISTS' act_del_xfor
add rewrite policy pol_check_cip 'HTTP.REQ.HEADER("client-ip").EXISTS' act_del_cip
bind rewrite global pol_check_xfor 100 200
bind rewrite global pol_check_cip 200 300
```

To delete old X-Forwarded and Client-IP headers from a request by using the configuration utility

In the Create Rewrite Action dialog box, create two rewrite actions with the following descriptions.

Name	Type	Argument(s)
act_del_xfor	delete_http_header	x-forwarded-for
act_del_cip	delete_http_header	client-ip

In the Create Rewrite Policy dialog box, create two rewrite policies with the following descriptions.

Name	Expression	Action
pol_check_xfor	'HTTP.REQ.HEADER("x-forwarded-for").EXISTS'	act_del_xfor
pol_check_cip	'HTTP.REQ.HEADER("client-ip").EXISTS'	act_del_cip

Bind both policies to global, assigning the priorities and goto expression values shown below.

Name	Priority	Goto Expression
pol_check_xfor	100	200
pol_check_xfor	200	300

All old X-Forwarded-For and Client-IP HTTP headers are now deleted from incoming requests.

Example 2: Adding a Local Client-IP Header

Example Inc. wants to add a local Client-IP HTTP header to incoming requests. This example contains two slightly different versions of the same basic task.

To add a local Client-IP header by using the command line interface

At the command prompt, type the following commands in the order shown:

```
add rewrite action act_ins_client insert_http_header NS-Client 'CLIENT.IP.SRC'
add rewrite policy pol_ins_client 'HTTP.REQ.HEADER("x-forwarded-for").EXISTS || HTTP.REQ.HEADER("client-
bind rewrite global pol_ins_client 300 END
```

To add a local Client-IP header by using the configuration utility

In the Create Rewrite Action dialog box, create a rewrite action with the following description.

Name	Type	Argument(s)
act_ins_client	insert_http_header	NS-Client 'CLIENT.IP.SRC'

In the Create Rewrite Policy dialog box, create a rewrite policy with the following description.

Name	Expression	Action
pol_ins_client	'HTTP.REQ.HEADER("x-forwarded-for").EXISTS || HTTP.REQ.HEADER("client-ip").EXISTS'	act_ins_client

Bind both policies to global, assigning the priorities and goto expression values shown below.

Name	Priority	Goto Expression
pol_check_xfor	100	200
pol_check_xfor	200	300

A local Client-IP HTTP header is now added to incoming requests. You can also modify the configuration above to append all IPs from X-Forwarded-For headers to the new Client-IP header, as shown below.

Example 3: Tagging Secure and Insecure Connections

Example Inc. wants to tag incoming requests with a header that indicates whether or not the connection is a secure connection. This helps the server keep track of secure connections after the NetScaler has decrypted the connections.

To implement this configuration, you would begin by creating rewrite actions with the values shown in the following tables. These actions label connections to port 80 as insecure connections, and connections to port 443 as secure connections.

Action Name	Type of Rewrite Action	Header Name	Value
Action-Rewrite-SSL_YES	INSERT_HTTP_HEADER	SSL	YES

Action Name	Type of Rewrite Action	Header Name	Value
Action-Rewrite-SSL_NO	INSERT_HTTP_HEADER	SSL	NO

You would then create a rewrite policy with the values shown in the following tables. These policies check incoming requests to determine which requests are directed to port 80 and which are directed to port 443. The policies then add the correct SSL header.

Policy Name	Action Name	Undefined Action	Expression
Policy-Rewrite-SSL_YES	Action-Rewrite-SSL_YES	NOREWRITE	CLIENT.TCP.DSTPORT.EQ(443)
Policy-Rewrite-SSL_NO	Action-Rewrite-SSL_NO	NOREWRITE	CLIENT.TCP.DSTPORT.EQ(80)

Finally, you would bind the rewrite policies to NetScaler, assigning the first policy a priority of 200, and the second a priority of 300, and setting the goto expression of both policies to END.

Each incoming connection to port 80 now has an SSL:NO HTTP header added to it and each incoming connection to port 443 has an SSL:YES HTTP header added to it.

Example 4: Mask the HTTP Server Type

Example Inc. wants to modify the HTTP Server: header so that unauthorized users and malicious code cannot use the header to identify the software that the HTTP server uses.

To modify the HTTP Server: header, you would create a rewrite action and a rewrite policy with the values in the following tables.

Action Name	Type of Rewrite Action	Expression to choose target reference	String expression for replacement text
Action-Rewrite-Server_Mask	REPLACE	HTTP.RES.HEADER("Server")	"Web Server 1.0"

Policy Name	Action Name	Undefined Action	Expression
Policy-Rewrite-Server_Mask	Action-Rewrite-Server_Mask	NOREWRITE	HTTP.RES.IS_VALID

You would then globally bind the rewrite policy, assigning a priority of 100 and setting the Goto Priority Expression of the policy to END.

The HTTP Server: header is now modified to read “Web Server 1.0,” masking the actual HTTP server software used by the Example Inc. Web site.

Example 5: Redirect an External URL to an Internal URL

Example Inc. wants to hide its actual server room configuration from users to improve security on its Web servers.

To do this, you would create a rewrite action with the values as shown in the following tables. For request headers, the action in the table modifies `www.example.com` to web.hq.example.net. For response headers, the action does the opposite, translating `web.hq.example.net to www.example.com`.

Action Name	Type of Rewrite Action	Expression to choose target reference	String expression for replacement text
Action-Rewrite-Request_Server_Replace	REPLACE	HTTP.REQ.HOSTNAME.SERVER	"Web.hq.example.net"
Action-Rewrite-Response_Server_Replace	REPLACE	HTTP.RES.HEADER("Server")	"www.example.com"

Next, you would create rewrite policies using the values shown in the following tables. The first policy checks incoming requests to see if they are valid, and if they are, it performs the Action-Rewrite-Request_Server_Replace action. The second policy checks responses to see if they originate at the server web.hq.example.net. If they do, it performs the Action-Rewrite-Response_Server_Replace action.

ne	Action Name	Undefined Action	Expression
vrite-Request_Server_Replace	Action-Rewrite-Request_Server_Replace	NOREWRITE	HTTP.REQ.HOSTNAME.SERVER.EQ("w
vrite-Response_Server_Replace	Action-Rewrite-Response_Server_Replace	NOREWRITE	HTTP.RES.HEADER("Server").EQ("web

Finally, you would bind the rewrite policies, assigning each a priority of 500 because they are in different policy banks and therefore will not conflict. You should set the goto expression to NEXT for both bindings.

All instances of `www.example.com` in the request headers are now changed to `web.hq.example.net`, and all instances of web.hq.example.net in response headers are now changed to `www.example.com`.

Example 6: Migrating Apache Rewrite Module Rules

Example Inc., is currently using the Apache rewrite module to process search requests sent to its Web servers and redirect those requests to the appropriate server on the basis of information in the request URL. Example Inc. wants to simplify its setup by migrating these rules onto the NetScaler platform.

Several Apache rewrite rules that Example currently uses are shown below. These rules redirect search requests to a special results page if they do not have a SiteID string or if they have a SiteID string equal to zero (0), or to the standard results page if these conditions do not apply.

The following are the current Apache rewrite rules:

- RewriteCond %{REQUEST_FILENAME} ^/search$ [NC]
- RewriteCond %{QUERY_STRING} !SiteId= [OR]
- RewriteCond %{QUERY_STRING} SiteId=0
- RewriteCond %{QUERY_STRING} CallName=DisplayResults [NC]
- RewriteRule ^.*$ /results2.html [P,L]
- RewriteCond %{REQUEST_FILENAME} ^/search$ [NC]
- RewriteCond %{QUERY_STRING} CallName=DisplayResults [NC]
- RewriteRule ^.*$ /results.html [P,L]

To implement these Apache rewrite rules on the NetScaler, you would create rewrite actions with the values in the following tables.

Action Name	Type of Rewrite Action	Expression to choose target reference	String expression for replacement text
Action-Rewrite-Display_Results_NulSiteID	REPLACE	HTTP.REQ.URL	"/results2.html"
Action-Rewrite-Display_Results	REPLACE	HTTP.REQ.URL	"/results2.html"

You would then create rewrite policies with the values as shown in the tables below.

	Action Name	Undefined Action	Expression
ts_NulSiteID	Action-Rewrite-Display_Results_NulSiteID	NOREWRITE	HTTP.REQ.URL.PATH.SET_TEXT_MODE(IGNORECASE).EQ (!HTTP.REQ.URL.QUERY.CONTAINS("SiteId=") || HTTP.R HTTP.REQ.URL.QUERY.SET_TEXT_MODE(IGNORECASE).C

ts	Action-Rewrite-Display_Results	NOREWRITE	HTTP.REQ.URL.PATH.SET_TEXT_MODE(IGNORECASE).EQ HTTP.REQ.URL.QUERY.SET_TEXT_MODE(IGNORECASE).C

Finally, you would bind the rewrite policies, assigning the first a priority of 600 and the second a priority of 700, and then set the goto expression to NEXT for both bindings.

The NetScaler now handles these search requests exactly as the Web server did before the Apache rewrite module rules were migrated.

Example 7: Marketing Keyword Redirection

The marketing department at Example Inc. wants to set up simplified URLs for certain predefined keyword searches on the company's Web site. For these keywords, it wants to redefine the URL as shown below.

- External URL: `http://www.example.com/<marketingkeyword>`
- Internal URL: `http://www.example.com/go/kwsearch.asp?keyword=<marketingkeyword>`

To set up redirection for marketing keywords, you would create a rewrite action with the values in the following table.

Action Name	Type of Rewrite Action	Expression to choose target location	String expression for replacement text
Action-Rewrite-Modify_URL	INSERT_BEFORE	HTTP.REQ.URL.PATH.GET(1)	""go/kwsearch.aspkeyword="\"

You would then create a rewrite policy with the values in the following table.

Policy Name	Action Name	Undefined Action	Expression
Policy-Rewrite-Modify_URL	Action-Rewrite-Modify_URL	NOREWRITE	HTTP.REQ.HOSTNAME.SERVER.EQ("www.example.c

Finally, you would bind the rewrite policy, assigning it a priority of 800. Unlike the previous rewrite policies, this policy should be the last to be applied to a request that matches its criteria. For this reason, NetScaler administrator sets its Goto Priority Expression to END.

Any request using a marketing keyword is redirected to the keyword search CGI page, whereupon a search is performed and all remaining policies are skipped.

Example 8: Redirect Queries to the Queried Server

Example Inc. wants to redirect query requests to the appropriate server, as shown here.

- Request: `GET /query.cgi?server=5HOST: www.example.com`
- Redirect URL: `http://web-5.example.com/`

To implement this redirection, you would first create a rewrite action with the values in the following table.

on Name	Type of Rewrite Action	Expression to choose target reference	String expression for re
on-Rewrite-Replace_Hostheader	REPLACE	HTTP.REQ.HEADER("Host").BEFORE_STR(".example.com")	"server-" + HTTP.REQ.URL.QUERY.

You would then create a rewrite policy with the values in the following table.

icy Name	Action Name	Undefined Action	Expression
icy-Rewrite-Replace_Hostheader	Action-Rewrite-Replace_Hostheader	NOREWRITE	HTTP.REQ.HEADER("Host").EQ("www.exa

Finally, you would bind the rewrite policy, assigning it a priority of 900. Because this policy should be the last policy applied to a request that matches its criteria, you set the goto expression to END.

Incoming requests to any URL that begins with `http://www.example.com/query.cgi?server=` are redirected to the server number in the query.

Example 9: Home Page Redirection

New Company, Inc. recently acquired a smaller competitor, Purchased Company, and wants to redirect the home page for Purchased Company to a new page on its own Web site, as shown here.

- Old URL: `http://www.purchasedcompany.com/*`
- New URL: `http://www.newcompany.com/products/page.htm`

To redirect requests to the Purchased Company home page, you would create rewrite actions with the values in the following table.

Action Name	Type of Rewrite Action	Expression to choose target reference	String expression for replacement text
Action-Rewrite-Replace_URLr	REPLACE	HTTP.REQ.URL.PATH_AND_QUERY	"/products/page.htm"
Action-Rewrite-Replace_Host	REPLACE	HTTP.REQ.HOSTNAME	"www.newcompany.com"

You would then create rewrite policies with the values in the following table.

cy Name	Action Name	Undefined Action	Expression
cy-Rewrite-Replace-None	Action-Rewrite-Replace-None	NOREWRITE	!HTTP.REQ.HOSTNAME.SERVER.EQ("www.purchasedco
cy-Rewrite-Replace-Host	Action-Rewrite-Replace_Host	NOREWRITE	HTTP.REQ.HOSTNAME.SERVER.EQ("www.purchasedcon
cy-Rewrite-Replace-URL	Action-Rewrite-Replace_URL	NOREWRITE	HTTP.REQ.IS_VALID

Finally, you would bind the rewrite policies globally, assigning the first a priority of 100, the second a priority of 200, and the third a priority of 300. These policies should be the last policies applied to a request that matches the criteria. For this reason, set the goto expression to END for the first and third policies, and to 300 for the second policy. This ensures that all remaining requests are processed correctly.

Requests to the acquired company's old Web site are now redirected to the correct page on the New Company home page.

URL Transformation

The URL transformation feature provides a method for modifying all URLs in designated requests from an external version seen by outside users to an internal URL seen only by your Web servers and IT staff. You can redirect user requests seamlessly, without exposing your network structure to users. You can also modify complex internal URLs that users may find difficult to remember into simpler, more easily remembered external URLs.

Note: Before you can use the URL transformation feature, you must enable the Rewrite feature. To enable the Rewrite feature, see Enabling the Rewrite Feature.

To begin configuring URL transformation, you create profiles, each describing a specific transformation. Within each profile, you create one or more actions that describe the transformation in detail. Next, you create policies, each of which identifies a type of HTTP request to transform, and you associate each policy with an appropriate profile. Finally, you globally bind each policy to put it into effect.

Configuring URL Transformation Profiles

A profile describes a specific URL transformation as a series of actions. The profile functions primarily as a container for the actions, determining the order in which the actions are performed. Most transformations transform an external hostname and optional path into a different, internal hostname and path. Most useful transformations are simple and require only a single action, but you can use multiple actions to perform complex transformations.

You cannot create actions and then add them to a profile. You must create the profile first, and then add actions to it. In the CLI, creating an action and configuring the action are separate steps. Creating a profile and configuring the profile are separate steps in both the CLI and the configuration utility.

To create a URL transformation profile by using the NetScaler command line

At the NetScaler command prompt, type the following commands, in the order shown, to create a URL transformation profile and verify the configuration. You can then repeat the second and third commands to configure additional actions:

- add transform profile <profileName> -type URL [-onlyTransformAbsURLinBody (ON|OFF)] [-comment <comment>]
- add transform action <name> <profileName> <priority>
- set transform action <name> [-priority <priority>] [-reqUrlFrom <expression>] [-reqUrlInto <expression>] [-resUrlFrom <expression>] [-resUrlInto <expression>] [-cookieDomainFrom <expression>] [-cookieDomainInto <expression>] [-state (ENABLED|DISABLED)] [-comment "<string>"]
- show transform profile <name>

Example

```
> add transform profile shoppingcart -type URL
 Done
> add transform action actshopping shoppingcart 1000
 Done
> set transform action actshopping -priority 1000 -reqUrlFrom 'shopping.example.com' -reqUrlInto 'www.exar
 Done
> show transform profile shoppingcart
      Name: shoppingcart
            Type: URL       onlyTransformAbsURLinBody: OFF
      Comment:
      Actions:

1)            Priority 1000   Name: actshopping       ENABLED
```

Done

To modify an existing URL transformation profile or action by using the NetScaler command line

At the NetScaler command prompt, type the following commands to modify an existing URL transformation profile or action and verify the configuration:

Note: Use a set transform profile or set transform action command, respectively. The set transform profile command takes the same arguments as does the add transform profile command, and set transform action is the same command that was used for initial configuration.

- set transform action <name> [-priority <priority>] [-reqUrlFrom <expression>] [-reqUrlInto <expression>] [-resUrlFrom <expression>] [-resUrlInto <expression>] [-cookieDomainInto <expression>] [-state (ENABLED|DISABLED)] [-comment "<string>"]

- show transform profile <name>

Example

```
> set transform action actshopping -priority 1000 -reqUrlFrom 'searching.example.net' -reqUrlInto 'www.exar
 Done
> show transform profile shoppingcart
        Name: shoppingcart
              Type: URL       onlyTransformAbsURLinBody: OFF
        Comment:
        Actions:

1)              Priority 1000   Name: actshopping       ENABLED
 Done
```

To remove a URL transformation profile and actions by using the NetScaler command line

First remove all actions associated with that profile by typing the following command once for each action:

- rm transform action <name> After you have removed all actions associated with a profile, remove the profile as shown below.

- rm transform profile <name>

Parameters for configuring URL transformation profiles

profileName

A name for your new profile, or the name of the existing profile you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols.

onlyTransformAbsURLinBody

Transform only absolute URLs, not relative URLs, in HTTP body text. Possible values: YES, NO. Default: NO.

name

A name for your new action, or the name of the existing action you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols.

priority

The priority assigned to this URL transformation profile or action. Priorities assigned to profiles control the order in which matching URL transformation profiles are performed on a single request or response. Priorities assigned to actions control the order in which actions assigned to a single profile are performed.

reqUrlFrom

A PCRE-format regular expression that describes the request URL pattern to be transformed.

reqUrlInto

A PCRE-format regular expression that describes the transformation to be performed on the URLs in matching requests.

resUrlFrom

A PCRE-format regular expression that describes the response URL pattern to be transformed.

resUrlInto

A PCRE-format regular expression that describes the transformation to be performed on URLs in matching responses.

cookieDomainFrom

Pattern of the original domain in Set-Cookie headers.

cookieDomainInto

A PCRE-format regular expression that describes the transformation to be performed on cookies in matching requests and responses. The cookie domain to be transformed is extracted from the incoming request.

state

The state of a URL transformation action. (You can disable an action instead of removing it.) Possible values: ENABLED, DISABLED. Default: ENABLED.

comment

A text string, in quotation marks, that describes the purpose of this URL transformation action. This command is optional.

To create a URL transformation profile by using the configuration utility

1. In the navigation pane, expand Rewrite, expand URL Transformation, and then click Profiles.
2. In the details pane, click Add.
3. In the Create URL Transformation Profile dialog box, type or select values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring URL transformation profiles" as follows (asterisk indicates a required parameter):
   - Name*—name
   - Comment—comment
   - Only transform absolute URLs in response body—onlyTransformAbsURLinBody
4. Click Create, and then click Close. A message appears in the status bar, stating that the Profile has been configured successfully.

To configure a URL transformation profile and actions by using the configuration utility

1. In the navigation pane, expand Rewrite, expand URL Transformation, and then click Profiles.
2. In the details pane, select the profile you want to configure, and then click Open.
3. In the Configure URL Transformation Profile dialog box, do one of the following.
   - To create a new action, click Add.
   - To modify an existing action, select the action, and then click Open.
4. Fill in the Create URL Transformation Action or Modify URL Transformation Action dialog box by typing or selecting values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring URL transformation profiles" as follows (asterisk indicates a required parameter):
   - Action Name*—name
   - Comments—comment
   - Priority*—priority
   - Request URL from—reqUrlFrom
   - Request URL into—reqUrlInto
   - Response URL from—resUrlFrom
   - Response URL into—resUrlInto
   - Cookie Domain from—cookieDomainFrom
   - Cookie Domain into—cookieDomainInto
   - Enabled—state
5. Save your changes.
   - If you are creating a new action, click Create, and then Close.
   - If you are modifying an existing action, click OK.

   A message appears in the status bar, stating that the Profile has been configured successfully.
6. Repeat step 3 through step 5 to create or modify any additional actions.
7. To delete an action, select the action, and then click Remove. When prompted, click OK to confirm the deletion.
8. Click OK to save your changes and close the Modify URL Transformation Profile dialog box.

9. To delete a profile, in the details pane select the profile, and then click Remove. When prompted, click OK to confirm the deletion.

Configuring URL Transformation Policies

After you create a URL transformation profile, you next create a URL transformation policy to select the requests and responses that the NetScaler should transform by using the profile. URL transformation considers each request and the response to it as a single unit, so URL transformation policies are evaluated only when a request is received. If a policy matches, the NetScaler transforms both the request and the response.

Note: The URL transformation and rewrite features cannot both operate on the same HTTP header during request processing. Because of this, if you want to apply a URL transformation to a request, you must make sure that none of the HTTP headers it will modify are manipulated by any rewrite action.

To configure a URL transformation policy by using the NetScaler command line

You must create a new policy. On the command line, an existing policy can only be removed. At the NetScaler command prompt, type the following commands to configure a URL transformation policy and verify the configuration:

- add transform policy <name> <rule> <profileName>
- show transform policy <name>

Example

```
> add transform policy polsearch  HTTP.REQ.URL.SUFFIX.EQ("Searching") prosearching
 Done
> show transform policy polsearch
1)      Name: polsearch
        Rule: HTTP.REQ.URL.SUFFIX.EQ("Searching")
        Profile: prosearching
        Priority: 0
        Hits: 0
 Done
```

To remove a URL transformation policy by using the NetScaler command line

At the NetScaler command prompt, type the following command to remove a URL transformation policy:

rm transform policy <name>

Example

```
> rm transform policy polsearch
Done
```

Parameters for configuring URL transformation policies

name

A name for your new policy, or the name of the existing policy you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols.

rule

A NetScaler advanced expression that defines the rule for this policy. The expression can be a simple expression, or a complex expression that contains several expressions in a structured relationship.

profileName

The name of the profile to execute when a request or response matches this policy.

To configure a URL transformation policy by using the configuration utility

1. In the navigation pane, expand Rewrite, expand URL Transformation, and then click Policies.

2. In the details pane, do one of the following:

   - To create a new policy, click Add.

   - To modify an existing policy, select the policy, and then click Open.

3. In the Create URL Transformation Policy or Configure URL Transformation Policy dialog box, type or select values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring URL transformation policies" as follows (asterisk indicates a required parameter):

   - Name*—name (Cannot be changed for a previously configured policy.)

   - Profile*—profileName

   - Expression—rule

   If you want help with creating an expression for a new policy, you can either hold down the `Control key` and press the `space bar` while your cursor is in the Expression text box. To create the expression, you can type it directly as described below, or you can use the Add Expression dialog box as described in To add an expression by using the Add Expression dialog box.

   a. Click Prefix, and choose the prefix for your expression.

      Your choices are:

      - HTTP—The HTTP protocol. Choose this if you want to examine some aspect of the request that pertains to the HTTP protocol.

      - SYS—The protected Web site(s). Choose this if you want to examine some aspect of the request that pertains to the recipient of the request.

      - CLIENT—The computer that sent the request. Choose this if you want to examine some aspect of the sender of the request.

      - SERVER—The computer to which the request was sent. Choose this if you want to examine some aspect of the recipient of the request.

      - URL—The URL of the request. Choose this if you want to examine some aspect of the URL to which the request was sent.

      - TEXT—Any text string in the request. Choose this if you want to examine a text string in the request.

      - TARGET—The target of the request. Choose this if you want to examine some aspect of the request target.

        After you choose a prefix, the NetScaler displays a two-part prompt window that displays the possible next choices at the top, and a brief explanation of

what the selected choice means at the bottom. The choices depend on which prefix you chose.

b. Select your next term.

If you chose HTTP as your prefix, your choices are REQ, which specifies HTTP requests, and RES, which specifies HTTP responses. If you chose another prefix, your choices are more varied. For help on a specific choice, click that choice once to display information about it in the lower prompt window.

When you are certain which choice you want, double-click it to insert it into the Expression window.

c. Type a period, and then continue selecting terms from the list boxes that appear to the right of the previous list box. You type the appropriate text strings or numbers in the text boxes that appear to prompt you to enter a value, until your expression is finished.

4. Click Create or OK, depending on whether you are creating a new policy or modifying an existing policy.

5. Click Close. A message appears in the status bar, stating that the Policy has been configured successfully.

To add an expression by using the Add Expression dialog box

1. In the Create Responder Action or Configure Responder Action dialog box, click Add.
2. In the Add Expression dialog box, in the first list box choose the first term for your expression.

   HTTP

   The HTTP protocol. Choose this if you want to examine some aspect of the request that pertains to the HTTP protocol.

   SYS

   The protected Web site(s). Choose this if you want to examine some aspect of the request that pertains to the recipient of the request.

   CLIENT

   The computer that sent the request. Choose this if you want to examine some aspect of the sender of the request.

   SERVER

   The computer to which the request was sent. Choose this if you want to examine some aspect of the recipient of the request.

   URL

   The URL of the request. Choose this if you want to examine some aspect of the URL to which the request was sent.

   TEXT

   Any text string in the request. Choose this if you want to examine a text string in the request.

   TARGET

   The target of the request. Choose this if you want to examine some aspect of the request target.

   When you make your choice, the rightmost list box lists appropriate terms for the next part of your expression.

3. In the second list box, choose the second term for your expression. The choices depend upon which choice you made in the previous step, and are appropriate to the context. After you make your second choice, the Help window below the Construct Expression window (which was blank) displays help describing the purpose and use of the term you just chose.
4. Continue choosing terms from the list boxes that appear to the right of the previous list box, or typing strings or numbers in the text boxes that appear to prompt you to enter a

value, until your expression is finished.

Globally Binding URL Transformation Policies

After you have configured your URL transformation policies, you bind them to Global or a bind point to put them into effect. After binding, any a request or response that matches a URL transformation policy is transformed by the profile associated with that policy.

When you bind a policy, you assign a priority to it. The priority determines the order in which the policies you define are evaluated. You can set the priority to any positive integer. In the NetScaler OS, policy priorities work in reverse order - the higher the number, the lower the priority.

Because the URL transformation feature implements only the first policy that a request matches, not any additional policies that it might also match, policy priority is important for achieving the results that you intend. If you give your first policy a low priority (such as 1000), you tell the NetScaler to perform it only if other policies with a higher priority do not match a request. If you give your first policy a high priority (such as 1), you tell the NetScaler to perform it first, and skip any other policies that might also match. You can leave yourself plenty of room to add other policies in any order, without having to reassign priorities, by setting priorities with intervals of 50 or 100 between each policy when you globally bind your policies.

Note: URL transformation policies cannot be bound to TCP-based virtual servers.

To bind a URL transformation policy by using the NetScaler command line

At the NetScaler command prompt, type the following commands to globally bind a URL transformation policy and verify the configuration:

- bind transform global <policyName> <priority>
- show transform global

Example

```
> bind transform global polisearching 100
 Done
> show transform global
1)      Policy Name: polisearching
       Priority: 100

 Done
```

Parameters for binding URL transformation policies

policyName

The name of the URL transformation policy you want to bind.

priority

The priority assigned to this URL transformation policy. The priority determines the order in which policies are evaluated, allowing the NetScaler to evaluate the most specific policy first, and more general policies in descending order, finishing with the most general policy.

To bind a URL transformation policy by using the configuration utility

1. In the navigation pane, expand Rewrite, then expand URL Transformation, and then click Policies.
2. In the details pane, click Policy Manager.
3. In the Transform Policy Manager dialog box, choose the bind point to which you want to bind the policy. The choices are:
   - **Override Global.** Policies that are bound to this bind point process all traffic from all interfaces on the NetScaler appliance, and are applied before any other policies.
   - **LB Virtual Server.** Policies that are bound to a load balancing virtual server are applied only to traffic that is processed by that load balancing virtual server, and are applied before any Default Global policies. After selecting LB Virtual Server, you must also select the specific load balancing virtual server to which you want to bind this policy.
   - **CS Virtual Server.** Policies that are bound to a content switching virtual server are applied only to traffic that is processed by that content switching virtual server, and are applied before any Default Global policies. After selecting CS Virtual Server, you must also select the specific content switching virtual server to which you want to bind this policy.
   - **Default Global.** Policies that are bound to this bind point process all traffic from all interfaces on the NetScaler appliance.
   - **Policy Label.** Policies that are bound to a policy label process traffic that the policy label routes to them. The policy label controls the order in which policies are applied to this traffic.
4. Select Insert Policy to insert a new row and display a drop-down list with all available, unbound URL transformation policies.
5. Select the policy you want to bind, or select New Policy to create a new policy. The policy that you selected or created is inserted into the list of globally bound URL transformation policies.
6. Make any additional adjustments to the binding.
   - To modify the policy priority, click the field to enable it, and then type a new priority. You can also select Regenerate Priorities to renumber the priorities evenly.
   - To modify the policy expression, double click that field to open the Configure Transform Policy dialog box, where you can edit the policy expression.
   - To set the Goto Expression, double click field in the Goto Expression column heading to display the drop-down list, where you can choose an expression.
   - To set the Invoke option, double click field in the Invoke column heading to display the drop-down list, where you can choose an expression
7. Repeat steps 3 through 6 to add any additional URL transformation policies you want to globally bind.

8. Click OK to save your changes. A message appears in the status bar, stating that the Policy has been configured successfully.

Diameter Support for Rewrite

The Rewrite feature now supports the Diameter protocol. You can configure Rewrite to modify Diameter requests and response as you would HTTP or TCP requests and responses, allowing you to use Rewrite to manage the flow of Diameter requests and make necessary modifications. For example, if the "Origin-Host" value in a Diameter request is inappropriate, you can use Rewrite to replace it with a value that is acceptable to the Diameter server.

To configure Rewrite to modify a Diameter request

To configure the Rewrite feature to replace the Origin-Host in a diameter request with a different value, at the command prompt, type the following commands:

- add rewrite action <actname> replace "DIAMETER.REQ.AVP(264,\"netscaler.example.net\")"
  For <actname>, substitute a name for your new action. The name can consist of from one to 127 characters in length, and can contain letters, numbers, and the hyphen (-) and underscore (_) symbols. For netscaler.example.net, substitute the Host-Origin that you want to use instead of the original Host-Name.

- add rewrite policy <polname> "diameter.req.avp(264).value.eq(\"host.example.com\")" <actname>
  For <polname>, substitute a name for your new policy. As with <actname>, the name can consist of from one to 127 characters in length, and can contain letters, numbers, and the hyphen (-) and underscore (_) symbols. For host.example.com, substitute the name of the Host-Origin that you want to change. For <actname>, substitute the name of the action that you just created.

- bind lb vserver <vservername> -policyName <polname> -priority <priority> -type REQUEST
  For <vservername>, substitute the name of the load balancing virtual server to which you want to bind the policy. For <polname>, substitute the name of the policy you just created. For <priority>, substitute a priority for the policy.

Example

To create a Rewrite action and policy to modify all Diameter Host-Origins of "host.example.com" to "netscaler.example.net", you could add the following action and policy, and bind the policy as shown.

```
> add rewrite action rw_act_replace_avp replace "diameter.req.avp(264)" "diameter.new.avp(264,\"netscale
> add rewrite policy rw_diam_pol "diameter.req.avp(264).value.eq(\"client.realm2.net\")" rw_act_replace_a
> bind lb vserver vs1 -policyName rw_diam_pol -priority 10 -type REQUEST

Done
```

String Maps

You can use string maps to perform pattern matching in all NetScaler features that use the default policy syntax. A string map is a NetScaler entity that consists of key-value pairs. The keys and values are strings in either ASCII or UTF-8 format. String comparison uses two new functions, `MAP_STRING(<string_map_name>)` and `IS_STRINGMAP_KEY(<string_map_name>)`.

A policy configuration that uses string maps performs better than one that does string matching through policy expressions, and you need fewer policies to perform string matching with a large number of key-value pairs. String maps are also intuitive, simple to configure, and result in a smaller configuration.

How String Maps Work

String maps are similar in structure to pattern sets (a pattern set defines a mapping of index values to strings; a string map defines a mapping of strings to strings) and the configuration commands for string maps (commands such as add, bind, unbind, remove, and show) are syntactically similar to configuration commands for pattern sets. Also, as with index values in a pattern set, each key in a string map must be unique across the map. The following table illustrates a string map called url_string_map, which contains URLs as keys and values.

Table 1. String Map "url_string_map"

Key	Value
/url_1.html	http://www.redirect_url_1.com/url_1.html
/url_2.html	http://www.redirect_url_2.com/url_2.html
/url_3.html	http://www.redirect_url_1.com/url_1.html

The following table describes the two functions that have been introduced to enable string matching with keys in a string map. String matching is always performed with the keys. Additionally, the following functions perform a comparison between the keys in the string map and the complete string that is returned by the expression prefix. The examples in the descriptions refer to the preceding example.

Table 2. String Map Functions

nction	Description
EXT>.MAP_STRING(<string_map_name>)	Checks whether the value returned by the expression prefix TEXT matches a in the string map, and returns the value that corresponds to the key. If no ke map matches the value returned by the expression prefix, the function return string. The IGNORECASE and NOIGNORECASE functions can be used for case and case-sensitive comparison, respectively. **Example 1:** HTTP.REQ.URL.MAP_STRING("url_string_map") checks wh string returned by HTTP.REQ.URL is a key in the string map url_string_map. of HTTP.REQ.URL is /url_1.html, the function returns http://www.redirect_url_1.com/url_1.html. **Example 2:** HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).MAP_STRING("url_str checks whether the string returned by HTTP.REQ.URL is a key in the string r url_string_map. The comparison does not consider case. If the string returned HTTP.REQ.URL is /URL_1.html, the function returns http://www.redirect_url_1.com/url_1.html. **Parameters:** string_map_name - The string map.

EXT>.IS_STRINGMAP_KEY(<string_map_name>)	Returns TRUE if the string returned by the expression prefix TEXT is a key in map. The IGNORECASE and NOIGNORECASE functions can be used for case- and case-sensitive string matching, respectively. **Example 1:** HTTP.REQ.URL.IS_STRINGMAP_KEY("url_string_map") returns TRUE HTTP.REQ.URL is one of the keys in url_string_map. **Example 2:** HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE). IS_STRINGMAP_KEY("url_string_map") returns TRUE if the value of HT is one of the keys in url_string_map. In this case, key lookup does not conside Therefore, the function returns TRUE even if the value of HTTP.REQ.URL is /URL_3.html. **Parameters:** string_map_name - The string map.

Configuring a String Map

You first create a string map and then bind key-value pairs to it. You can create a string map from the command line interface (CLI) or the configuration utility.

To configure a string map by using the command line interface

At the command prompt, do the following:

1. Create a string map.

   add policy stringmap <name> -comment <string>

2. Bind a key-value pair to the string map.

   bind policy stringmap <name> <key> <value>

   Example:

   > bind policy stringmap url_string_map1 "/url_1.html" "http://www.redirect_url_1.com/url_1.html"

To configure a string map by using the configuration utility

Create a string map and bind the key-value pair to the created entity.

Navigate to AppExpert > String Maps,click Add and specify the relevant details.

String Maps Use Cases

You can use string maps in all features that support the newer default policy syntax. For example, string maps can be used in responder redirects and rewrite actions. You can also reuse a given string map in multiple features.

Use Case: Responder Policy With a Redirect Action

The following use case involves a responder policy with a redirect action. In the example below, the first four commands create the string map `url_string_map` and bind the three key-value pairs used in the earlier example. After creating the map and binding the key-value pairs, you create a responder action (`act_url_redirects`) that redirects the client to the corresponding URL in the string map or to `www.default.com`. You also configure a responder policy (`pol_url_redirects`) that checks whether requested URLs match any of the keys in `url_string_map` and then performs the configured action. Finally, you bind the responder policy to the content switching virtual server that receives the client requests that are to be evaluated.

```
add stringmap url_string_map

bind stringmap url_string_map /url_1.html
http://www.redirect_url_1.com/url_1.html

bind stringmap url_string_map /url_2.html
http://www.redirect_url_2.com/url_2.html

bind stringmap url_string_map /url_3.html
http://www.redirect_url_1.com/url_1.html

add responder action act_url_redirects redirect
'HTTP.REQ.URL.MAP_STRING("url_string_map") ALT "www.default.com"'
-bypassSafetyCheck yes

add responder policy pol_url_redirects TRUE act_url_redirects

bind cs vserver csw_redirect -policyname pol_url_redirects -priority
1 -type request
```

Security

2015-05-17 05:04:51 UTC

Contents

Security

The following topics cover configuration and installation information for NetScaler security features. Most of these features are policy based.

Authentication, Authorization, Auditing (AAA)	Keeps unauthorized users out of the network, denies users access to tasks for which they are not authorized, and tracks the resources used during user sessions.
Application Firewall	Prevents security breaches, data loss, and possible unauthorized modifications to web sites that access sensitive business or customer information.
Content Filtering	Blocks inappropriate HTML requests, preventing the requests from reaching the Web servers.
HTTP Denial-of-Service Protection	Prevents hackers from attacking your Web site with large numbers of HTTP requests.
Priority Queuing	Detects high-priority connections and allows those connections to proceed ahead of other connections, guaranteeing unimpeded access to those users.
SureConnect	Services all incoming connections with either the requested content or a custom Web page that displays information about a delay in the request being serviced.
Surge Protection	Detects any rapid rise in connection attempts and adjusts the rate at which connections are allowed to proceed to the server, preventing server overload.

AAA Application Traffic

Many companies restrict web site access to valid users only, and control the level of access permitted to each user. The AAA feature allows a site administrator to manage access controls with the NetScaler appliance instead of managing these controls separately for each application. Doing authentication on the appliance also permits sharing this information across all web sites within the same domain that are protected by the appliance.

The AAA feature supports authentication, authorization, and auditing for all application traffic. To use AAA, you must configure authentication virtual servers to handle the authentication process and traffic management virtual servers to handle the traffic to web applications that require authentication. You also configure your DNS to assign FQDNs to each virtual server. After configuring the virtual servers, you configure a user account for each user that will authenticate via the NetScaler appliance, and optionally you create groups and assign user accounts to groups. After creating user accounts and groups, you configure policies that tell the appliance how to authenticate users, which resources to allow users to access, and how to log user sessions. To put the policies into effect, you bind each policy globally, to a specific virtual server, or to the appropriate user accounts or groups. After configuring your policies, you customize user sessions by configuring session settings and binding your session policies to the traffic management virtual server. Finally, if your intranet uses client certs, you set up the client certificate configuration.

Before configuring AAA, you should be familiar with and understand how to configure load balancing, content switching, and SSL on the NetScaler appliance.

AAA Application Traffic

Many companies restrict web site access to valid users only, and control the level of access permitted to each user. The AAA feature allows a site administrator to manage access controls with the NetScaler appliance instead of managing these controls separately for each application. Doing authentication on the appliance also permits sharing this information across all web sites within the same domain that are protected by the appliance.

The AAA feature supports authentication, authorization, and auditing for all application traffic. To use AAA, you must configure authentication virtual servers to handle the authentication process and traffic management virtual servers to handle the traffic to web applications that require authentication. You also configure your DNS to assign FQDNs to each virtual server. After configuring the virtual servers, you configure a user account for each user that will authenticate via the NetScaler appliance, and optionally you create groups and assign user accounts to groups. After creating user accounts and groups, you configure policies that tell the appliance how to authenticate users, which resources to allow users to access, and how to log user sessions. To put the policies into effect, you bind each policy globally, to a specific virtual server, or to the appropriate user accounts or groups. After configuring your policies, you customize user sessions by configuring session settings and binding your session policies to the traffic management virtual server. Finally, if your intranet uses client certs, you set up the client certificate configuration.

Before configuring AAA, you should be familiar with and understand how to configure load balancing, content switching, and SSL on the NetScaler appliance.

How AAA Works

AAA provides security for a distributed Internet environment by allowing any client with the proper credentials to connect securely to protected application servers from anywhere on the Internet. This feature incorporates the three security features of authentication, authorization, and auditing. Authentication enables the NetScaler appliance to verify the client's credentials, either locally or with a third-party authentication server, and allow only approved users to access protected servers. Authorization enables the appliance to verify which content on a protected server it should allow each user to access. Auditing enables the appliance to keep a record of each user's activity on a protected server.

To understand how AAA works in a distributed environment, consider an organization with an intranet that its employees access in the office, at home, and when traveling. The content on the intranet is confidential and requires secure access. Any user who wants to access the intranet must have a valid user name and password. To meet these requirements, the NetScaler appliance does the following:

- Redirects the user to the login page if the user accesses the intranet without having logged in.
- Collects the user's credentials, delivers them to the authentication server, and caches them in a directory that is accessible through LDAP.
- Verifies that the user is authorized to access specific intranet content before delivering the user's request to the application server.
- Maintains a session timeout after which users must authenticate again to regain access to the intranet. (You can configure the timeout.)
- Logs the user accesses, including invalid login attempts, in an audit log.

Authentication requires that several entities—the client, the NetScaler appliance, the external authentication server if one is used, and the application server—respond to each other when prompted by performing a complex series of tasks in the correct order. If you are using an external authentication server, this process can be broken down into the following fifteen steps.

- The client sends a GET request for a URL on the application server.
- The NetScaler appliance's traffic management virtual server redirects the request to the application server.
- The application server determines that the client has not been authenticated, and therefore sends an HTTP 200 OK response via the TM vserver to the client. The response contains a hidden script that causes the client to issue a POST request for /cgi/tm.
- The client sends a POST request for /cgi/tm.
- The NetScaler appliance's authentication virtual server redirects the request to the authentication server.

- The authentication server creates an authentication session, sets and caches a cookie that consists of the initial URL and the domain of the traffic management virtual server, and then sends an HTTP 302 response via the authentication virtual server, redirecting the client to /vpn/index.html.
- The client sends a GET request for /vpn/index.html.
- The authentication virtual server redirects the client to the authentication server login page.
- The client sends a GET request for the login page, enters credentials, and then sends a POST request with the credentials back to the login page.
- The authentication virtual server redirects the POST request to the authentication server.
- If the credentials are correct, the authentication server tells the authentication virtual server to log the client in and redirect the client to the URL that was in the initial GET request.
- The authentication virtual server logs the client in and sends an HTTP 302 response that redirects the client to the initially requested URL.
- The client sends a GET request for their initial URL.
- The traffic management virtual server redirects the GET request to the application server.
- The application server responds via the traffic management virtual server with the initial URL.

If you use local authentication, the process is similar, but the authentication virtual server handles all authentication tasks instead of forwarding connections to an external authentication server. The following figure illustrates the authentication process.

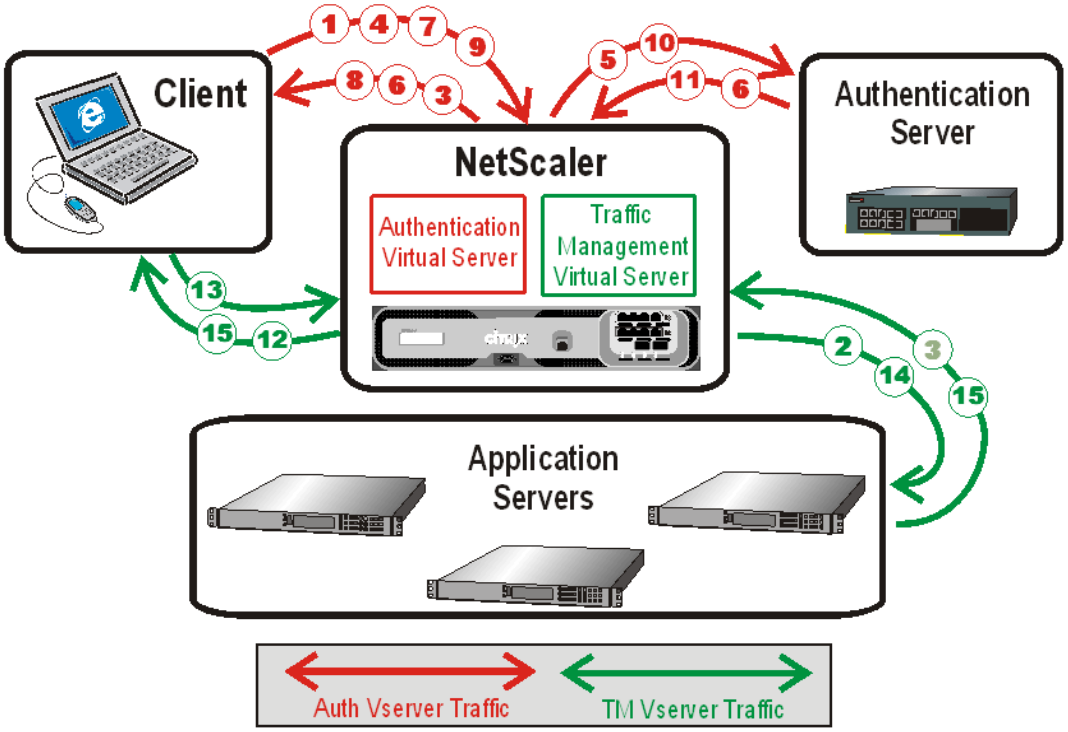


Figure 1. Authentication Process Traffic Flow

When an authenticated client requests a resource, the NetScaler appliance, before sending the request to the application server, checks the user and group policies associated with the client account, to verify that the client is authorized to access that resource. The appliance handles all authorization on protected application servers. You do not need to do any special configuration of your protected application servers.

AAA-TM handles password changes for users by using the protocol-specific method for the authentication server. For most protocols, neither the user nor the administrator needs to do anything different than they would without AAA-TM. Even when an LDAP authentication server is in use, and that server is part of a distributed network of LDAP servers with a single designated domain administration server, password changes are usually handled seamlessly. When an authenticated client of an LDAP server changes his or her password, the client sends a credential modify request to AAA-TM, which forwards it to the LDAP server. If the user's LDAP server is also the domain administration server, that server responds appropriately and AAA-TM then performs the requested password change. Otherwise, the LDAP server sends AAA-TM an LDAP_REFERRAL response to the domain administration server. AAA-TM follows the referral to the indicated domain administration server, authenticates to that server, and performs the password change on that server.

When configuring AAA-TM with an LDAP authentication server, the system administrator must keep the following conditions and limitations in mind:

- AAA-TM assumes that the domain administration server in the referral accepts the same bind credentials as the original server.
- AAA-TM only follows LDAP referrals for password change operations. In other cases AAA-TM refuses to follow the referral.
- AAA-TM only follows one level of LDAP referrals. If the second LDAP server also returns a referral, AAA-TM refuses to follow the second referral.

The NetScaler appliance supports auditing of all states and status information, so you can see the details of what each user did while logged on, in chronological order. To provide this information, the appliance logs each event, as it occurs, either to a designated audit log file on the appliance or to a syslog server. Auditing requires configuring the appliance and any syslog server that you use.

Enabling AAA

To use the AAA - Application Traffic feature, you must enable it. You can configure AAA entities—such as the authentication and traffic management virtual servers—before you enable the AAA feature, but the entities will not function until the feature is enabled.

To enable AAA by using the command line interface

At the command prompt, type the following commands to enable AAA and verify the configuration:

- enable ns feature AAA
- show ns feature

Example

```
> enable feature AAA
 Done

> show ns feature

      Feature                 Acronym           Status
      -------                 -------           ------
1)    Web Logging               WL                OFF
2)    Surge Protection          SP                ON
.
.
.
15)   AAA                     AAA               ON
.
.
.
23)   HTML Injection            HTMLInjection     ON
24)   NetScaler Push            push              OFF
Done
```

To enable AAA by using the configuration utility

1. Navigate to System > Settings.
2. In the details pane, under Modes and Features, click Change basic features.
3. In the Configure Basic Features dialog box, select the Authentication, Authorization and Auditing check box.
4. Click OK.

Setting up AAA Virtual Servers and DNS

You can configure AAA by using the built-in wizard, or manually. To use the wizard, in the main AAA pane of the configuration utility, you click AAA - Application Traffic wizard and follow the prompts.

To configure AAA manually, you first configure an authentication virtual server, which involves binding an SSL certificate-key pair. You then associate the authentication virtual server with a new or existing traffic management virtual server. (Either a load balancing virtual server or a content switching virtual server can serve as a traffic management virtual server.) To complete the initial configuration, you configure DNS to assign hostnames to both the authentication virtual server and the traffic management virtual server, and verify that your virtual servers are UP and configured correctly.

Caution: Both virtual servers must have hostnames in the same domain, or the AAA configuration will not work.

Configuring the Authentication Virtual Server

To configure AAA, first configure an authentication virtual server to handle authentication traffic. Next, bind an SSL certificate-key pair to the virtual server to enable it to handle SSL connections. For additional information about configuring SSL and creating a certificate-key pair, see the *Citrix NetScaler Traffic Management Guide* at "http://support.citrix.com/article/CTX132359."

To configure an authentication virtual server by using the command line interface

To configure an authentication virtual server and verify the configuration, at the command prompt type the following commands in the order shown:

- add authentication vserver <name> ssl <ipaddress>
- show authentication vserver <name>
- bind ssl certkey <sslkeyname> <name>
- show authentication vserver <name>
- set authentication vserver <name> -authenticationDomain <FQDN>
- show authentication vserver <name>

Example

```
> add authentication vserver Auth-Vserver-2 SSL 10.102.29.77 443
 Done
> show authentication vserver Auth-Vserver-2
      Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT
      State: DOWN[Certkey not bound]
      Client Idle Timeout: 180 sec
      Down state flush: DISABLED
      Disable Primary Vserver On Down : DISABLED
      Authentication : ON
      Current AAA Users: 0
 Done
> bind ssl certkey Auth-Vserver-2 Auth-Cert-1
 Done
> show authentication vserver Auth-Vserver-2
      Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT
      State: UP
      Client Idle Timeout: 180 sec
```

```
        Down state flush: DISABLED
        Disable Primary Vserver On Down : DISABLED
        Authentication : ON
        Current AAA Users: 0
        Authentication Domain: myCompany.employee.com
 Done
> set authentication vserver Auth-Vserver-2 -AuthenticationDomain myCompany.employee.com
 Done
> show authentication vserver Auth-Vserver-2
        Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT
        State: DOWN[Certkey not bound]
        Client Idle Timeout: 180 sec
        Down state flush: DISABLED
        Disable Primary Vserver On Down : DISABLED
        Authentication : ON
        Current AAA Users: 0
        Authentication Domain: myCompany.employee.com
 Done
```

Parameters for configuring the authentication virtual server

name

A name for your new authentication virtual server, or the name of an existing authentication virtual server. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. (Cannot be changed after the virtual server is created.)

ipaddress

IP address assigned to the authentication virtual server in DNS.

sslkeyname

Name of the SSL certificate-key pair to associate with the virtual server.

authenticationDomain

The fully qualified domain name to be assigned to the authentication virtual server in your DNS. Must match the domain name in the SSL certificate-key pair.

To configure an authentication virtual server by using the configuration utility

1. Navigate to Security > AAA - Application Traffic > Virtual Servers.
2. In the details pane, do one of the following:
   - To create a new authentication virtual server, click Add.
   - To modify an existing authentication virtual server, select the virtual server, and then click Open.
3. In the Create Virtual Server (Authentication) or Configure Virtual Server (Authentication) dialog box, specify values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring the authentication virtual server" as follows (asterisk indicates a required parameter):
   - Name*—name (Cannot be changed for a previously created virtual server)
   - IP Address*—ipaddress
   - Domain*—authenticationDomain

   Note: The authentication virtual server uses only the SSL protocol and port 443, so those options are greyed out.
4. On the Certificates tab, in the Available list, select the SSL certificate you want to associate with this authentication virtual server, and click the Add button. If your configuration requires CA certs and you will use this SSL certificate as the CA server certificate, you click the Add as CA button instead. The certificate moves from the Available to the Configured list.
5. Click Create or OK, and then click Close. If you created a new authentication virtual server, it now appears in the Authentication Virtual Servers pane.

Configuring a Traffic Management Virtual Server

After you have created and configured your authentication virtual server, you next create or configure a traffic management virtual server and associate your authentication virtual sever with it. You can use either a load balancing or content switching virtual server for a traffic management virtual server. For more information about creating and configuring either type of virtual server, see the *Citrix NetScaler Traffic Management Guide* at http://support.citrix.com/article/CTX132359Traffic Management.

Note: The FQDN of the traffic management virtual server must be in the same domain as the FQDN of the authentication virtual server for the domain session cookie to function correctly.

You configure a traffic management virtual server for AAA by enabling authentication and then assigning the FQDN of the authentication server to the traffic management virtual server. You can also configure the authentication domain on the traffic management virtual server at this time. If you do not configure this option, the NetScaler appliance assigns the traffic management virtual server an FQDN that consists of the FQDN of the authentication virtual server without the hostname portion. For example, if domain name of the authentication vserver is `tm.xyz.bar.com`, the appliance assigns `xyz.bar.com`. as the authentication domain.

To configure a TM virtual server for AAA by using the command line interface

At the command prompt, type one of the following sets of commands to configure a TM virtual server and verify the configuration:

- set lb vserver <name> –authentication ON -authenticationhost <FQDN> [-authenticationdomain <authdomain>]
- show lb vserver <name>
- set cs vserver <name> –authentication ON -authenticationhost <FQDN> [-authenticationdomain <authdomain>]
- show cs vserver <name>

Example

```
> set lb vserver vs-cont-sw -Authentication ON -AuthenticationHost mywiki.index.com
 Done
> show lb vserver vs-cont-sw
      vs-cont-sw (0.0.0.0:0) - TCP    Type: ADDRESS
```

```
        State: DOWN
        Last state change was at Wed Aug 19 10:03:15 2009 (+410 ms)
        Time since last state change: 5 days, 20:00:40.290
        Effective State: DOWN
        Client Idle Timeout: 9000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Connection Failover: DISABLED
        Authentication: ON      Host: mywiki.index.com
Done
```

Parameters for configuring a traffic management virtual server

name

The name of the load balancing or content switching virtual server being configured as a traffic management virtual server.

authentication

Toggle authentication of application traffic on the traffic management virtual server. Possible values: ON, OFF. Default: OFF.

authenticationhost

FQDN assigned to the authentication virtual server.

authenticationdomain

The common domain in the FQDNs of both the authentication virtual server and the traffic management virtual server.

To configure a TM virtual server for AAA by using the configuration utility

1. In the navigation pane, do one of the following.
   - Expand Load Balancing, and then click Virtual Servers.
   - Expand Content Switching, and then click Virtual Servers.

   The AAA configuration process for either type of virtual server is identical.
2. In the details pane, select the virtual server on which you want to enable authentication, and then click Open.
3. In the Domain text box, type the authentication domain. See `authenticationdomain`, in "Parameters for configuring a traffic management virtual server," for information about this parameter.
4. On the Advanced tab, select the Authentication check box.
5. In the Authentication Host text box, type the fully qualified domain name of the authentication virtual server. See authenticationhost in the table above for information about this parameter.
6. Click OK. A message appears in the status bar, stating that the vserver has been configured successfully.

Configuring DNS

For the domain session cookie used in the authentication process to function correctly, you must configure DNS to assign both the authentication and the traffic management virtual servers to FQDNs in the same domain. For information about how to the configure DNS address records, see the *Citrix NetScalerTraffic Management Guide* at "http://support.citrix.com/article/CTX132359."

Verifying Your Setup for AAA

After you configure authentication and traffic management virtual servers and before you create user accounts, you should verify that both virtual servers are configured correctly and are in the UP state.

To verify authentication virtual server setup by using the command line interface

At the command prompt, type the following command:

show authentication vserver <name>

Example

```
> show authentication vserver Auth-Vserver-2
      Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT
      State: UP
      Client Idle Timeout: 180 sec
      Down state flush: DISABLED
      Disable Primary Vserver On Down : DISABLED
      Authentication : ON
      Current AAA Users: 0
      Authentication Domain: myCompany.employee.com
 Done
```

Parameters for Verifying your Setup for AAA

State

Current state of the service or virtual server. Possible values:

UP – The virtual server can respond to requests. Your authentication virtual server should be UP.

OUT OF SERVICE – The virtual server has been manually disabled. New requests received by this virtual server are dropped unless a backup virtual server or HTTP redirection is configured.

DOWN – The virtual server cannot respond to requests. An authentication virtual server is DOWN when a valid SSL certificate-key pair is not bound to it.

Client Idle Timeout

Idle time (in seconds) after which client connections are terminated. Default value for HTTP/SSL-based services: 180.

Down state flush

Perform delayed cleanup of connections on this virtual server. Possible values: ENABLED, DISABLED. Default: ENABLED.

Disable Primary Vserver On Down

Keep the primary virtual server secondary, when it comes back up, until manually forced to take over as primary. If enabled, preserves database updates on the backup, enabling you to synchronize the databases before restoring the primary. Possible values: ENABLED, DISABLED. Default: DISABLED.

Authentication

Authenticate application traffic for the traffic management virtual server. Possible values: ON, OFF. Default: OFF. This value must be ON for AAA to function.

Current AAA Users

Number of AAA users configured. This number should be zero if you have just started to create a AAA configuration.

Authentication Domain

Authentication domain configured for the authentication virtual server.

Beneath this information are listed any policies bound globally or to this authentication virtual server, and their priorities.

To verify your AAA virtual server setup by using the configuration utility

1. In the navigation pane, expand AAA - Application Traffic, and then click Virtual Servers.
2. Review the information in the AAA Virtual Servers pane to verify that your configuration is correct and your authentication virtual server is accepting traffic. You can select a specific virtual server to view detailed information in the details pane.

   Note: For descriptions of what the information signifies, see the list above.

Configuring Users and Groups

After configuring the AAA basic setup, you create users and groups. You first create a user account for each person who will authenticate via the NetScaler appliance. If you are using local authentication controlled by the NetScaler appliance itself, you create local user accounts and assign passwords to each of those accounts.

You also create user accounts on the NetScaler appliance if you are using an external authentication server. In this case, however, each user account must exactly match an account for that user on the external authentication server, and you do not assign passwords to the user accounts that you create on the NetScaler. The external authentication server manages the passwords for users that authenticate with the external authentication server.

If you are using an external authentication server, you can still create local user accounts on the NetScaler appliance if, for example, you want to allow temporary users (such as visitors) to log in but do not want to create entries for those users on the authentication server. You assign a password to each local user account, just as you would if you were using local authentication for all user accounts.

Each user account must be bound to policies for authentication and authorization. To simplify this task, you can create one or more groups and assign user accounts to them. You can then bind policies to groups instead of individual user accounts.

To create a local AAA user account by using the command line interface

At the command prompt, type the following commands to create a local AAA user account and verify the configuration:

- add aaa user <username> [-password <password>]
- `show aaa user`

Example

```
> add aaa user user-2 -password emptybag
 Done
> show aaa user
1)      UserName: user-1
2)      UserName: user-2
 Done
```

To change the password for an existing AAA local user account by using the command line interface

At the command prompt, type the following command and, when prompted, type the new password:

set aaa user <username>

Example

```
> set aaa user user-2
Enter password:
Done
```

Parameters for Configuring AAA Local Users

username

A name for the user. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. (Cannot be changed for an existing user.)

password

A password that the user uses to log in. This parameter is required for all user accounts if you are not using an external authentication server. If you are using an external authentication server, you provide a password only for local user accounts that do not exist on the authentication server.

To configure AAA local users by using the configuration utility

1. In the navigation pane, expand AAA - Application Traffic, and then click Users.
2. In the details pane, do one of the following:
   - To create a new user account, click Add.
   - To modify an existing user account, select the user account, and then click Open.
3. In the Create AAA User dialog box, in the User Name text box, type a name for the user. For rules for user names, see the list above.
4. If creating a locally authenticated user account, clear the External Authentication check box and provide a local password that the user will use to log on.
5. Click Create or OK, and then click Close. A message appears in the status bar, stating that the user has been configured successfully.

To create AAA local groups and add users to them by using the command line interface

At the command prompt, type the following commands. Type the first command one time, and type the second command once for each user:

- add aaa group <groupname>
- show aaa group

  Example

```
> add aaa group group-2
Done
> show aaa group
1)      GroupName: group-1
2)      GroupName: group-2
Done
```

- bind aaa group <groupname> -username <username>

  Example

```
> bind aaa group group-2 -username user-2
 Done
> show aaa group group-2
        GroupName: group-2

                UserName: user-2
 Done
```

To remove users from an AAA group by using the command line interface

At the command prompt, unbind users from the group by typing the following command once for each user account that is bound to the group:

unbind aaa group <groupname> -username <username>

Example

```
> unbind aaa group group-hr -username user-hr-1
 Done
```

To remove an AAA group by using the command line interface

First remove all users from the group. Then, at the command prompt, type the following command to remove an AAA group and verify the configuration:

- rm aaa group <groupname>
- show aaa group

Example

```
> rm aaa group group-hr
 Done
> show aaa group
1)      GroupName: group-1
2)      GroupName: group-finance
 Done
```

Parameters for Configuring AAA Local Groups

groupname

A name for the group you are creating. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. (Cannot be changed for existing groups.)

username

The name of a user account to be added to the new group.

To configure AAA local groups and add users to them by using the configuration utility

1. In the navigation pane, expand AAA - Application Traffic, and then click Groups.
2. In the details pane, do one of the following:
   - To create a new group, click Add.
   - To modify an existing group, select the group, and then click Open.
3. If you are creating a new group, in the Create AAA Group dialog box, in the Group Name text box, type a name for the group. For information about group names, see the list above, under groupname.
4. On the Users tab, configure the users assigned to the group.
   a. To add a user to the group, in the Available Users list, select the user, and then click Add.
   b. To remove a user from the group, in the Configured Users list, select the user, and then click Remove.
   c. To create a new user account and add it to the group, click New, and then follow the instructions in “To configure AAA local users by using the configuration utility.”
5. Click Create or OK, and then click Close. The group that you created appears in the AAA Groups page.

Configuring AAA Policies

After you set up your users and groups, you next configure authentication policies, authorization policies, and audit policies to define which users are allowed to access your intranet, which resources each user or group is allowed to access, and what level of detail AAA will preserve in the audit logs. An authentication policy defines the type of authentication to apply when a user attempts to log on. If external authentication is used, the policy also specifies the external authentication server. Authorization policies specify the network resources that users and groups can access after they log on. Auditing policies define the audit log type and location.

You must bind each policy to put it into effect. You bind authentication policies to authentication virtual servers, authorization policies to one or more user accounts or groups, and auditing policies both globally and to one or more user accounts or groups.

When you bind a policy, you assign a priority to it. The priority determines the order in which the policies you define are evaluated. You can set the priority to any positive integer. In the NetScaler operating system, policy priorities work in reverse order: the higher the number, the lower the priority. For example, if you have three policies with priorities of 10, 100, and 1000, the policy assigned a priority of 10 is performed first, then the policy assigned a priority of 100, and finally the policy assigned an order of 1000. The AAA feature implements only the first of each type of policy that a request matches, not any additional policies of that type that a request might also match, so policy priority is important for getting the results you intend.

You can leave yourself plenty of room to add other policies in any order, and still set them to evaluate in the order you want, by setting priorities with intervals of 50 or 100 between each policy when you bind the policies. You can then add additional policies at any time without having to reassign the priority of an existing policy.

For additional information about binding policies on the NetScaler, see the *Citrix NetScaler Traffic Management Guide* at "http://support.citrix.com/article/CTX132359."

Authentication Policies

The NetScaler appliance can authenticate users with local user accounts or by using an external authentication server. The appliance supports the following authentication types:

LOCAL

Authenticates to the NetScaler by using a password, without reference to an external authentication server. User data is stored locally on the NetScaler appliance.

RADIUS

Authenticate to an external Radius server.

LDAP

Authenticates to an external LDAP authentication server.

TACACS

Authenticates to an external Terminal Access Controller Access-Control System (TACACS) authentication server.

Note: When authenticating through a TACACS server, AAA-TM logs only successfully executed TACACS commands, to prevent the logs from showing TACACS commands that were entered by users who were not authorized to execute them.

CERT

Authenticates to the NetScaler appliance by using a client certificate, without reference to an external authentication server.

NEGOTIATE

Authenticates to a Kerberos authentication server. If there is an error in Kerberos authentication, NetScaler uses NTLM authentication.

SAML

Authenticates to a server that supports the Security Assertion Markup Language (SAML).

An authentication policy is comprised of an expression and an action. Authentication policies use NetScaler expressions, which are described in detail in the *Citrix NetScaler Policy Configuration and Reference Guide* at "."

After creating an authentication action and an authentication policy, bind it to an authentication virtual server and assign a priority to it. When binding it, also designate it as either a primary or a secondary policy. Primary policies are evaluated before secondary policies. In configurations that use both types of policy, primary policies are normally more specific policies while secondary policies are normally more general policies intended to handle authentication for any user accounts that do not meet the more specific criteria.

To add an authentication action by using the command line interface

If you do not use LOCAL authentication, you need to add an explicit authentication action. To do this, at the command prompt, type the following command:

add authentication tacacsAction <name> -serverip <IP> [-serverPort <port>] [-authTimeout <positive_integer>] [...]

Example

```
> add authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -serverport 1812
            -authtimeout 15 -tacacsSecret "minotaur" -authorization OFF -accounting ON
            -auditFailedCmds OFF -defaultAuthenticationGroup "users"
Done
```

To configure an authentication action by using the command line interface

To configure an existing authentication action, at the command prompt, type the following command:

set authentication tacacsAction <name> -serverip <IP> [-serverPort <port>] [-authTimeout <positive_integer>] [...]

Example

```
> set authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -serverport 1812
            -authtimeout 15 -tacacsSecret "minotaur" -authorization OFF -accounting ON
            -auditFailedCmds OFF -defaultAuthenticationGroup "users"
Done
```

To remove an authentication action by using the command line interface

To remove an existing RADIUS action, at the command prompt, type the following command:

rm authentication radiusAction <name>

Example

```
> rm authentication tacacsaction Authn-Act-1
Done
```

Parameters for Configuring an Action

name

The name of the action. Called by the `-reqAction` option when configuring the matching policy.

-serverip <IP>

The IP the hosts the authentication server, in IPV4 or IPV6 format. The format is autodetected if configured at the command line.

-serverPort <port>

The port on which the authentication server accepts connections.

-authtimeout <timeout>

The timeout after which the authentication attempt will be deemed to have failed, and the user be notified.

In addition to the parameter listed above, each type of action has its own list of parameters that are specific to that action. For help with LDAP actions, see "LDAP Authentication Policies." For help with RADIUS actions, see "RADIUS Authentication Policies." For help with SAML actions, see "SAML Authentication Policies."

To configure an authentication server by using the configuration utility

Note: In the configuration utility, the term server is used instead of action, but refers to the same task.

1. Navigate to AAA - Application Traffic > Policies > Authentication, and then click the type of authentication you want to configure.
2. In the details pane, on the Servers tab, do one of the following:
   - To create a new authentication server, click Add.
   - To modify an existing authentication server, select the server, and then click Open.
3. In the Create Authentication Server or Configure Authentication Server dialog box, type or select values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring an action" as follows (asterisk indicates a required parameter):
   - Name*—radiusActionName (Cannot be changed for a previously configured action)
   - Authentication Type*—authtype (Set to RADIUS, cannot be changed)
   - IP Address*—serverip <IP>
   - IPV6*—Select the checkbox if the server IP is an IPv6 IP. (No command line equivalent.)

- Port*—serverPort
- Time-out (seconds)*—authTimeout

4. Click Create or OK, and then click Close. The policy that you created appears in the Authentication Policies and Servers page.

To create and bind an authentication policy by using the command line interface

At the command prompt, type the following commands in the order shown to create and bind an authentication policy and verify the configuration:

- add authentication negotiatePolicy <name> <rule> <reqAction>
- show authentication localPolicy <name>
- bind authentication vserver <name> -policy <policyname> [-priority <priority>] [-secondary]]
- show authentication vserver <name>

Example

```
> add authentication localPolicy Authn-Pol-1 ns_true
 Done

> show authentication localPolicy
1)      Name: Authn-Pol-1       Rule: ns_true
       Request action: LOCAL
 Done
> bind authentication vserver Auth-Vserver-2 -policy Authn-Pol-1
 Done
> show authentication vserver Auth-Vserver-2
       Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT
       State: UP
       Client Idle Timeout: 180 sec
       Down state flush: DISABLED
       Disable Primary Vserver On Down : DISABLED
       Authentication : ON
       Current AAA Users: 0
       Authentication Domain: myCompany.employee.com

1)             Primary authentication policy name: Authn-Pol-1 Priority: 0
 Done
```

To modify an existing authentication policy by using the command line interface

At the command prompt, type the following commands to modify an existing authentication policy:

set authentication localPolicy <name> <rule> [-reqaction <action>]

Example

```
> set authentication localPolicy Authn-Pol-1 'ns_true'
Done
```

To remove an authentication policy by using the command line interface

At the command prompt, type the following command to remove an authentication policy:

rm authentication localPolicy <name>

Example

```
> rm authentication localPolicy Authn-Pol-1
Done
```

Parameters for configuring authentication policies

authType

Type of authentication. Possible values: LOCAL, RADIUS, LDAP, TACACS, CERT, NEGOTIATE, SAML. Default value: LOCAL

Note: If you are creating an authentication policy for a RADIUS server, you must also create an authentication action. See To create and bind an authentication policy by using the command line interface for instructions.

name

A name for the policy you are creating. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. (Cannot be changed for existing policies.)

rule (expression)

An expression that defines the requests to be authenticated. For a complete description of NetScaler expressions, see the *Citrix NetScaler Policy Configuration and Reference Guide* at "http://support.citrix.com/article/CTX132362."

reqAction

The action associated with your policy. Leave this blank unless you are using an external authentication server that requires an action. If you are enabling LDAP referral support, see "Authentication Policies" for instructions. If you are creating an authentication policy for a RADIUS server, see "RADIUS Authentication Policies" for instructions. If you are creating an authentication policy for a SAML server, see "SAML Authentication Policies" for instructions.

authVsName

The name of the authentication virtual server to which you are binding this policy.

priority

The priority assigned to this authentication policy.

secondary

Designate this policy as a secondary authentication policy.

To configure and bind authentication policies by using the configuration utility

1. Navigate to Security > AAA - Application Traffic > Policies > Authentication, and then select the type of policy that you want to create.
2. In the details pane, on the Policies tab, do one of the following:
   - To create a new policy, click Add.
   - To modify an existing policy, select the action, and then click Open.
3. In the Create Authentication Policy or Configure Authentication Policy dialog box, type or select values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring authentication policies" as follows (asterisk indicates a required parameter):
   - Name*—policyname (Cannot be changed for a previously configured action)
   - Authentication Type*—authtype
   - Server*—authVsName
   - Expression*—rule (You enter expressions by first choosing the type of expression in the leftmost drop-down list beneath the Expression window, and then by typing your expression directly into the expression text area, or by clicking Add to open Add Expression dialog box and using the drop-down lists in it to construct your expression.)
4. Click Create or OK, and then click Close. The policy that you created appears in the Authentication Policies and Servers page.
5. Click the Servers tab, and in the details pane do one of the following:
   - To use an existing server, select it, and then click Open.
   - To create a new server, click Add, and follow the instructions in "Configuring the Authentication Virtual Server." If you are configuring a RADIUS authentication server, follow the instructions in "RADIUS Authentication Policies" If you are configuring a SAML authentication server, follow the instructions in "SAML Authentication Policies."
6. If you want to designate this policy as a secondary authentication policy, on the Authentication tab, click Secondary. If you want to designate this policy as a primary authentication policy, skip this step.
7. Click Insert Policy.
8. Choose the policy you want to bind to the authentication virtual server from the drop-down list.
9. In the Priority column to the left, modify the default priority as needed to ensure that the policy is evaluated in the proper order.
10. Click OK. A message appears in the status bar, stating that the policy has been configured successfully.

Authorization Policies

After you create authentication policies, you next create any authorization policies you need. Authorization policies, like other policies, consist of an expression and action. There are only two actions for authorization policies: ALLOW and DENY. ALLOW permits users to access the specified resource; DENY blocks access. The default setting for authorization when no specific policy exists is to deny access to network resources. This means that a user or group can access a particular resource only if an authorization policy explicitly allows access. For optimum security, the best practice is not to change the default setting and to create specific authorization policies for users who need access to specific resources.

Authorization use both default syntax expressions and classic expressions. These expressions are described in detail in the *Citrix NetScaler Policy Configuration and Reference Guide* at "http://support.citrix.com/article/CTX132362."

After you create an authorization policy, you bind it to the appropriate user accounts or groups to put it into effect.

To create an authorization policy

At the NetScaler command prompt, type the following commands to create an authorization policy and verify the configuration:

- add authorization policy <policyname> <rule> -action <action>
- show authorization policy <name>

Example

```
> add authorization policy authz-pol-1 "HTTP.REQ.URL.SUFFIX.EQ(\"gif\")" DENY
 Done
> show authorization policy authz-pol-1
1)      Name: authz-pol-1    Rule: HTTP.REQ.URL.SUFFIX.EQ("gif")
       Action: DENY
 Done
>
```

To modify an authorization policy

At the command prompt, type the following command to modify an authorization policy:

set authorization policy <policyname> [-rule <expression>] -action <action>

Example

```
> set authorization policy authz-pol-1 -rule "HTTP.REQ.URL.SUFFIX.EQ(\"gif\")" -action ALLOW
 Done
> show authorization policy authz-pol-1
1)      Name: authz-pol-1    Rule: HTTP.REQ.URL.SUFFIX.EQ("gif")
       Action: ALLOW
 Done
>
```

To bind an authorization policy to a user account or group

At the command prompt, type one of the following commands to bind an authorization policy to a user account or group and verify the configuration:

- bind aaa user <userName> [-policy <policyname> [-priority <priority]] [-intranetApplication <appname>] [-urlName <urlname>] [-intranetIP <intranetip> [<netmask>]]
- show aaa user <name>
- bind aaa group <groupName> [-policy <policyname> [-priority <priority]] [-intranetApplication <appname>] [-urlName <urlname>] [-intranetIP <intranetip> [<netmask>]]
- show aaa group <name>

Example

```
> bind aaa user user-hr-1 -policy authz-pol-1
  Done
> show aaa user user-hr-1
       UserName: user-hr-1

              Policy: authz-pol-1, Priority: 0
 Done
> bind aaa group group-1 -policy authz-pol-1
 Done
> show aaa group group-1
       GroupName: group-1

              UserName: user-2
              UserName: user-1

              Policy: authz-pol-1, Priority: 0
 Done
```

To unbind an authorization policy from a user account or group

At the command prompt, type one of the following commands to unbind an authorization policy from a user account or group:

- unbind aaa user <userName> -policy <policyname>
- unbind aaa group <groupName> -policy <policyname>

Example

```
> unbind aaa user aaa-user-1 -policy auth-pol-1
Done
```

To remove an authorization policy

First unbind the policy from all user accounts and groups, and then, at the NetScaler command prompt, type the following command to remove an authorization policy:

rm authorization policy <policyname>

Parameters for configuring authorization policies

policyname

A name for the authorization policy you are creating. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. (Cannot be changed for existing policies.)

rule

A NetScaler default syntax or classic syntax expression that defines which requests to allow or deny. For a complete description of NetScaler default syntax and classic syntax expressions, see the *Citrix NetScaler Policy Configuration and Reference Guide* at "http://support.citrix.com/article/CTX132362."

action

The action to perform when a connection matches the policy. Possible values: ALLOW, DENY. Default: ALLOW.

username or groupname

The name of the user account or the group to which you are binding the authorization policy.

priority

The priority you are assigning to the policy.

internetApplication

The name of the intranet application to which you are binding the authorization policy.

urlname

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

intranetip

The intranet IP of the intranet application to which you are binding the authorization policy.

netmask

If the intranet application to which you are binding the authorization policy resides on an IP range, the subnet mask of that intranet range.

To configure and bind authorization policies by using the configuration utility

1. In the navigation pane, expand AAA - Application Traffic, and then click Authorization.
2. In the details pane, do one of the following:
   - To create a new authorization policy, click Add.
   - To modify an existing authorization policy, select the policy, and then click Open.
3. In the Create Authorization Policy or Configure Authorization Policy dialog box, type or select values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring authorization policies" as follows (asterisk indicates a required parameter):
   - Name*—policyname(Cannot be changed for a previously configured policy.)
   - Action*— action
   - Expression*—rule (By default, the Expression box accepts default syntax policies. To switch to the classic syntax view, click Switch to Classic Syntax.)
4. Click Create or OK, and then click Close. The policy that you created appears on the Authorization Policies page.
5. To bind an authorization policy to a user account or group, in the navigation pane, under AAA - Application Traffic, click either Users or Groups, as appropriate, and then add that policy to the user account list:
   a. In the details pane, select the appropriate user account, and then click Open.
   b. Click the Authorization tab.
   c. Click Insert Policy.
   d. Choose the policy you want to bind to the group from the drop-down list.
   e. In the Priority column, modify the default priority as needed to ensure that the policy is evaluated in the proper order.
   f. Click OK.

   A message appears in the status bar, stating that the policy has been configured successfully.

Auditing Policies

After you create authentication policies, you next create any auditing policies you need. The NetScaler appliance allows auditing of all states and status information, so you can see the event history for any user in chronological order. When you configure auditing on the NetScaler appliance, you can choose to store the log files locally on the NetScaler appliance or to send them to a syslog server.

To put your auditing policies into effect, you bind them globally, to a specific authentication virtual server, or to specific user accounts or groups.

To create an auditing policy by using the command line interface

At the command prompt, type the following commands to create an auditing policy and verify the configuration:

- add audit nslogPolicy <name> [-rule <rule>] [-action <action>]
- show audit nslogPolicy

Example

```
> add audit nslogPolicy audit-1 ns_true audit_server
 Done
> show audit nslogPolicy
1)      Name: audit-pol Rule: ns_true
       Action: audit_server
2)      Name: audit-1   Rule: ns_true
       Action: audit_server
 Done
```

To modify an auditing policy by using the command line interface

At the command prompt, type the following commands to modify an auditing policy and verify the configuration:

- set audit nslogPolicy <name> [-rule <expression>] [-action <string>]
- show audit nslogPolicy

Example

```
> set audit nslogPolicy audit-1 ns_true audit_server
 Done
> show audit nslogPolicy
1)      Name: audit-pol Rule: ns_true
       Action: audit_server
2)      Name: audit-1    Rule: ns_true
       Action: audit_server
 Done
```

To globally bind an auditing policy by using the command line interface

At the command prompt, type the following commands to globally bind an auditing policy:

bind tm global [-policyName <string> [-priority <positive_integer>]]

Example

```
> bind tm global -policyName Audit-Pol-1 -priority 1000
Done
```

To bind an auditing policy to an authentication virtual server by using the command line interface

At the command prompt, type the following commands to bind an auditing policy to an authentication virtual server and verify the configuration:

- bind authentication vserver <name> [-policy <string> [-priority <positive_integer>] [-secondary] [-groupExtraction]]
- show authentication vserver [<name>]

Example

```
> bind authentication Vserver Auth-Vserver-2 -policy Authn-Pol-1
 Done
> show authentication Vserver Auth-Vserver-2
      Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT
      State: UP
      Client Idle Timeout: 180 sec
      Down state flush: DISABLED
      Disable Primary Vserver On Down : DISABLED
      Authentication : ON
      Current AAA Users: 0
      Authentication Domain: myCompany.employee.com
```

1) Primary authentication policy name: Authn-Pol-1 Priority: 0
Done

To bind an auditing policy to a user account or a group by using the command line interface

At the command prompt, type one of the following commands to bind an auditing policy to a user account or a group:

- bind audit <logtype> user <userName> -policy <policyname> [-priority <priority]
- bind audit <logtype> user <userName> -policy <policyname> [-priority <priority]

Example

> bind audit nslogPolicy user aaa-user-1 -policyName Audit-Pol-1 -priority 1000
Done

To unbind a globally bound auditing policy by using the command line interface

At the command prompt, type the following commands to unbind a globally-bound auditing policy:

unbind audit <logtype> global -policy <policyname>

Example

> unbind audit nslogPolicy global -policy Audit-Pol-1
Done

To unbind an auditing policy from an authentication virtual server by using the command line interface

At the command prompt, type the following commands to unbind an auditing policy from an authentication virtual server:

unbind authentication vserver <name> [-policy <string> [-secondary][-groupExtraction]]

Example

```
> unbind authentication vserver auth-vserver-1 -policyName Audit-Pol-1
Done
```

To unbind an auditing policy from a user account or a group by using the command line interface

At the command prompt, type one of the following commands to unbind an auditing policy from a user account or a group:

- unbind audit <logtype> user <userName> -policy <policyname>
- unbind audit <logtype> group <groupName> -policy <policyname>

Example

```
> unbind audit nslogPolicy group aaa-group-1 -policyName Audit-Pol-1
Done
```

To remove an auditing policy by using the command line interface

First unbind the policy from all users and groups, and then, at the command prompt, type the following command to remove an auditing policy:

rm audit <logtype> <policyname>

Parameters for configuring auditing policies

logtype

Which type of log your policy uses. If your policy logs to nslog, type nslogPolicy. If your policy logs to an external syslog server, type syslogPolicy.

policyname

A name for the policy you are creating. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. (Cannot be changed for existing policies.)

rule

A NetScaler classic expression that defines which requests to audit. If you do not specify a rule, audit policies default to ns_true, which logs all connections. For a complete description of NetScaler classic expressions, see the *Citrix NetScaler Policy Configuration and Reference Guide* at "http://support.citrix.com/article/CTX132362."

action

The action associated with this policy. For auditing policies, the action is the name of the nslog or syslog server to which you want to direct connections that match the audit log policy. If you do not specify a server, the default nslog server or syslog server is used.

authvsname

The name of the authentication virtual server to which you are binding the policy.

username

The name of the user account to which you are binding the policy.

groupname

The name of the group to which you are binding the policy.

priority

The priority assigned to this auditing policy.

To configure and bind auditing policies by using the configuration utility

1. In the navigation pane, expand AAA - Application Traffic, expand Policies, and then click Auditing.
2. In the details pane, do one of the following:
   - To create a new auditing policy, click Add.
   - To modify an existing auditing policy, select the policy, and then click Open.
3. In the Create Auditing Policy or Configure Auditing Policy dialog box, type or select values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring auditing policies" as follows (asterisk indicates a required parameter):
   - Name*—policyname (Cannot be changed for a previously configured policy.)
   - Auditing type*—logtype (When creating auditing policies by using the configuration utility, you cannot specify a rule.)
   - Server*—action
4. Click Create, and then click Close. The policy that you created appears in the Auditing Policies and Servers page.
5. Click OK.
6. To globally bind an auditing policy, in the details pane, click Global Bindings and fill in the Bind/Unbind Audit Policies to Global dialog box.
   a. Select the name of the audit policy you want to globally bind.
   b. Click OK.

   A message appears in the status bar, stating that the policy has been configured successfully.
7. To bind an auditing policy to an authentication virtual server, in the navigation pane, click Virtual Servers, and add that policy to the authentication policies list.
   a. In the details pane, select the appropriate virtual server, and then click Open.
   b. Click the Policies tab.
   c. Click Insert Policy.
   d. Choose the policy you want to bind to the authentication virtual server from the drop-down list.
   e. In the Priority column, modify the default priority as needed to ensure that the policy is evaluated in the proper order.
   f. Click OK.
8. To bind an auditing policy to a user account or group, in the navigation pane, click Users or Groups, and add that policy to the user account list.

a. In the details pane, select the appropriate user account, and then click Open.

b. Click the Policies tab.

c. Click Insert Policy.

d. Choose the policy you want to bind to the group from the drop-down list.

e. In the Priority column, modify the default priority as needed to ensure that the policy is evaluated in the proper order.

f. Click OK.

A message appears in the status bar, stating that the policy has been configured successfully.

Session Settings

After you configure your authentication, authorization, and auditing profiles, you configure session settings to customize your user sessions. The session settings are:

The session timeout.

Controls the period after which the user is automatically disconnected and must authenticate again to access your intranet.

The default authorization setting.

Determines whether the NetScaler appliance will by default allow or deny access to content for which there is no specific authorization policy.

The single sign-on setting.

Determines whether the NetScaler appliance will log users onto all web applications automatically after they authenticate, or will pass users to the web application logon page to authenticate for each application.

The credential index setting.

Determines whether the NetScaler appliance will use primary or the secondary authentication credentials for single signon.

To configure the session settings, you can take one of two approaches. If you want different settings for different user accounts or groups, you create a profile for each user account or group for which you want to configure custom sessions settings. You also create policies to select the connections to which to apply particular profiles, and you bind the policies to users or groups. You can also bind a policy to the authentication virtual server that handles the traffic to which you want to apply the profile.

If you want the same settings for all sessions, or if you want to customize the default settings for sessions that do not have specific profiles and policies configured, you can simply configure the global session settings.

Session Profiles

To customize your user sessions, you first create a session profile. The session profile allows you to override global settings for any of the session parameters.

Note: The terms “session profile” and “session action” mean the same thing.

To create a session profile by using the command line interface

At the command prompt, type the following commands to create a session profile and verify the configuration:

- add tm sessionAction <name> [-sessTimeout <mins>] [-defaultAuthorizationAction (ALLOW | DENY)] [-SSO (ON | OFF)] [-ssoCredential (PRIMARY | SECONDARY)] [-ssoDomain <string>] [-httpOnlyCookie (YES | NO)] [-persistentCookie (ENABLED | DISABLED)] [-persistentCookieValidity <minutes>]
- show tm sessionAction <name>

Example

```
> add tm sessionAction session-profile -sessTimeout 30 -defaultAuthorization ALLOW
 Done
> show tm sessionAction session-profile
1)      Name: session-profile
       Authorization action : ALLOW
       Session timeout: 30 minutes
 Done
```

To modify a session profile by using the command line interface

At the command prompt, type the following commands to modify a session profile and verify the configuration:

- set tm sessionAction <name> [-sessTimeout <mins>] [-defaultAuthorizationAction (ALLOW | DENY)] [-SSO (ON | OFF)] [-ssoCredential (PRIMARY | SECONDARY)] [-ssoDomain <string>] [-httpOnlyCookie (YES | NO)] [-persistentCookie (ENABLED | DISABLED)] [-persistentCookieValidity <minutes>]
- show tm sessionAction

Example

```
> set tm sessionAction session-profile -sessTimeout 30 -defaultAuthorization ALLOW
 Done
> show tm sessionAction session-profile
1)      Name: session-profile
       Authorization action : ALLOW
       Session timeout: 30 minutes
 Done
```

To remove a session profile by using the command line interface

At the command prompt, type the following command to remove a session profile:

rm tm sessionAction <name>

Parameters for configuring session profiles

actionname

A name for the session action, or the name of the existing session action you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. (Cannot be changed for existing session actions.)

sesstimeout

The session timeout in minutes. Possible values: 1-65536. Default: 30.

defaultAuthorizationAction

Whether to allow or deny access to resources by default when no specific policy overrides this setting. Possible values: ALLOW, DENY. Default: DENY

sso

Whether to use single sign-on or not for all web applications. Possible values: YES, NO. Default: NO.

ssocredential

Whether to use the primary or secondary authentication server for single sign-on credentials. Possible values: PRIMARY, SECONDARY. Default: PRIMARY.

ssoDomain

The domain for single sign-on, as a string.

httpOnlyCookie

Whether to set the HTTPOnly flag on the sso cookie. Possible values: YES, NO. Default: NO.

persistentCookie

Whether to use a persistent sso cookie. Possible values: ENABLED, DISABLED. Default: DISABLED.

persistentCookieValidity

The number of minutes, as an integer, that the persistent cookie remains valid.

To configure session profiles by using the configuration utility

1. In the navigation pane, expand AAA - Application Traffic, and then click Session.
2. In the details pane, click the Profiles tab.
3. On the Profiles tab, do one of the following:
   - To create a new session profile, click Add.
   - To modify an existing session profile, select the profile, and then click Open.
4. In the Create TM Session Profile dialog box, type or select values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring session profiles" as follows (asterisk indicates a required parameter):
   - Name*—actionname (Cannot be changed for a previously configured session action.)
   - Session Time-out—sesstimeout
   - Default Authorization Action—defaultAuthorizationAction
   - Single Signon to Web Applications—sso
   - Credential Index—ssocredential
   - Single Sign-on Domain—ssoDomain
   - HTTPOnly Cookie—httpOnlyCookie
   - Enable Persistent Cookie—persistentCookie
   - Persistent Cookie Validity—persistentCookieValidity
5. Click Create or OK, and then click Close. The session profile that you created appears in the Session Policies and Profiles pane.

Session Policies

After you create one or more session profiles, you create session policies and then bind the policies globally or to an authentication virtual server to put them into effect.

To create a session policy by using the command line interface

At the command prompt, type the following commands to create a session policy and verify the configuration:

- add tm sessionPolicy <policyname> <rule> <actionname>
- show tm sessionPolicy <name>

Example

```
> add tm sessionPolicy session-pol "URL == /*.gif" session-profile
 Done
> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/*.gif'
       Action: session-profile
 Done
```

To modify a session policy by using the command line interface

At the command prompt, type the following commands to modify a session policy and verify the configuration:

- set tm sessionPolicy <policyname> [-rule <expression>] [-action <action>]
- show tm sessionPolicy <name>

Example

```
> set tm sessionPolicy session-pol "URL == /*.gif" session-profile
 Done
> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/*.gif'
       Action: session-profile
 Done
```

To globally bind a session policy by using the command line interface

At the command prompt, type the following commands to globally bind a session policy and verify the configuration:

bind tm global -policyName <policyname> [-priority <priority>]

Example

```
> bind tm global -policyName session-pol
 Done

> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/*.gif'
       Action: session-profile
       Policy is bound to following entities
       1) TM GLOBAL    PRIORITY : 0
 Done
```

To bind a session policy to an authentication virtual server by using the command line interface

At the command prompt, type the following command to bind a session policy to an authentication virtual and verify the configuration:

bind authentication vserver <authvsname> -policy <policyname> [-priority <priority>]

Example

```
> bind authentication vserver auth-vserver-1 -policyName Session-Pol-1 -priority 1000
Done
```

To unbind a session policy from an authentication virtual server by using the command line interface

At the command prompt, type the following commands to unbind a session policy from an authentication virtual server and verify the configuration:

unbind authentication vserver <authvsname> -policy <policyname>

Example

```
> unbind authentication vserver auth-vserver-1 -policyName Session-Pol-1
Done
```

To unbind a globally bound session policy by using the command line interface

At the command prompt, type the following commands to unbind a globally-bound session policy:

unbind tm global -policyName <policyname>

Example

```
> unbind tm global -policyName Session-Pol-1
Done
```

To remove a session policy by using the command line interface

First unbind the session policy from global, and then, at the command prompt, type the following commands to remove a session policy and verify the configuration:

rm tm sessionPolicy <policyname>

Example

```
> rm tm sessionPolicy Session-Pol-1
Done
```

Parameters for configuring session policies

policyname

A name for the session policy, or the name of the existing session policy you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. (Cannot be changed for existing session policies.)

rule

A NetScaler classic expression that defines the requests to select. If you do not specify a rule, session profiles default to ns_true, which selects all connections. For a complete description of NetScaler classic expressions, see the *Citrix NetScaler Policy Configuration and Reference Guide* at "http://support.citrix.com/article/CTX132362."

actionname

The name of the session profile to apply to connections that match this policy.

priority

The priority assigned to this session policy.

authvsname

The name of the authentication virtual server to which you are binding this session policy.

To configure and bind session policies by using the configuration utility

1. In the navigation pane, expand AAA - Application Traffic, and then click Session.
2. In the details pane, on the Policies tab, do one of the following:
   - To create a new session policy, click Add.
   - To modify an existing session policy, select the policy, and then click Open.
3. In the Create Session Policy or Configure Session Policy dialog box, type or select values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring session policies" as follows (asterisk indicates a required parameter):
   - Name*—policyname (Cannot be changed for a previously configured session policy.)
   - Request Profile*—actionname
   - Expression*—rule (You enter expressions by first choosing the type of expression in the leftmost drop-down list beneath the Expression text area and then typing your expression directly into the expression text area, or by clicking Add to open the Add Expression dialog box and using the drop-down lists in it to construct your expression.)
4. Click Create or OK, and then click Close. The policy that you created appears in the details pane of the Session Policies and Profiles page.
5. To globally bind an auditing policy, in the details pane, click Global Bindings and fill in the Bind/Unbind Session Policies to Global dialog box.
   a. Select the name of the session policy you want to globally bind.
   b. Click OK.
6. To bind a session policy to an authentication virtual server, in the navigation pane, click Virtual Servers, and add that policy to the policies list.
   a. In the details pane, select the appropriate virtual server, and then click Open.
   b. Click the Policies tab.
   c. Click Insert Policy.
   d. Choose the policy you want to bind to the authentication virtual server from the drop-down list.
   e. In the Priority column to the left, modify the default priority as needed to ensure that the policy is evaluated in the proper order.
   f. Click OK.

A message appears in the status bar, stating that the policy has been configured successfully.

Global Session Settings

In addition to or instead of creating session profiles and policies, you can configure global session settings. These settings control the session configuration when there is no explicit policy overriding them.

To configure the session settings by using the command line interface

At the command prompt, type the following commands to configure the global session settings and verify the configuration:

set tm sessionParameter [-sessTimeout <mins>] [-defaultAuthorizationAction (ALLOW | DENY)] [-SSO (ON | OFF)] [-ssoCredential (PRIMARY | SECONDARY)] [-ssoDomain <string>] [-httpOnlyCookie (YES | NO)] [-persistentCookie (ENABLED | DISABLED)] [-persistentCookieValidity <minutes>]

Example

```
> set tm sessionParameter -sessTimeout 30
  Done
> set tm sessionParameter -defaultAuthorizationAction DENY
  Done
> set tm sessionParameter -SSO ON
  Done
> set tm sessionParameter -ssoCredential PRIMARY
  Done
```

Parameters for configuring global session settings

sessTimeout

The timeout for user sessions, as an integer value representing a number of minutes.

defaultAuthorizationAction

The default authorization action for a user request, when no specific policy is available. Possible values: ALLOW, DENY. Default: DENY.

sso

Whether to allow a user to authenticate once and then have access to all web applications on your intranet, or to require authentication for each application. Possible values: ON, OFF. Default: OFF.

ssoCredential

If single signon is enabled, which group of credentials to use for authentication. Possible values: Primary, Secondary. Default: Primary.

ssoDomain

The domain for single sign-on, as a string.

httpOnlyCookie

Whether to set the HTTPOnly flag on the sso cookie. Possible values: YES, NO. Default: NO.

persistentCookie

Whether to use a persistent sso cookie. Possible values: ENABLED, DISABLED. Default: DISABLED.

persistentCookieValidity

The number of minutes, as an integer, that the persistent cookie remains valid.

To configure the session settings by using the configuration utility

1. Navigate to Security > AAA - Application Traffic
2. In the details pane, under Settings, click Change global settings.
3. In the Global Session Settings dialog box, type or select values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring global session settings" as follows
   - Session Time-out—sessTimeout
   - Default Authorization Action—defaultAuthorizationAction
   - Single Sign-on to Web Applications—sso
   - Credential Index—ssoCredential
   - Single Sign-on Domain—ssoDomain
   - HTTPOnly Cookie—httpOnlyCookie
   - Enable Persistent Cookie—persistentCookie
   - Persistent Cookie Validity—persistentCookieValidity
4. Click OK, and then click Close. A message appears in the status bar, stating that the settings have been configured successfully.

Traffic Settings

If you use forms-based or SAML single sign-on (SSO) for your protected applications, you configure that feature in the Traffic settings. SSO enables your users to log on once to access all protected applications, rather than requiring them to log on separately to access each one.

Forms-based SSO allows you to use a web form of your own design as the sign-on method instead of a generic pop-up window. You can therefore put you company logo and other information you might want your users to see on the logon form. SAML SSO allows you to configure one NetScaler appliance or virtual appliance instance to authenticate to another NetScaler appliance on behalf of users who have authenticated with the first appliance.

To configure either type of SSO, you first create a forms or SAML SSO profile. Next, you create a traffic profile and link it to the SSO profile you created. Next, you create a policy, link it to the traffic profile. Finally, you bind the policy globally or to an authentication virtual server to put your configuration into effect.

Traffic Profiles

After creating at least one forms or SAML sso profile, you must next create a traffic profile.

Note: In this feature, the terms “profile” and “action” mean the same thing.

To create a traffic profile by using the command line interface

At the command prompt, type:

add tm trafficAction <name> [-appTimeout <mins>] [-SSO (ON | OFF) [-formSSOAction <string>]] [-persistentCookie (ENABLED | DISABLED)] [-InitiateLogout (ON | OFF)]

Example

add tm trafficAction Traffic-Prof-1 –appTimeout 10 -SSO ON -formSSOAction SSO-Prof-1

To modify a session profile by using the command line interface

At the command prompt, type:

set tm trafficAction <name> [-appTimeout <mins>] [-SSO (ON | OFF) [-formSSOAction <string>]] [-persistentCookie (ENABLED | DISABLED)] [-InitiateLogout (ON | OFF)]

Example

set tm trafficAction Traffic-Prof-1 –appTimeout 10 -SSO ON -formSSOAction SSO-Prof-1

To remove a session profile by using the command line interface

At the command prompt, type:

rm tm trafficAction <name>

Example

rm tm trafficAction Traffic-Prof-1

Parameters for configuring traffic profiles

name

A name for the traffic action, or the name of the existing traffic action you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. (Cannot be changed for existing SSO actions.)

appTimeout

The application timeout in minutes. Possible values: 1-65536. Default: 30.

SSO

Whether to enable or disable SSO. Possible values: ON, OFF. Default: OFF.

formSSOAction

The name of the form SSO profile to use. (Use this only if you are configuring a traffic profile for forms SSO.)

samlSSOAction

The name of the SAML SSO profile to use. (Use this only if you are configuring a traffic profile for SAML SSO.)

persistentCookie

Whether to use a persistent SSO cookie. Possible values: ENABLED, DISABLED. Default: DISABLED.

InitiateLogout

Whether to initiate logout of the traffic management session. Possible values: ON, OFF. Default: OFF.

To configure traffic profiles by using the configuration utility

1. Navigate to Security > AAA - Application Traffic > Traffic.
2. In the details pane, click the Profiles tab.
3. On the Profiles tab, do one of the following:
   - To create a new traffic profile, click Add.
   - To modify an existing traffic profile, select the profile, and then click Open.
4. In the Create Traffic Profile or Configure Traffic Profile dialog box, specify values for the parameters. The contents of the dialog box correspond to the parameters described in “Parameters for configuring form traffic profiles” as follows (an asterisk indicates a required parameter):
   - Name*—name (Cannot be changed for a previously configured session action.)
   - AppTimeout—appTimeout
   - Single Sign-On—SSO
   - Form SSO Action—formSSOAction
   - SAML SSO Action—samlSSOAction
   - Enable Persistent Cookie—persistentCookie
   - Initiate Logout—InitiateLogout
5. Click Create or OK, and then click Close. The traffic profile that you created appears in the Traffic Policies, Profiles, and either the Form SSO Profiles or SAML SSO Profiles pane, as appropriate.

Traffic Policies

After you create one or more form SSO and traffic profiles, you create traffic policies and then bind the policies, either globally or to an authentication virtual server, to put them into effect.

To create a traffic policy by using the command line interface

At the command prompt, type:

add tm trafficPolicy <name> <rule> <action>

Example

add tm trafficPolicy Traffic-Pol-1 "HTTP.REQ.HEADER("Cookie").CONTAINS("login=true")" Traffic-Prof-1

To modify a traffic policy by using the command line interface

At the command prompt, type:

set tm trafficPolicy <name> <rule> <action>

Example

set tm trafficPolicy Traffic-Pol-1 "HTTP.REQ.HEADER("Cookie").CONTAINS("login=true")" Traffic-Prof-1

To globally bind a traffic policy by using the command line interface

At the command prompt, type:

bind tm global -policyName <string> [-priority <priority>]

Example

bind tm global -policyName Traffic-Pol-1

To bind a traffic policy to an authentication virtual server by using the command line interface

At the command prompt, type:

bind authentication vserver <name> -policy <policyName> [-priority <priority>]

Example

bind authentication vserver auth-vserver-1 -policyName Traffic-Pol-1 -priority 1000

To unbind a globally bound traffic policy by using the command line interface

At the command prompt, type:

unbind tm global -policyName <policyname>

Example

unbind tm global -policyName Traffic-Pol-1

To unbind a traffic policy from an authentication virtual server by using the command line interface

At the command prompt, type:

unbind authentication vserver <name> -policy <policyname>

Example

unbind authentication vserver auth-vserver-1 -policyName Traffic-Pol-1

To remove a traffic policy by using the command line interface

First unbind the session policy from global, and then, at the command prompt, type:

rm tm trafficPolicy <name>

Example

rm tm trafficPolicy Traffic-Pol-1

Parameters for configuring form traffic profiles

policyName

A name for the traffic policy, or the name of the existing traffic policy you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. (Cannot be changed for existing SSO actions.)

rule

A NetScaler advanced expression that defines the requests to select. For a complete description of NetScaler advanced expressions, see the *Citrix NetScaler Policy Configuration and Reference Guide* at http://support.citrix.com/article/CTX132362.

actionname

The name of the traffic profile to apply to connections that match this policy.

priority

The priority assigned to this traffic policy.

authvsname

The name of the authentication virtual server to which you are binding this traffic policy.

To configure and bind traffic policies by using the configuration utility

1. In the navigation pane, expand AAA - Application Traffic, then expand Policies, and then click Traffic.

2. In the details pane, do one of the following:

   - To create a new session policy, click Add.

   - To modify an existing session policy, select the policy, and then click Open.

3. In the Create Traffic Policy or Configure Traffic Policy dialog box, specify values for the parameters. The contents of the dialog box correspond to the parameters described in “Parameters for configuring form traffic profiles” as follows (an asterisk indicates a required parameter):

   - Name*—policyName (Cannot be changed for a previously configured session policy.)

   - Profile*—actionName

   - Expression—rule (You enter expressions by first choosing the type of expression in the leftmost drop-down list beneath the Expression text area and then typing your expression directly into the expression text area, or by clicking Add to open the Add Expression dialog box and using the drop-down lists in it to construct your expression.)

4. Click Create or OK, and then click Close. The policy that you created appears in the details pane of the Session Policies and Profiles page.

5. To globally bind a traffic policy, in the details pane, click Global Bindings and fill in the Bind/Unbind Session Policies to Global dialog box.

   a. Select the name of the traffic policy you want to globally bind.

   b. Click OK.

6. To bind a traffic policy to an authentication virtual server, in the navigation pane, click Virtual Servers, and add that policy to the policies list.

   a. In the details pane, select the appropriate virtual server, and then click Open.

   b. Click the Policies tab

   c. Click Insert Policy.

   d. Choose the policy you want to bind to the authentication virtual server from the drop-down list.

   e. In the Priority column to the left, modify the default priority as needed to ensure that the policy is evaluated in the proper order.

   f. Click OK.

Form SSO Profiles

To enable and configure forms-based SSO, you first create an SSO profile.

Note: In this feature, the terms “profile” and “action” mean the same thing.

To create a form SSO profile by using the command line interface

At the command prompt, type:

add tm formSSOAction <name> -actionURL <URL> -userField <string> -passwdField <string> -ssoSuccessRule <expression> [-nameValuePair <string>] [-responsesize <positive_integer>] [-nvtype (STATIC | DYNAMIC)] [-submitMethod (GET | POST)

Example

add tm formSSOAction SSO-Prof-1 -actionURL "/logon.php"
-userField "loginID" -passwdField "passwd"
-nameValuePair "loginID passwd" -responsesize "9096"
-ssoSuccessRule "HTTP.RES.HEADER("Set-Cookie").CONTAINS("LogonID")"
-nvtype STATIC -submitMethod GET
–sessTimeout 10 -defaultAuthorizationAction ALLOW

To modify a form SSO by using the command line interface

At the command prompt, type:

set tm formSSOAction <name> -actionURL <URL> -userField <string> -passwdField <string> -ssoSuccessRule <expression> [-nameValuePair <string>] [-responsesize <positive_integer>] [-nvtype (STATIC | DYNAMIC)] [-submitMethod (GET | POST)

Example

set tm formSSOAction SSO-Prof-1 -actionURL "/logon.php"
-userField "loginID" -passwdField "passwd"
-ssoSuccessRule "HTTP.RES.HEADER("Set-Cookie").CONTAINS("LogonID")"
-nameValuePair "loginID passwd" -responsesize "9096"
-nvtype STATIC -submitMethod GET
–sessTimeout 10 -defaultAuthorizationAction ALLOW

To remove a form SSO profile by using the command line interface

At the command prompt, type:

rm tm formSSOAction <name>

Example

rm tm sessionAction SSO-Prof-1

Parameters for configuring form SSO profiles

name

A name for the SSO action, or the name of the existing SSO action you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. (Cannot be changed for existing SSO actions.)

actionURL

The URL where the SSO logon form is located.

userField

The form field where the user types in the user ID or login.

passwdField

The form field where the user types in the password.

ssoSuccessRule

An expression that describes the action that this profile should take when invoked by a policy.

responsesize

The number of bytes to allow for the complete response size. Responses that exceed this value are blocked.

nameValuePair

The userField value, followed by a space, followed by the passwdField value. When typing this at the NetScaler command line, you should enclose the nameValuePair in straight double quotes.

nvtype

Whether the name/value pair is static or dynamic. Possible values: STATIC, DYNAMIC. Default: STATIC.

submitMethod

HTTP method used by the SSO logon form to send the logon credentials to the logon server. Possible values: GET, POST. Default: POST.

To configure form SSO profiles by using the configuration utility

1. Navigate to Security > AAA - Application Traffic > Policies > Traffic.
2. In the details pane, click the Form SSO Profiles tab.
3. On the Form SSO Profiles tab, do one of the following:
   - To create a new form SSO profile, click Add.
   - To modify an existing form SSO profile, select the profile, and then click Open.
4. In the Create Form SSO Profile dialog box, specify values for the parameters. The contents of the dialog box correspond to the parameters described in “Parameters for configuring form SSO profiles” as follows (an asterisk indicates a required parameter):
   - Name*—name (Cannot be changed for a previously configured session action.)
   - Action URL*—actionURL
   - User Name Field*—userField
   - Password Field*—passField
   - SSO Success Rule*—ssoSuccessRule
   - Name Value Pair—nameValuePair
   - Response Size—responsesize
   - Extraction—nvtype
   - Submit Method—submitMethod
5. Click Create or OK, and then click Close. The form SSO profile that you created appears in the Traffic Policies, Profiles, and Form SSO Profiles pane.

Authenticating with Client Certificates

Web sites that contain sensitive content, such as online banking web sites or Web sites with employee personal information, sometimes require client certificates for authentication. To configure AAA to authenticate users on the basis of client-side certificate attributes, you first enable client authentication on the traffic management virtual server and bind the root certificate to the authentication virtual server. Then, you implement one of two options. You can configure the default authentication type on the authentication virtual server as CERT, or you can create a certificate action that defines what the NetScaler appliance must do to authenticate users on the basis of a client certificate. In either case, your authentication server must support CRLs. You configure the NetScaler appliance to extract the user name from the SubjectCN field or another specified field in the client certificate.

When the user tries to log in to an authentication virtual server for which an authentication policy is not configured, and a global cascade is not configured, the user name information is extracted from the specified field of the certificate. If the required field is extracted, the authentication succeeds. If the user does not provide a valid certificate during the SSL handshake, or if the user name extraction fails, authentication fails. After it validates the client certificate, the NetScaler appliance presents a login page to the user.

The following procedures assume that you have already created a functioning AAA configuration, and therefore they explain only how to enable authentication by using client certificates. These procedures also assume that you have obtained your root certificate and client certificates and have placed them on the NetScaler appliance in the /nsconfig/ssl directory.

To configure the AAA client certificate parameters by using the command line interface

At the command prompt, type the following commands in the order shown and verify the configuration:

- add ssl certKey <certkeyName> -cert <certFile> -key <keyFile> -password -inform <inform> -expiryMonitor <expiryMonitor> -notificationPeriod <notificationPeriod>
- bind ssl certKey <certkeyName> -vServer <certkeyName> -CA -crlCheck Mandatory
- set aaa parameter -defaultAuthType CERT
- set aaa certParams -userNameField "Subject:CN"

Parameters for authentication with client certificates

certkeyName

The name of the certificate-key pair.

certFile

The name of the file containing the certificate.

keyFile

The name of the file containing the private key.

password

The password to the private key. If you are entering this at the NetScaler command line, you simply include the -password parameter, and then, after entering the command, enter the actual password when prompted. If you are using the configuration utility, you type the password in the appropriate text box.

inform

The format of the certificate-key pair. Possible values: DER, PEM. Default: PEM.

expiryMonitor

Whether to monitor the certificate-key pair for expiration. Possible values: ENABLED, DISABLED. Default: ENABLED.

notificationPeriod

The period, in days before the certificate-key pair expires, during which the NetScaler appliance should notify the administrator of the impending expiration.

vservername

The name of the authentication virtual server to which to bind the root certificate.

To configure the AAA client certificate parameters by using the configuration utility

1. Navigate to Security > AAA - Application Traffic > Virtual Servers.
2. In the details pane, select the virtual server that you want to configure to handle client certificate authentication, and then click Open.
3. In the Configure Virtual Server (Authentication) dialog box, in the Certificates tab, click Install.
4. In the Install Certificate dialog box, type or select values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for authentication with client certificates" as follows (asterisk indicates a required parameter):
   - Certificate-Key Pair Name*—certkeyName
   - Certificate File Name—certFile
   - Private Key File Name—keyFile
   - Password—password
   - Certificate Format—inform
   - Notify When Expires—expiryMonitor
   - Notification Period—notificationPeriod
5. Click Install, and then click Close.
6. In the Configure Virtual Server (Authentication) dialog box, in the Available list, select the root certificate.
7. Click Add as CA.
8. Click OK.
9. In the navigation pane, expand Policies, and then click Authentication.
10. In the details pane, select the policy you want to configure to handle client certificate authentication, and then click Open.
11. In the Authentication Type drop-down list, select CERT.
12. In the Server drop-down list, select the virtual server you just configured to handle client certificate authentication.
13. Click OK. A message appears in the status bar, stating that the configuration completed successfully.

Configuring AAA with Commonly Used Protocols

Configuring the NetScaler for Authentication, Authorization, and Auditing (AAA) needs a specific setup on the NetScaler and clients' browsers. The configuration varies with the protocol used for AAA.

For more information about configuring the NetScaler for Kerberos authentication, see Handling Authentication, Authorization and Auditing with Kerberos/NTLM.

Handling Authentication, Authorization and Auditing with Kerberos/NTLM

Kerberos, a computer network authentication protocol, provides secure communication over the Internet. Designed primarily for client-server applications, it provides for mutual authentication by which the client and server can each ensure the other's authenticity. Kerberos uses a trusted third party, referred to as Key Distribution Center (KDC). A KDC consists of an Authentication Server (AS), which authenticates a user, and a Ticket Granting Server (TGS).

Each entity on the network (client or server) has a secret key that is known only to itself and the KDC. The knowledge of this key implies authenticity of the entity. For communication between two entities on the network, the KDC generates a session key, referred to as the *Kerberos ticket* or *service ticket*. The client makes a request to the AS for credentials for a specific server. The client then receives a ticket, referred to as *Ticket Granting Ticket (TGT)*. The client then contacts the TGS, using the TGT it received from the AS to prove its identity, and asks for a service. If the client is eligible for the service, the TGS issues a Kerberos ticket to the client. The client then contacts the server hosting the service (referred to as the *service server*), using the Kerberos ticket to prove that it is authorized to receive the service. The Kerberos ticket has a configurable lifetime. The client authenticates itself with the AS only once. If it contacts the physical server multiple times, it reuses the AS ticket.

The following figure shows the basic functioning of the Kerberos protocol.

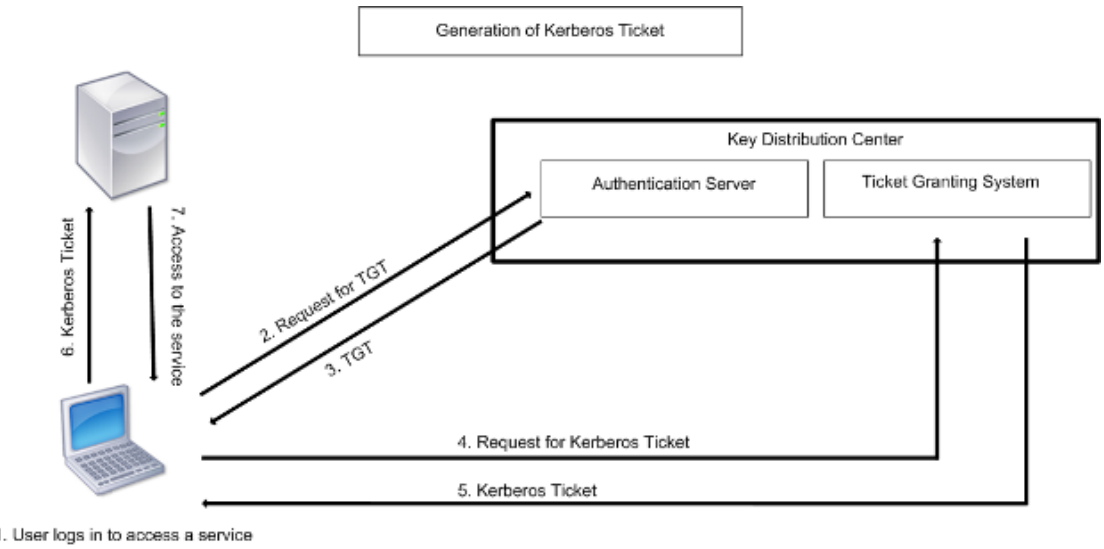


Figure 1. **Functioning of Kerberos**

Kerberos authentication has the following advantages:

- Faster authentication. When a physical server gets a Kerberos ticket from a client, the server has enough information to authenticate the client directly. It does not have to contact a domain controller for client authentication, and therefore the authentication process is faster.

- Mutual authentication. When the KDC issues a Kerberos ticket to a client and the client uses the ticket to access a service, only authenticated servers can decrypt the Kerberos ticket. If the virtual server on the NetScaler is able to decrypt the Kerberos ticket, you can conclude that both the virtual server and client are authenticated. Thus, the authentication of the server happens along with the authentication of the client.

- Single sign-on between Windows and other operating systems that support Kerberos.

Kerberos authentication may have the following disadvantages:

- Kerberos has strict time requirements; the clocks of the involved hosts must be synchronized with the Kerberos server clock to ensure that the authentication does not fail. You can mitigate this disadvantage by using the Network Time Protocol daemons to keep the host clocks synchronized. Kerberos tickets have an availability period, which you can configure.

- Kerberos needs the central server to be available continuously. When the Kerberos server is down, no one can log on. You can mitigate this risk by using multiple Kerberos servers and fallback authentication mechanisms.

- Because all the authentication is controlled by a centralized KDC, any compromise in this infrastructure, such as the user's password for a local workstation being stolen, can allow an attacker to impersonate any user. You can mitigate this risk to some extent by using only a desktop machine or laptop that you trust, or by enforcing preauthentication by means of a hardware-token.

To use Kerberos authentication, you must configure it on the NetScaler appliance and on each client.

How NetScaler Implements Kerberos Authentication

Note: Kerberos/NTLM authentication is supported only in the NetScaler 9.3 nCore release or later, and it can be used only for AAA traffic management (AAA-TM) virtual servers.

NetScaler handles the components involved in Kerberos authentication in the following way:

Key Distribution Center (KDC)

In the Windows 2000 Server or later versions, the Domain Controller and KDC are part of the Windows Server. If the Windows Server is UP and running, it indicates that the Domain Controller and KDC are configured. The KDC is also the Active Directory server.

Note: All Kerberos interactions are validated with the Windows Kerberos Domain Controller.

Authentication Service and Protocol Negotiation

A NetScaler appliance supports Kerberos authentication on the AAA-TM authentication virtual servers. If the Kerberos authentication fails, the NetScaler uses the NTLM authentication.

By default, Windows 2000 Server and later Windows Server versions use Kerberos for AAA. If you create an authentication policy with NEGOTIATE as the authentication type, the NetScaler attempts to use the Kerberos protocol for AAA and if the client's browser fails to receive a Kerberos ticket, the NetScaler uses the NTLM authentication. This process is referred to as *negotiation*.

The client may fail to receive a Kerberos ticket in any of the following cases:

- Kerberos is not supported on the client.
- Kerberos is not enabled on the client.
- The client is in a domain other than that of the KDC.
- The Access Directory on the KDC is not accessible to the client.

For Kerberos/NTLM authentication, the NetScaler does not use the data that is present locally on the NetScaler appliance.

Authorization

The traffic management virtual server can be a load balancing virtual server or a content switching virtual server.

Auditing

The NetScaler appliance supports auditing of Kerberos authentication with the following audit logging:

- Complete audit trail of the traffic management end-user activity
- SYSLOG and high performance TCP logging
- Complete audit trail of system administrators
- All system events
- Scriptable log format

Supported Environment

Kerberos authentication does not need any specific environment on the NetScaler. The client (browser) must provide support for Kerberos authentication.

High Availability

In a high availability setup, only the active NetScaler joins the domain. In case of a failover, the NetScaler lwagent daemon joins the secondary NetScaler appliance to the domain. No specific configuration is required for this functionality.

Kerberos Authentication Process

The following figure shows a typical process for Kerberos authentication in the NetScaler environment.

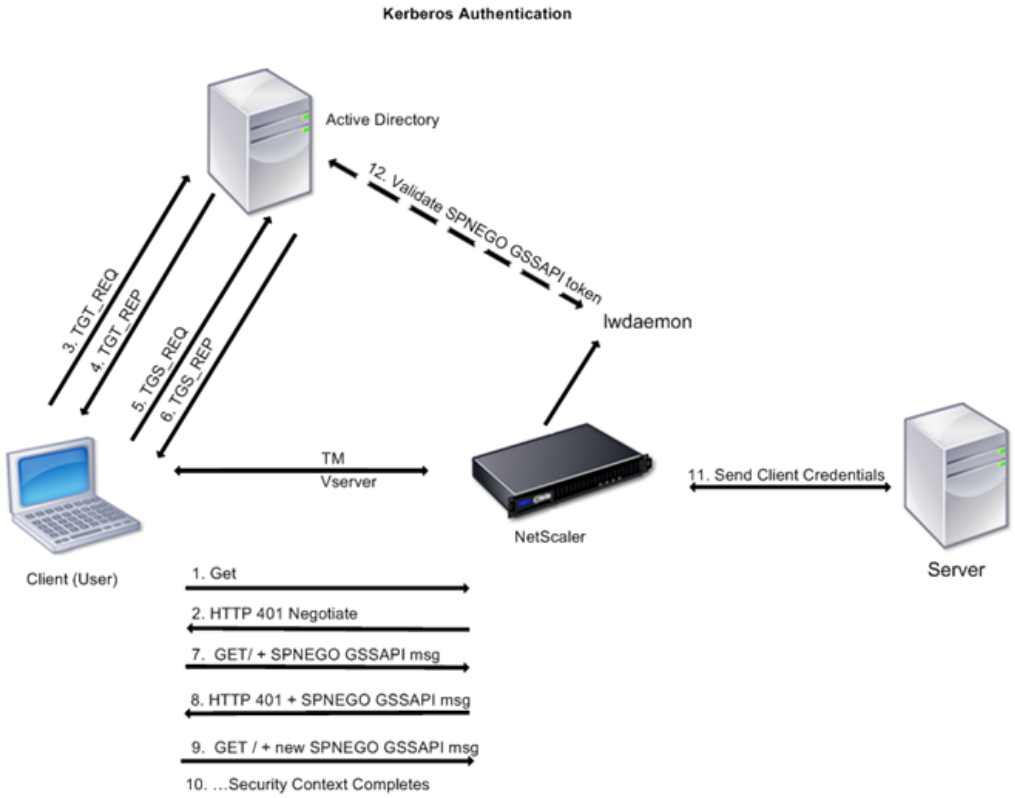


Figure 1. Kerberos Authentication Process on NetScaler

The Kerberos authentication occurs in the following stages:

Client authenticates itself to the KDC.

1. The NetScaler appliance receives a request from a client.
2. The traffic management (load balancing or content switching) virtual server on the NetScaler sends a challenge to the client.
3. To respond to the challenge, the client gets a Kerberos ticket.
    - The client sends the Authentication Server of the KDC a request for a ticket-granting ticket (TGT) and receives the TGT. (See 3, 4 in the figure, Kerberos Authentication Process.)
    - The client sends the TGT to the Ticket Granting Server of the KDC and receives a Kerberos ticket. (See 5, 6 in the figure, Kerberos Authentication Process.)

Note: The above authentication process is not necessary if the client already has a Kerberos ticket whose lifetime has not expired. In addition, clients such as Web Services, .NET, or J2EE, which support SPNEGO, get a Kerberos ticket for the target server, create an SPNEGO token, and insert the token in the HTTP header when they send an HTTP request. They do not go through the client authentication process.

Client requests a service.

1. The client sends the Kerberos ticket containing the SPNEGO token and the HTTP request to the traffic management virtual server on the NetScaler. The SPNEGO token has the necessary GSSAPI data.
2. The NetScaler establishes a security context between the client and the NetScaler. If the NetScaler cannot accept the data provided in the Kerberos ticket, the client is asked to get a different ticket. This cycle repeats till the GSSAPI data is acceptable and the security context is established. The traffic management virtual server on the NetScaler acts as an HTTP proxy between the client and the physical server.

NetScaler completes the authentication.

1. After the security context is complete, the traffic management virtual server validates the SPNEGO token.
2. From the valid SPNEGO token, the virtual server extracts the user ID and GSS credentials, and passes them to the authentication daemon.
3. A successful authentication completes the Kerberos authentication.

Kerberos Authentication - Configuration on the NetScaler Appliance

To configure Kerberos authentication on the NetScaler appliance, perform the following tasks:

1. Enable the Authentication, Authorization, and Auditing (AAA) feature on the NetScaler appliance.

2. On the Active Directory, add a user for Kerberos authentication, map the HTTP service to this user, and generate a keytab file and import it to the NetScaler appliance. You can map more than one service if the Kerberos authentication is required for more than one service. The keytab file should contain entries for every service that is bound to the traffic management virtual server on the NetScaler. The keytab file is necessary for decrypting the secret received from the client during Kerberos authentication. The authentication details of all the services are stored in a single keytab file on the NetScaler.

3. Add a DNS server.

   Note: The NetScaler must obtain the IP address of the domain controller from the fully qualified domain name (FQDN). Therefore, Citrix recommends configuring the NetScaler with a DNS server. A less preferred alternative is to create a static DNS entry.

4. Create an authentication negotiation policy with a negotiation action.

5. Configure an authentication server and bind the authentication policy to the authentication virtual server.

6. Configure an authentication service and a traffic management virtual server, and bind the service to the virtual server. You can use either a load balancing or a content switching virtual server.

7. Verify the configuration.

Enabling AAA on the NetScaler

Enable authentication of the traffic on the NetScaler appliance.

To enable Authentication, Authorization, and Auditing (AAA) by using the command line interface

At the command prompt, type the following commands to enable AAA and verify the configuration:

- enable ns feature AAA
- show ns feature

Example

```
> enable feature aaa
 Done
> show ns feature
 Feature Acronym Status
 ------- ------- ------
1) Web Logging WL ON
 …
3) Load Balancing LB ON
4) Content Switching CS ON
5) Cache Redirection CR ON
 …
14) SSL VPN SSLVPN ON
15) AAA AAA ON
 …
26) CloudBridge CloudBridge OFF
 Done
```

To enable Authentication, Authorization, and Auditing (AAA) on NetScaler by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features, click Configure basic features.
3. In the Configure Basic Features dialog box, select the Authentication, Authorization and Auditing check box.
4. Click OK.
5. In the confirmation dialog box, click Yes. A message appears in the status bar to indicate that the feature is enabled.

Adding a Keytab file

The keytab file contains information about services necessary for Kerberos authentication. The keytab file is necessary for decrypting the secret received from the client during Kerberos authentication. You can map more than one service if the Kerberos authentication is required for more than one service. The keytab file should contain entries for every service that is bound to the traffic management virtual server on the NetScaler. The authentication details of all the services are stored in a single keytab file on the NetScaler.

To generate a keytab file and import it to the NetScaler appliance, follow the procedure described below:

Note: You can generate the keytab file and import it onto the NetScaler only from the command line.

1. Log onto the Active Directory server and create a user for Kerberos authentication.

   For example, type the following command:

   net user Kerb-SVC-Account freebsd!@#456 /add

2. In the User Properties section, ensure the following settings:

   - The Change password at next logon option is not selected.
   - The Password does not expire option is selected.

3. Map the HTTP service to the above user and export the keytab file. For example, run the following command on the Active Directory server:

   ktpass /out keytabfile /princ HTTP/owa.newacp.com@NEWACP.COM /pass freebsd!@#456 /mapuser newacp\dummy /ptype KRB5_NT_PRINCIPAL

   Note: If you want to map more services, repeat the above command for every service. You can give the same name or different names for the output file.

4. Transfer the keytab file to the NetScaler by using the unix ftp command or any other file transfer utility of your choice.

5. Log onto the NetScaler appliance, and run the ktutil utility to verify the keytab file. The keytab file has an entry for the HTTP service after it is imported.

Example

```
root@ns# ktutil
ktutil: rkt /var/keytabfile
ktutil: list
slot KVNO Principal
----------------------------------------------------------------------
```

```
ktutil: wkt /etc/ krb5.keytab
ktutil: list
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
1 2 HTTP/owa.newacp.com@NEWACP.COM
ktutil: quit
```

Adding a DNS Server

The NetScaler appliance should obtain the IP address of the domain controller from the fully qualified domain name (FQDN). Therefore, Citrix recommends configuring the NetScaler with a DNS server. A less preferred alternative is to create a static DNS entry.

To add a DNS server by using the command line interface

At the command prompt, type the following command:

add dns nameserver <IP>

Note: Alternatively, you can add static host entries or use any other means so that the NetScaler can resolve the FQDN name of the domain controller to an IP address.

Example

add dns nameserver 1.2.3.4

Parameters for configuring the DNS server

dnsIpAddress

The IP address of the name server that is used to resolve domain names to IP addresses.

To add a DNS server by using the NetScaler configuration utility

1. In the navigation pane, expand DNS, and then click Name Servers.
2. In the details pane, click Add.
3. In the IP Address box, type the IP address.
4. Click Create, and then Close.
5. Verify that the details pane shows the newly added DNS server.

Creating an Authentication Negotiation Policy

Create a negotiation policy with a negotiation action for Kerberos authentication of services.

To create an authentication negotiation policy by using the command line interface

At the command prompt, type the following commands:

- add authentication negotiateAction <name> -domain <domainName> -domainUser <domainUsername> -domainUserPasswd <domainUserPassword> -encrypted
- add authentication negotiatePolicy <negotiatePolicyName> <negotiatePolicyExpression> <negotiateActionName>

Example

```
add authentication negotiateAction negact -domain newacp.com -domainUser Administrator -domainUserPas
add authentication negotiatePolicy negopol ns_true negact
```

Parameters for creating an authentication negotiation policy

negotiateActionName

The name of the negotiate action associated with the negotiate policy.

domainName

The fully qualified domain name in which the client and KDC are present.

domainUsername

The user name of the user who can access the domain.

domainUserPassword

The password of the user who can access the domain.

negotiatePolicyName

A name for the policy you are creating. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. (Cannot be changed for existing policies.)

negotiatePolicyExpression

A policy expression that defines the requests to be authenticated.

To create an authentication negotiation policy by using the NetScaler configuration utility

1. In the navigation pane, expand AAA-Application Traffic, expand Policies, and then click Authentication.
2. In the details pane, on the Policies tab, click Add.
3. In the Create Authentication Policy dialog box, set the following parameters:
   - Name
   - Authentication Type - Select NEGOTIATE.
   - Server - Select an existing server from the dropdown list. To add a new authentication server, click New…, and in the Create Authentication Server dialog box, set the following parameters:
     - Domain Name
     - User Name
     - Password
     - Confirm Password - Retype the password.
   - Expression - In the Named Expression list, select General and select True Value from the dropdown list, and then click Add Expression.
4. Click Create, and then click Close.
5. Verify that the policy you created appears in the Authentication Policies and Servers pane.

Creating an Authentication Virtual Server

Configure an authentication virtual server and bind the authentication negotiation policy to the authentication virtual server.

To create an authentication virtual server and bind the negotiation policy by using the command line interface

At the command prompt, type the following commands:

- add authentication vserver <name> SSL <ipAuthVserver> 443 -authenticationDomain <domainName>
- bind authentication vserver <name> -policy <negotiatePolicyName>

Example

```
add authentication vserver authen1 SSL 10.102.113.166 443 -authenticationDomain newacp.com
add ssl certKey cert1 -cert "/nsconfig/ssl/complete/server/server_rsa_2048.pem" -key "/nsconfig/ssl/compl
bind ssl vserver authen1 -certkeyName cert1
bind authentication vserver authen1 -policy negopol
```

Parameters for configuring an authentication virtual server and binding the negotiation policy

authVserverName

A name for the new authentication virtual server. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. (Cannot be changed after the virtual server is created.)

ipAuthVserver

The IP address of the authentication virtual server.

domainName

The fully qualified domain name in which the client and KDC are present. This domain is assigned to the authentication virtual server.

negotiatePolicyName

A name for the policy you are creating. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. (Cannot be changed for existing policies.)

To create an authentication virtual server and bind the negotiation policy by using the NetScaler configuration utility

1. In the navigation pane, expand AAA - Application Traffic and click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Authentication) dialog box, set the following parameters:
   - Name
   - IP Address
   - Protocol - Select SSL
   - Domain - Type the fully qualified domain name added while creating the keytab file.

   Note: For AAA, the protocol must be SSL protocol and port must be 443. Therefore, these options are not provided.
4. On the Authentication tab, click Insert Policy. In the Authentication Policies group, from the Policy Name dropdown list, select the negotiate authentication policy you added for Kerberos authentication.
5. On the Certificates tab, select an SSL certificate from the list of available certificates, and then click Add. If the certificate you want to bind is not displayed in the Available Certificates list, click Install..., and then select the certificate file.
6. Click Create, and then click Close. The new authentication virtual server appears in the Authentication Virtual Servers pane.

Configuring a Traffic Management Virtual Server

Configure an authentication service and a traffic management virtual server, and bind the service to the virtual server. You can use either a load balancing or a content switching virtual server.

To create a traffic management virtual server and service, and bind the service by using the command line interface

At the command prompt, type the following commands:

- add service <name>@ <ipBackendWebserver> HTTP 80
- add lb vserver <name>@ SSL <ipAddressLbVserver> 443 -authn401 ON -authnVsName <authVserverName>
- bind lb vserver <name>@ <serviceName>

Note: Use a similar procedure for using a content switching virtual server as the traffic management virtual server.

Example

```
add service svc1 10.217.28.92 HTTP 80
 add lb vserver v2 HTTP 10.102.113.164 80 -persistenceType NONE -cltTimeout 180 -authn401 ON -authnVsNa
bind lb vserver v2 svc1
```

Parameters for configuring the traffic management virtual server

serviceName

Name of the service. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

ipBackendWebServer

IP address of the Web server used in backend communication.

lbVserverName

Name of the load balancing virtual server used as the traffic management virtual server.

csVserverName

Name of the content switching virtual server used as the traffic management virtual server.

ipAddressLbVserver

IP address of the load balancing virtual server.

ipAddressCsVserver

IP address of the content switching virtual server.

authVserverName

Name of the authentication virtual server associated with the traffic management virtual server.

To create a traffic management virtual server and service, and bind the service by using the NetScaler configuration utility

1. In the navigation pane, expand Load Balancing and click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, set the following parameters:
   - Service Name
   - Server
   - Protocol - Select HTTP.
   - Port - Select 80.
4. In the navigation pane, expand Load Balancing and click Virtual Servers.
5. In the details pane, click Add.
6. In the Create Virtual Server (Load balancing) dialog box, set values for the following parameters:
   - Name
   - IP Address

- Protocol
- Port

7. In the Create Virtual Server (Load balancing) dialog box, on the Services tab, select the service you created in Step 3 to Step 5.
8. In the Create Virtual Server (Load balancing) dialog box, on the Advanced tab, expand Authentication Settings, and then select the 401 Based Authentication check box.
9. Click Create, and then click Close. The new load balancing virtual server appears in the Load Balancing Virtual Servers pane.
10. In the details pane, verify the settings of the virtual server.

Note: Use a similar procedure to create a content switching virtual server.

Note: For more information, see Setting up basic load balancing.

Verifying the configuration for Kerberos Authentication

Ensure that you completed the following tasks and verify whether the configuration is complete and correct.

- Enable the AAA feature
- Import the keytab file
- Configure the DNS server
- Configure negotiation policies and actions
- Configure authentication virtual server
- Configure traffic management virtual server

To verify the configuration:

1. Access the load balancing virtual server, using the FQDN. For example, http://owa.newacp.com.
2. View the AAA session on the NetScaler. show aaa session

Example

```
ClientIp (ClientPort) ->ServerIp(ServerPort)
 ---------------------------------------------
 PE id : 4
 User name: john.smith@NEWACP.COM Session Type: TM
Done
```

Configuration of Kerberos Authentication on a Client

Kerberos support must be configured on the browser to use Kerberos for authentication. You can use any Kerberos-compliant browser. Instructions for configuring Kerberos support on Internet Explorer and Mozilla Firefox follow. For other browsers, see the documentation of the browser.

To configure Internet Explorer for Kerberos authentication

1. In the Tools menu select Internet Options.
2. On the Security tab, click Local Intranet, and then click Sites.
3. In the Local Intranet dialog box, make sure that the Automatically detect intranet network option is selected, and then click Advanced.
4. In the Local Intranet dialog box, add the web sites of the domains of the traffic management virtual server on the NetScaler. The specified sites become local intranet sites.
5. Click Close or OK to close the dialog boxes.

To configure Mozilla Firefox for Kerberos authentication

1. Make sure that you have Kerberos properly configured on your computer.
2. Type `about:config` in the URL bar.
3. In the filter text box, type `network.negotiate`.
4. Change network.negotiate-auth.delegation-uris to the domain that you want to add.
5. Change network.negotiate-auth.trusted-uris to the domain that you want to add.

   Note: If you are running Windows, you also need to enter `sspi` in the filter text box and change the network.auth.use-sspi option to `False`.

Offloading Kerberos Authentication from Physical Servers

The NetScaler appliance can offload authentication tasks from servers. Instead of the physical servers authenticating the requests from clients, the Netscaler authenticates all the client requests before it forwards them to any of the physical servers bound to it. The user authentication is based on Active Directory tokens.

There is no authentication between the NetScaler and the physical server, and the authentication offload is transparent to the end users. After the initial logon to a Windows computer, the end user does not have to enter any additional authentication information in a pop-up or on a logon page.

In the current NetScaler release, Kerberos authentication is available only for Authentication, Authorization, and Auditing (AAA) Traffic Management Virtual Servers. Kerberos authentication is not supported for SSL VPN in the Access Gateway Enterprise Edition appliance or for NetScaler appliance management.

Kerberos authentication requires configuration on the NetScaler appliance and on client browsers.

To configure Kerberos authentication on the NetScaler appliance

1. Create a user account on Active Directory. When creating a user account, verify the following options in the User Properties section:

   - Make sure that you do not select the Change password at next logon option.

   - Be sure to select the Password does not expire option.
2. On the NetScaler appliance, at the CLI command prompt, type:

   - ktpass -princ HTTP/kerberos.crete.lab.net@crete.lab.net -ptype KRB5_NT_PRINCIPAL -mapuser kerbuser@crete.lab.net -mapop set -pass Citrix1 -out C:\kerbtabfile.txt

   Note: Be sure to type the above command on a single line. The output of the above command is written into the `C:\kerbatabfile.txt` file.

3. Upload the `kerbatabfile.txt` file to the */etc* directory of the NetScaler appliance by using a Secure Copy (SCP) client.

4. Run the following command to add a DNS server to the NetScaler appliance.

   - add dns nameserver `1.2.3.4`

   The NetScaler appliance cannot process Kerberos requests without the DNS server. Be sure to use the same DNS server that is used in the Microsoft Windows domain.

5. Switch to the shell prompt and run the following commands from the shell prompt:

   - ktutil # rkt /etc/kerbtabfile.txt

   - # wkt /etc/krb5.keytab

   - # list

     The list command displays the user account details that you created in the Active Directory. A sample screen of the output of the list command is shown below.

```
> shell
Copyright (c) 1992-2008 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992,
        The Regents of the University of California. All righ

root@ns# cd /etc
root@ns# ls -la *.txt
-rw-r--r--  1 root  wheel  82 Apr  4 00:43 kerbtabfile.txt
root@ns# ktutil
ktutil:  rkt /etc/kerbtabfile.txt
ktutil:  wkt /etc/krb5.keytab
ktutil:  list
slot KVNO Principal
---- ---- ---------------------------------------------------
   1    3 HTTP/kerberos.crete.example.com@crete.example.com
ktutil:  quit
root@ns#
```

Figure 1. Sample Output of the list Command

6. Switch to the command line interface of NetScaler.

7. Run the following command to create a Kerberos authentication server:

   - add authentication negotiateAction KerberosServer -domain "crete.lab.net" -domainUser kerbuser -domainUserPasswd Citrix1

8. Run the following command to create a negotiation policy:

   - add authentication negotiatePolicy Kerberos-Policy "REQ.IP.DESTIP == 192.168.17.200" KerberosServer

9. Run the following command to create an authentication virtual server.

   - add authentication vserver Kerb-Auth SSL 192.168.17.201 443 -AuthenticationDomain crete.example.com

10. Run the following command to bind the Kerberos policy to the authentication virtual server:

    - bind authentication vserver Kerb-Auth -policy Kerberos-Policy -priority 100

11. Run the following command to bind an SSL certificate to the authentication virtual server. You can use one of the test certificates, which you can install from the GUI NetScaler appliance. Run the following command to use the ServerTestCert sample certificate.

    - bind ssl vserver Kerb-Auth -certkeyName ServerTestCert

12. Create an HTTP load balancing virtual server with the IP address, 192.168.17.200.

    Ensure that you create a virtual server from the command line interface for NetScaler 9.3 releases if they are older than 9.3.47.8.

13. Run the following command to configure an authentication virtual server:

    - set lb vserver LB-Vserver-Name -authn401 ON -authnVsName Kerb-Auth

14. Enter the host name `http://www.crete.example.com` in the address bar of the Web browser.

    The Web browser displays an authentication dialog box because the Kerberos authentication is not set up in the browser.

Note: Kerberos authentication requires a specific configuration on the client. Ensure that the client can resolve the hostname, which results in the Web browser connecting to an HTTP virtual server.

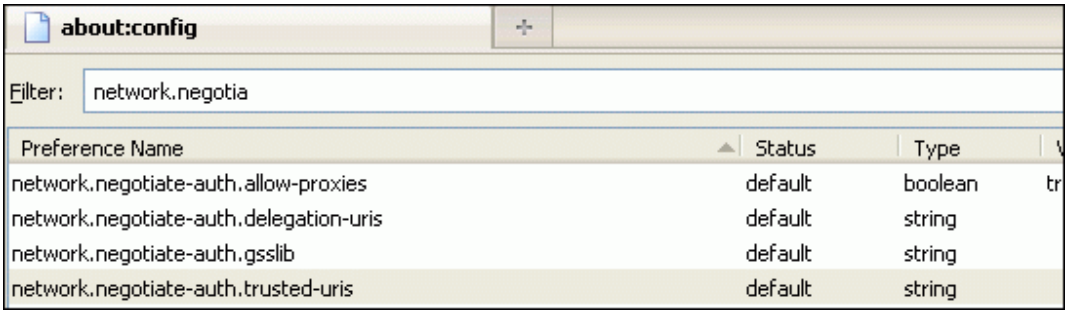
15. Configure Kerberos on the Web browser of the client computer.
    - For configuring on Internet Explorer, see "Configuring Internet Explorer for Kerberos authentication."
    - For configuring on Mozilla Firefox, see "Configuring Mozilla Firefox for Kerberos authentication."
16. Verify whether you can access the backend physical server without authentication.

To configure Internet Explorer for Kerberos authentication

1. Select Internet Options from the Tools menu.
2. Activate the Security tab.
3. Select Local Intranet from the Select a zone to view change security settings section.
4. Click Sites.
5. Click Advanced.
6. Specify the URL, `http://www.crete.example.com` and click Add.
7. Restart Internet Explorer.

To configure Mozilla Firefox for Kerberos authentication

1. Enter `about:config` in the address bar of the browser.
2. Click the warning disclaimer.
3. Type `Network.Negotiate-auth.trusted-uris` in the Filter box.
4. Double click `Network.Negotiate-auth.trusted-uris`. A sample screen is shown below.



5. In the Enter String Value dialog box, specify `www.crete.example.com`.
6. Restart Firefox.

NetScaler Kerberos Single Sign-On

NetScaler appliances now support single sign-on (SSO) using the Kerberos 5 protocol. Users log on to a proxy, the Application Delivery Controller (ADC), which then provides access to protected resources.

The NetScaler Kerberos SSO implementation requires the user's password for SSO methods that rely on basic, NTLM, or forms-based authentication. The user's password is not required for Kerberos SSO, although if Kerberos SSO fails and the NetScaler appliance has the user's password, it uses the password to attempt NTLM SSO.

If the user's password is available, the KCD account is configured with a realm, and no delegated user information is present, the NetScaler Kerberos SSO engine impersonates the user to obtain access to authorized resources. Impersonation is also called *unconstrained delegation*.

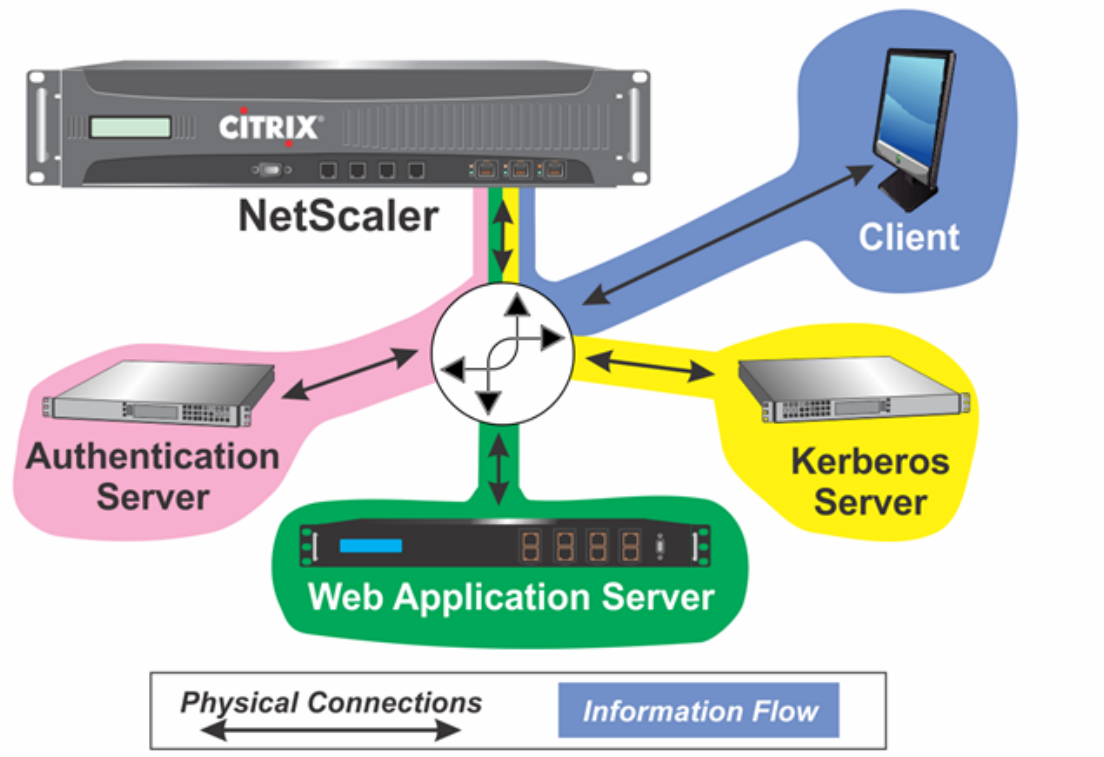
The NetScaler Kerberos SSO engine can also be configured to use a delegated account to obtain access to protected resources on the user's behalf. This configuration requires delegated user credentials, a keytab, or a delegated user certificate and matching CA certificate. Configuration that uses a delegated account is called *constrained delegation*.

An Overview of NetScaler Kerberos SSO

To use the NetScaler Kerberos SSO feature does, users first authenticate with Kerberos or a supported third-party authentication server. Once authenticated, the user requests access to a protected web application. The web server responds with a request for proof that the user is authorized to access that web application. The user's browser contacts the Kerberos server, which verifies that the user is authorized to access that resource, and then provides the user's browser with a service ticket that provides proof. The browser resends the user's request to the web application server with the service ticket attached. The web application server verifies the service ticket, and then allows the user to access the application.

AAA-TM implements this process as shown in the following diagram. The diagram illustrates the flow of information through the NetScaler appliance and AAA-TM, on a secure network with LDAP authentication and Kerberos authorization. AAA-TM environments that use other types of authentication have essentially the same information flow, although they might differ in some details.

Figure 1. A Secure Network with LDAP and Kerberos



NetScaler AAA-TM authentication and authorization in a Kerberos environment requires that the following actions take place.

1. The client sends a request for a resource to the traffic management virtual server on the NetScaler appliance.

2. The traffic management virtual server passes the request to the authentication virtual server, which authenticates the client and then passes the request back to the traffic

management virtual server.

3. The traffic management virtual server sends the client's request to the web application server.
4. The web application server responds to the traffic management virtual server with a 401 Unauthorized message that requests Kerberos authentication, with fallback to NTLM authentication if the client does not support Kerberos.
5. The traffic management virtual server contacts the Kerberos SSO daemon.
6. The Kerberos SSO daemon contacts the Kerberos server and obtains a ticket-granting ticket (TGT) allowing it to request service tickets authorizing access to protected applications.
7. The Kerberos SSO daemon obtains a service ticket for the user and sends that ticket to the traffic management virtual server.
8. The traffic management virtual server attaches the ticket to the user's initial request and sends the modified request back to the web application server.
9. The web application server responds with a 200 OK message.

These steps are transparent to the client, which just sends a request and receives the requested resource.

Integration of NetScaler Kerberos SSO with Authentication Methods

All AAA-TM authentication mechanisms support NetScaler Kerberos SSO. AAA-TM supports the Kerberos SSO mechanism with the Kerberos, CAC (Smart Card) and SAML authentication mechanisms with any form of client authentication to the NetScaler appliance. It also supports the HTTP-Basic, HTTP-Digest, Forms-based, and NTLM (versions 1 and 2) SSO mechanisms if the client uses either HTTP-Basic or Forms-Based authentication to log on to the NetScaler appliance.

The following table shows each supported client-side authentication method, and the supported server-side authentication method for that client-side method.

Table 1. Supported Authentication Methods

	Basic/Digest/ NTLM	Kerberos Constrained Delegation	User Impersonation
CAC (Smart Card): at SSL/TLS Layer		X	X
Forms-Based (LDAP/RADIUS/TACACS)	X	X	X

HTTP Basic (LDAP/RADIUS/TACACS)	X	X	X
Kerberos		X	
NTLM v1/v2		X	X
SAML		X	
SAML Two-Factor	X	X	X
Certificate Two-Factor	X	X	X

Setting up NetScaler SSO

You can configure NetScaler SSO to work in one of two ways: by impersonation or by delegation. SSO by impersonation is a simpler configuration than SSO by delegation, and is therefore usually preferable when your configuration allows it. To configure NetScaler SSO by impersonation, you must have the user's user name and password.

To configure NetScaler SSO by delegation, you must have the delegated user's credentials in one of the following formats: the user's user name and password, the keytab configuration that includes the user name and an encrypted password, or the delegated user certificate and the matching CA certificate.

Prerequisites

Before you configure NetScaler SSO, you need to have your NetScaler appliance fully configured to manage traffic to and authentication for your web application servers. Therefore, you must configure either load balancing or content switching, and then AAA, for these web application servers. You should also verify routing between the appliance, your LDAP server, and your Kerberos server.

If your network is not already configured in this manner, perform the following configuration tasks:

- Configure a server and service for each web application server.
- Configure a traffic management virtual server to handle traffic to and from your web application server.

Following are brief instructions and examples for performing each of these tasks from the NetScaler command line. For further assistance, see ns-lb-setup-wrapper-con.html and Setting up AAA Virtual Servers and DNS.

To create a server and service by using the NetScaler command line

For NetScaler SSO to obtain a TGS (service ticket) for a service, either the FQDN assigned to the server entity on the NetScaler appliance must match the FQDN of the web application server, or the server entity name must match the NetBios name of the web application server. You can take either of the following approaches:

- Configure the NetScaler server entity by specifying the FQDN of the web application server.
- Configure the NetScaler server entity by specifying the IP address of the web application server, and assign the server entity the same name as the NetBios name of the web application server.

At the command prompt, type the following commands:

- add server <serverName> <serverFQDN>
- add service <serviceName> <serverName> <type> <port>

For the variables, substitute the following values:

- **serverName**—A name for the NetScaler appliance to use to refer to this server.
- **serverFQDN**—The FQDN of the server. If the server has no domain assigned to it, use the server's IP address and make sure that the server entity name matches the NetBios name of the web application server.

- **serviceName**—A name for the NetScaler appliance to use to refer to this service.
- **type**—The protocol used by the service, either HTTP or MSSQLSVC.
- **port**—The port on which the service listens. HTTP services normally listen on port 80. Secure HTTPS services normally listen on port 443.

Example

The following examples add server and service entries on the NetScaler appliance for the web application server `was1.example.com`. The first example uses the FQDN of the web application server; the second uses the IP address.

To add the server and service using the web application server FQDN, `was1.example.com`, you would type the following commands:

```
add server was1 was1.example.com
add service was1service was1 HTTP 80
```

To add the server and service using the web application server IP and NetBios name, where the web application server IP is `10.237.64.87` and its NetBios name is `WAS1`, you would type the following commands:

```
add server WAS1 10.237.64.87
add service was1service WAS1 HTTP 8
```

To create a traffic management virtual server by using the NetScaler command line

The traffic management virtual server manages traffic between the client and the web application server. You can use either a load balancing or a content switching virtual server as the traffic management server. The SSO configuration is the same for either type.

To create a load balancing virtual server, at the command prompt, type the following command:

add lb vserver <vserverName> <type> <IP> <port>

For the variables, substitute the following values:

- **vserverName**—A name for the NetScaler appliance to use to refer to this virtual server.
- **type**—The protocol used by the service, either HTTP or MSSQLSVC.
- **IP**—The IP address assigned to the virtual server. This would normally be an IANA-reserved, non-public IP address on your LAN.
- **port**—The port on which the service listens. HTTP services normally listen on port 80. Secure HTTPS services normally listen on port 443.

Example

To add a load balancing virtual server called `tmvserver1` to a configuration that manages HTTP traffic on port 80, assigning it a LAN IP address of `10.217.28.20` and then binding the load balancing virtual server to the `wasservice1` service, you would type the following commands:

```
add lb vserver tmvserver1 HTTP 10.217.28.20 80
bind lb vserver tmvserv1 wasservice1
```

To create an authentication virtual server by using the NetScaler command line

The authentication virtual server manages authentication traffic between the client and the authentication (LDAP) server. To create an authentication virtual server, at the command prompt type the following commands:

- add authentication vserver <authvserverName> SSL <IP> 443
- set authentication vserver <authvserverName> –authenticationdomain <domain>

For the variables, substitute the following values:

- **authvserverName** —A name for the NetScaler appliance to use to refer to this authentication virtual server.
- **IP**—The IP address assigned to the authentication virtual server. As with the traffic management virtual server, this address would normally be an IANA-reserved, non-public IP on your LAN.
- **domain**—The domain assigned to the virtual server. This would usually be the domain of your network. It is customary, though not required, to enter the domain in all capitals when configuring the authentication virtual server.

Example

To add an authentication virtual server called `authverver1` to your configuration and assign it the LAN IP `10.217.28.21` and the domain `EXAMPLE.COM`, you would type the following commands:

```
add authentication vserver authvserver1 SSL 10.217.28.21 443
set authentication vserver authvserver1 –authenticationdomain EXAMPLE.COM
```

To configure a traffic management virtual server to use an authentication profile

The authentication virtual server can be configured to handle authentication for a single domain or for multiple domains. If it is configured to support authentication for multiple domains, you must also specify the domain for NetScaler SSO by creating an authentication profile, and then configuring the traffic management virtual server to use that authentication profile.

Note: The traffic management virtual server can be either a load balancing (`lb`) or content switching (`cs`) virtual server. The following instructions assume that you are using a load balancing virtual server. To configure a content switching virtual server, simply substitute `set cs vserver` for `set lb vserver`. The procedure is otherwise the same.

To create the authentication profile, and then configure the authentication profile on a traffic management virtual server, type the following commands:

- add authentication authnProfile <authnProfileName> {-authvserverName <string>} {-authenticationHost <string>} {-authenticationDomain <string>}
- set lb vserver <vserverName> -authnProfile <authnprofileName>

For the variables, substitute the following values:

- **authnprofileName**—A name for the authentication profile. Must begin with a letter, number, or the underscore character (_), and must consist of from one to thirty-one alphanumeric or hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.
- **authvserverName**—The name of the authentication virtual server that this profile uses for authentication.
- **authenticationHost**—Host name of the authentication virtual server.
- **authenticationDomain**—Domain for which NetScaler SSO handles authentication. Required if the authentication virtual server performs authentication for more than one domain, so that the correct domain is included when the NetScaler appliance sets the traffic management virtual server cookie.

Example

To create an authentication profile named `authnProfile1` for authentication of the `example.com` domain, and to configure the load balancing virtual server `vserver1` to use the authentication profile `authnProfile1`, you would type the following commands:

```
add authentication authnProfile authnProfile1 -authnvsName authvsesrver1
    -authenticationHost authvsesrver1 -authenticationDomain example.com
set lb vserver vserver1 -authnProfile authnProfile1
```

Configuring SSO

Configuring NetScaler SSO to authenticate by impersonation is simpler than configuring than SSO to authenticate by delegation, and is therefore usually preferable when your configuration allows it. You just create a KCD account. You can use the user's password.

If you do not have the user's password, you can configure NetScaler SSO to authenticate by delegation. Although somewhat more complex than configuring SSO to authenticate by impersonation, the delegation method provides flexibility in that a user's credentials might not be available to the NetScaler appliance in all circumstances.

For either impersonation or delegation, you must also enable integrated authentication on the web application server.

Enabling Integrated Authentication on the Web Application Server

To set up NetScaler Kerberos SSO on each web application server that Kerberos SSO will manage, use the configuration interface on that server to configure the server to require authentication. Select Kerberos (negotiate) authentication by preference, with fallback to NTLM for clients that do not support Kerberos.

Following are instructions for configuring Microsoft Internet Information Server (IIS) to require authentication. If your web application server uses software other than IIS, consult the documentation for that web server software for instructions.

To configure Microsoft IIS to use integrated authentication

1. Log on to the IIS server and open Internet Information Services Manager.
2. Select the web site for which you want to enable integrated authentication. To enable integrated authentication for all IIS web servers managed by IISM, configure authentication settings for the Default Web Site. To enable integrated authentication for individual services (such as Exchange, Exadmin, ExchWeb, and Public), configure these authentication settings for each service individually.
3. Open the Properties dialog box for the default web site or for the individual service, and click the Directory Security tab.
4. Beside Authentication and Access Control, select Edit.
5. Disable anonymous access.
6. Enable Integrated Windows authentication (only). Enabling integrated Windows authentication should automatically set protocol negotiation for the web server to `Negotiate, NTLM`, which specifies Kerberos authentication with fallback to NTLM for non-Kerberos capable devices. If this option is not automatically selected, manually set protocol negotiation to `Negotiate, NTLM`.

Setting Up SSO by Impersonation

You can configure the KCD account for NetScaler SSO by impersonation. In this configuration, the NetScaler appliance obtains the user's username and passwordwhen the user authenticates to the authentication server and uses those credentials to impersonate the user to obtain a ticket-granting ticket (TGT). If the user's name is in UPN format, the appliance obtains the user's realm from UPN. Otherwise, it obtains the user's name and realm by extracting it from the SSO domain used during initial authentication, or from the session profile.

When configuring the KCD account, you must set the realm parameter to the realm of the service that the user is accessing. The same realm is also used as the user's realm if the user's realm cannot be obtained from authentication with the Netscaler appliance or from the session profile.

To create the KCD account for SSO by impersonation with a password

At the command prompt, type the following command:

add aaa kcdaccount <accountname> -realmStr <realm>

For the variables, substitute the following values:

- **accountname**—The KCD account name.
- **realm**—The domain assigned to NetScaler SSO.

Example:

To add a KCD account named `kcdccount1`, and use the keytab named `kcdvserver.keytab`, you would type the following command:

add aaa kcdAccount kcdaccount1 –realmStr EXAMPLE.COM

Configuring SSO by Delegation

To configure SSO by Delegation, you need to perform the following tasks:

- If you are configuring delegation by delegated user certificate, install the matching CA certificates on the NetScaler appliance and add them to the NetScaler configuration.
- Create the KCD account on the appliance. The appliance uses this account to obtain service tickets for your protected applications.
- Configure the Active Directory server.

Installing the Client CA Certificate on the NetScaler appliance

If you are configuring NetScaler SSO with a client certificate, you must copy the matching CA certificate for the client certificate domain (the *client CA certificate*) to the NetScaler appliance, and then install the CA certificate. To copy the client CA certificate, use the file transfer program of your choice to transfer the certificate and private-key file to the NetScaler appliance, and store the files in `/nsconfig/ssl`.

To install the client CA certificate on the NetScaler appliance

At the command prompt, type the following command:

add ssl certKey <certkeyName> -cert <cert> [(-key <key> [-password]) | -fipsKey <fipsKey>] [-inform (DER | PEM)] [-expiryMonitor (ENABLED | DISABLED | UNSET) [-notificationPeriod <positive_integer>]] [-bundle (YES | NO)]

For the variables, substitute the following values:

- **certkeyName**—A name for the client CA certificate. Must begin with an ASCII alphanumeric or underscore (_) character, and must consist of from one to thirty-one characters. Allowed characters include the ASCII alphanumerics, underscore, hash (#), period(.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the certificate-key pair is created. If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cert" or 'my cert').
- **cert**—Full path name and file name of the X509 certificate file used to form the certificate-key pair. The certificate file must be stored on the NetScaler appliance, in the /nsconfig/ssl/ directory.
- **key**—Full path name and file name of the file that contains the private key to the X509 certificate file. The key file must be stored on the NetScaler appliance in the /nsconfig/ssl/ directory.

- **password**—If a private key is specified, the passphrase used to encrypt the private key. Use this option to load encrypted private keys in PEM format.
- **fipsKey**—Name of the FIPS key that was created inside the Hardware Security Module (HSM) of a FIPS appliance, or a key that was imported into the HSM.

  Note: You can specify either a `key` or a `fipsKey`, but not both.
- **inform**—Format of the certificate and private-key files, either PEM or DER.
- **passplain**—Pass phrase used to encrypt the private key. Required when adding an encrypted private-key in PEM format.
- **expiryMonitor**—Configure the NetScaler appliance to issue an alert when the certificate is about to expire. Possible values: ENABLED, DISABLED, UNSET.
- **notificationPeriod**—If expiryMonitor is ENABLED, number of days before the certificate expires to issue an alert.
- **bundle**—Parse the certificate chain as a single file after linking the server certificate to its issuer's certificate within the file. Possible values: YES, NO.

Example

The following example adds the specified delegated user certificate `customer-cert.pem` to the NetScaler configuration along with the key `customer-key.pem`, and sets the password, certificate format, expiration monitor, and notification period.

To add the delegated user certificate, you would type the following commands:

```
add ssl certKey customer -cert "/nsconfig/ssl/customer-cert.pem"
      -key "/nsconfig/ssl/customer-key.pem" -password "dontUseDefaultPWs!"
      -inform PEM -expiryMonitor ENABLED [-notificationPeriod 14
```

Creating the KCD Account

If you are configuring NetScaler SSO by delegation, you can configure the KCD account to use the user's log-on name and password, to use the user's log-on name and keytab, or to use the user's client certificate. If you configure SSO with user name and password, the NetScaler appliance uses the delegated user account to obtain a Ticket Granting Ticket (TGT), and then uses the TGT to obtain service tickets for the specific services that each user requests. If you configure SSO with keytab file, the NetScaler appliance uses the delegated user account and keytab information. If you configure SSO with a delegated user certificate, the NetScaler appliance uses the delegated user certificate.

To create the KCD account for SSO by delegation with a password

At the command prompt, type the following commands:

add aaa kcdaccount <accountname> -delegatedUser root -kcdPassword <password> -realmStr <realm>

For the variables, substitute the following values:

- **accountname**—A name for the KCD account.
- **password**—A password for the KCD account.
- **realm**—The realm of the KCD account, usually the domain for which SSO is active.

Example (UPN Format)

To add a KCD account named `kcdaccount1` to the NetScaler appliance configuration with a password of `password1` and a realm of `EXAMPLE.COM`, specifying the delegated user account in UPN format (as root), you would type the following commands:

```
add aaa kcdaccount kcdaccount1 –delegatedUser root
-kcdPassword password1 -realmStr EXAMPLE.COM
```

Example (SPN Format)

To add a KCD account named `kcdaccount1` to the NetScaler appliance configuration with a password of `password1` and a realm of `EXAMPLE.COM`, specifying the delegated user account in SPN format, you would type the following commands:

```
add aaa kcdAccount kcdaccount1 -realmStr EXAMPLE.COM
-delegatedUser "host/kcdvserver.example.com" -kcdPassword password1
```

Creating the KCD account for SSO by delegation with a keytab

If you plan to use a keytab file for authentication, first create the keytab. You can create the keytab file manually by logging onto the AD server and using the ktpass utility, or you can use the NetScaler configuration utility to create a batch script, and then run that script on the AD server to generate the keytab file. Next, use FTP or another file transfer program to transfer the keytab file to the NetScaler appliance and place it in the /nsconfig/krb directory. Finally, configure the KCD account for NetScaler SSO by delegation and provide the path and file name of the keytab file to the NetScaler appliance.

To create the keytab file manually

Log on to the AD server command line and, at the command prompt, type the following command:

ktpass /princ <SPN> /ptype KRB5_NT_PRINCIPAL /mapuser <DOMAIN>\<username> /pass <password> -out <File_Path>

For the variables, substitute the following values:

- **SPN**—The service principal name for the KCD service account.

- **DOMAIN**—The domain of the Active Directory server.
- **username**—The KSA account username.
- **password**—The KSA account password.
- **path**— The full path name of the directory in which to store the keytab file after it is generated.

To use the NetScaler configuration utility to create a script to generate the keytab file.

1. Navigate to Security > AAA - Application Traffic
2. In the data pane, under Kerberos Constrained Delegation, click Batch file to generate Keytab.
3. In the Generate KCD (Kerberos Constrained Delegation) Keytab Script dialog box, set the following parameters:
   - **Domain User Name**—The KSA account username.
   - **Domain Password**—The KSA account password.
   - **Service Principal**—The service principal name for the KSA.
   - **Output File Name**—The full path and file name to which to save the keytab file on the AD server.
4. Clear the Create Domain User Account check box.
5. Click Generate Script.
6. Log on to the Active Directory server and open a command line window.
7. Copy the script from the Generated Script window and paste it directly into the Active Directory server command-line window. The keytab is generated and stored in the directory under the file name that you specified as **Output File Name**.
8. Use the file transfer utility of your choice to copy the keytab file from the Active Directory server to the NetScaler appliance and place it in the `/nsconfig/krb` directory.

To create the KCD account

At the command prompt, type the following command:

add aaa kcdaccount <accountname> –keytab <keytab>

Example:

To add a KCD account named `kcdccount1`, and use the keytab named `kcdvserver.keytab`, you would type the following commands:

add aaa kcdaccount kcdaccount1 –keytab kcdvserver.keytab

To create the KCD account for SSO by delegation with a delegated user cert

At the command prompt, type the following command:

add aaa kcdaccount <accountname> -realmStr <realm> -delegatedUser <user_name/SPN> -usercert <cert> -cacert <cacert>

For the variables, substitute the following values:

- **accountname**—A name for the KCD account.
- **realmStr**—The realm for the KCD account, usually the domain for which SSO is configured.
- **delegatedUser**—The delegated user name, in SPN format.
- **usercert**—The full path and name of the delegated user certificate file on the NetScaler appliance. The delegated user certificate must contain both the client certificate and the private key, and must be in PEM format. If you use smart card authentication, you might need to create a smart card certificate template to allow certificates to be imported with the private key.
- **cacert**—The full path to and name of the CA certificate file on the NetScaler appliance.

Example:

To add a KCD account named `kcdccount1`, and use the keytab named `kcdvserver.keytab`, you would type the following command:

```
add aaa kcdaccount kcdaccount1 -realmStr EXAMPLE.COM
    -delegatedUser "host/kcdvserver.example.com" -usercert /certs/usercert
    -cacert /cacerts/cacert
```

Setting up Active Directory for NetScaler SSO

When you configure SSO by delegation, in addition to creating the KCDAccount on the NetScaler appliance, you must also create a matching Kerberos Service Account (KSA) on your LDAP active directory server, and configure the server for SSO. To create the KSA, use the account creation process on the active directory server. To configure SSO on the active directory server, open the properties window for the KSA. In the Delegation tab, enable the following options: Trust this user for delegation to specified services only and Use any Authentication protocol. (The Kerberos only option does not work, because it does not enable protocol transition or constrained delegation.) Finally, add the services that NetScaler SSO will manage.

Note: If the Delegation tab is not visible in the KSA account properties dialog box, before you can configure the KSA as described, you must use the Microsoft `setspn` command-line tool to configure the active directory server so that the tab is visible.

To configure delegation for the Kerberos service account

1. In the LDAP account configuration dialog box for the Kerberos service account that you created, click the Delegation tab.

2. Choose "Trust this user for delegation to the specified services only".

3. Under "Trust this user for delegation to the specified services only," choose "Use any authentication protocol".

4. Under “Services to which this account can present delegated credentials,” click Add.

5. In the Add Services dialog box, click Users or Computers, choose the server that hosts the resources to be assigned to the service account, and then click OK.

   Note: Constrained delegation does not support services hosted in domains other than the domain assigned to the account, even though Kerberos might have a trust relationship with other domains

6. Back in the Add Services dialog box, in the Available Services list, choose the services assigned to the service account. NetScaler SSO supports the HTTP and MSSQLSVC services.

7. Click OK.

Application Firewall

The following topics cover installation and configuration of the Citrix Application Firewall feature.

Introduction	An overview of web application security and how the application firewall works.
Configuration	How to configure the application firewall to protect a web site, a web service, or a web 2.0 site.
Signatures	A detailed description of the signatures feature and how to configure the signatures, add signatures from a supported vulnerability scanning tool, and define your own signatures, with examples.
Advanced Protections	A detailed description of all of the application firewall security checks, with configuration information and examples.
Profiles	A description of how profiles are configured and used in the application firewall.
Policies	A description of how policies are used when configuring the application firewall, with examples of useful policies.
Imports	A description of how the application firewall uses different types of imported files, and how to import and export files.
Global Configuration	A description of application firewall features that apply to all profiles, and how to configure them.
Use Cases	Extended examples that demonstrate how to set up the application firewall to best protect specific types of more complex web sites and web services.
Logs, Statistics, and Reports	How to access and use the application firewall logs, the statistics, and the reports to assist in configuring the application firewall.

Introduction

The Citrix® Application Firewall™ prevents security breaches, data loss, and possible unauthorized modifications to web sites that access sensitive business or customer information. It does so by filtering both requests and responses, examining them for evidence of malicious activity, and blocking those that exhibit such activity. Your site is protected not only from common types of attacks, but also from new, as yet unknown attacks. In addition to protecting web servers and web sites from unauthorized access and misuse by hackers and malicious programs, the application firewall provides protection against security vulnerabilities in legacy CGI code or scripts, other web frameworks, web server software, and the underlying operating systems.

The Application Firewall is available as a stand-alone appliance, or as a feature on a Citrix NetScaler appliance or Citrix NetScaler virtual appliance. In the application firewall documentation, the term *application firewall appliance* refers to the platform on which the application firewall is running, regardless of whether that platform is a dedicated firewall appliance, a NetScaler appliance on which other features have also been configured, or a NetScaler virtual appliance,

To use the application firewall, you must create at least one security configuration to block connections that violate the rules that you set for your protected web sites. The number of security configurations that you might want to create depends on the complexity of your web site. In many cases, one is sufficient. You can probably use the defaults for the global settings, which affect all security configurations, but you can change the global settings if necessary.

Web Application Security

Web application security is that part of network security that covers computers and programs that communicate by using the HTTP and HTTPS protocols. This is an extremely broad area in which security flaws and weaknesses abound. Operating systems on both servers and clients have security issues and are vulnerable to attack. Web server software and web site enabling technologies such as CGI, Java, JavaScript, PERL and PHP have underlying vulnerabilities. Browsers and other client applications that communicate with web-enabled applications also have vulnerabilities. Web sites that use any technology but the simplest of HTML, including any site that allows interaction with visitors, often have vulnerabilities of their own.

In the past, a breach in security was often just an annoyance, but today that is seldom the case. For example, attacks in which a hacker gained access to a web server and made unauthorized modifications to (*defaced*) a web site used to be common. They were usually launched by hackers who had no motivation beyond demonstrating their skills to fellow hackers or embarrassing the targeted person or company. Most current security breaches, however, are motivated by a desire for money. The majority attempt to accomplish one or both of the following goals: to obtain sensitive and potentially valuable private information, or to obtain unauthorized access to and control of a web site or web server.

Certain forms of web attacks focus on obtaining private information. These attacks are often possible even against web sites that are secure enough to prevent an attacker from taking full control. The information that an attacker can obtain from a web site can include customer names, addresses, phone numbers, social security numbers, credit card numbers, medical records, and other private information. The attacker can then use this information or sell it to others. Much of the information obtained by such attacks is protected by law, and all of it by custom and expectation. A breach of this type can have extremely serious consequences for customers whose private information is compromised. At best, these customers will have to exercise vigilance to prevent others from abusing their credit cards, opening unauthorized credit accounts in their name, or appropriating their identities outright (identity theft). At worst, the customers may face ruined credit ratings or even be blamed for criminal activities in which they had no part.

Other web attacks are aimed at obtaining control of (or *compromising*) a web site or the server on which it operates, or both. A hacker who gains control of a web site or server can use it to host unauthorized content, act as a proxy for content hosted on another web server, provide SMTP services to send unsolicited bulk email, or provide DNS services to support such activities on other compromised web servers. Most web sites that are hosted on compromised web servers promote questionable or outright fraudulent businesses. For example, the majority of phishing web sites and child pornography web sites are hosted on compromised web servers.

Protecting your web sites and web services against these attacks requires a multilayered defense capable of both blocking known attacks with identifiable characteristics and protecting against unknown attacks, which can often be detected because they look different from the normal traffic to your web sites and web services.

Known Web Attacks

The first line of defense for your web sites is protection against the large number of attacks that are known to exist and have been observed and analyzed by web security experts. Common types of attacks against HTML-based web sites include:

- **Buffer overflow attacks.** Sending an extremely long URL, extremely long cookie, or other extremely long bit of information to a web server in hopes of causing it or the underlying operating system to hang, crash, or provide the attacker with access to the underlying operating system. A buffer overflow attack can be used to gain access to unauthorized information, to compromise a web server, or both.

- **Cookie security attacks.** Sending a modified cookie to a web server, usually in hopes of obtaining access to unauthorized content by using falsified credentials.

- **Forceful browsing.** Accessing URLs on a web site directly, without navigating to the URLs by means of hyperlinks on the home page or other common start URLs on the web site. Individual instances of forceful browsing may simply indicate a user who bookmarked a page on your web site, but repeated attempts to access nonexistent content, or content that users should never access directly, often represent an attack on web site security. Forceful browsing is normally used to gain access to unauthorized information, but can also be combined with a buffer overflow attack in an attempt to compromise your server.

- **Web form security attacks.** Sending inappropriate content to your web site in a web form. Inappropriate content can include modified hidden fields, HTML or code in a field intended for alphanumeric data only, an overly long string in a field that accepts only a short string, an alphanumeric string in a field that accepts only an integer, and a wide variety of other data that your web site does not expect to receive in that web form. A web form security attack can be used either to obtain unauthorized information from your web site or to compromise the web site outright, usually when combined with a buffer overflow attack.

Two specialized types of attacks on web form security deserve special mention:

- **SQL injection attacks.** Sending an active SQL command or commands in a web form or as part of a URL, with the goal of causing an SQL database to execute the command or commands. SQL injection attacks are normally used to obtain unauthorized information.

- **Cross-site scripting attacks.** Using a URL or a script on a web page to violate the same-origin policy, which forbids any script from obtaining properties from or modifying any content on a different web site. Since scripts can obtain information and modify files on your web site, allowing a script access to content on a different web site can provide an attacker the means to obtain unauthorized information, to compromise a web server, or both.

Attacks against XML-based web services normally fall into at least one of the following two categories: attempts to send inappropriate content to a web service, or attempts to breach security on a web service. Common types of attacks against XML-based web services include:

- **Malicious code or objects.** XML requests that contain code or objects that can either directly obtain sensitive information or can give an attacker control of the web service or underlying server.

- **Badly-formed XML requests.** XML requests that do not conform to the W3C XML specification, and that can therefore breach security on an insecure web service.

- **Denial of service (DoS) attacks.** XML requests that are sent repeatedly and in high volume, with the intent of overwhelming the targeted web service and denying legitimate users access to it.

In addition to standard XML-based attacks, XML web services and Web 2.0 sites are also vulnerable to SQL injection and cross-site scripting attacks, as described below:

- **SQL injection attacks.** Sending an active SQL command or commands in an XML-based request, with the goal of causing an SQL database to execute that command or commands. As with HTML SQL injection attacks, XML SQL injection attacks are normally used to obtain unauthorized information.

- **Cross-site scripting attacks.** Using a script included in an XML based application to violate the same-origin policy, which does not allow any script to obtain properties from or modify any content on a different application. Since scripts can obtain information and modify files by using your XML application, allowing a script access to content belonging to a different application can give an attacker the means to obtain unauthorized information, to compromise the application, or both.

Known web attacks can usually be stopped by filtering web site traffic for specific characteristics (*signatures*) that always appear for a specific attack and should never appear in legitimate traffic. This approach has the advantages of requiring relatively few resources and posing relatively little risk of false positives. It is therefore a valuable tool in fighting attacks on web sites and web services, and configuring basic signature protections that intercept most known web attacks is easy to do.

Unknown Web Attacks

The greatest threat against web sites and applications does not come from known attacks, but from unknown attacks. Most unknown attacks fall into one of two categories: newly-launched attacks for which security firms have not yet developed an effective defense (*zero-day* attacks), and carefully-targeted attacks on a specific web site or web service rather than many web sites or web services (*spear* attacks). These attacks, like known attacks, are usually intended to obtain sensitive private information, compromise the web site or web service and allow it to be used for further attacks, or both of those goals.

Zero-day attacks are a major threat to all users. These attacks are usually of the same types as known attacks; zero-day attacks often involve injected SQL, a cross-site script, a cross-site request forgery, or another type of attack similar to known attacks. In most cases, they target vulnerabilities that the developers of the targeted software, web site, or web service either are unaware of or have just learned about. Security firms have therefore usually not developed defenses against these attacks, and even if they have, users have usually not obtained and installed the patches or performed the workarounds necessary to protect against these attacks. The time between discovery of a zero-day attack and availability of a defense (the *vulnerability window*) is shrinking, but perpetrators can still count on hours or even days in which many web sites and web services lack any specific protection against the attack.

Spear attacks are a major threat, but to a more select group of users. A common type of spear attack, a spear phish, is usually targeted at customers of a specific bank or financial institution, or (less commonly) at employees of a specific company or organization. Unlike other phishes, which are often crudely written forgeries that a user with any familiarity with the actual communications of that bank or financial institution can recognize, spear phishes are letter perfect and extremely convincing. They can contain information specific to the individual that, at first look, no stranger should know or be able to obtain. The spear phisher is therefore able to convince his or her target to provide the requested information, which the phisher can then use to loot accounts, to process illegitimately obtained money from other sources, or to gain access to other, even more sensitive information.

Both of these types of attack have certain characteristics that can usually be detected, although not by using static patterns that look for specific characteristics, as do standard signatures. Detecting these types of attacks requires more sophisticated and more resource-intensive approaches, such as heuristic filtering and positive security model systems. Heuristic filtering looks, not for specific patterns, but for patterns of behaviors. Positive security model systems model the normal behavior of the web site or web service that they are protecting, and then block connections that do not fit within that model of normal use. URL based and web-form based security checks profile normal use of your web sites, and then control how users interact with your web sites, using both heuristics and positive security to block anomalous or unexpected traffic. Both heuristic and positive security, properly designed and deployed, can catch most attacks that signatures miss. However, they require considerably more resources than do signatures, and you must spend some time configuring them properly to avoid false positives. They are therefore usually used, not as the primary line of defense, but as backups to signatures or other less resource-intensive approaches.

By configuring these advanced protections in addition to signatures, you create a hybrid security model, which enables the application firewall to provide comprehensive protection against both known and unknown attacks.

How The Application Firewall Works

When you install the application firewall, you create an initial *security configuration*, which consists of a *policy*, a *profile*, and a *signatures object*. The policy is a rule that identifies the traffic to be filtered, and the profile identifies the patterns and types of behavior to allow or block when the traffic is filtered. The simplest patterns, which are called *signatures*, are not specified within the profile, but in a signatures object that is associated with the profile.

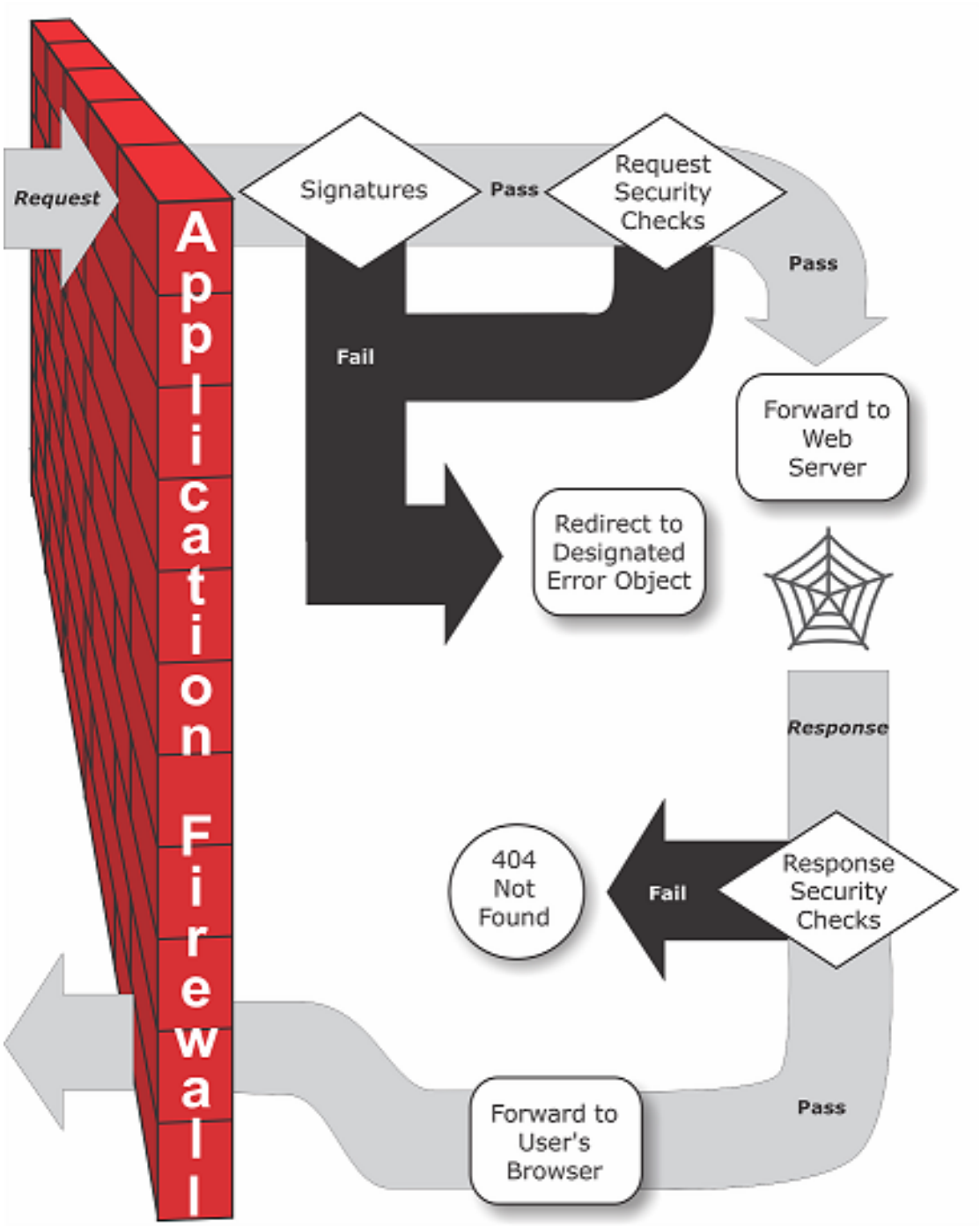
A signature is a string or pattern that matches a known type of attack. The application firewall contains over a thousand signatures in seven categories, each directed at attacks on specific types of web servers and web content. Citrix updates the list with new signatures as new threats are identified. During configuration, you specify the signature categories that are appropriate for the web servers and content that you need to protect. Signatures provide good basic protection with low processing overhead. If your applications have special vulnerabilities or you detect an attack against them for which no signature exists, you can add your own signatures.

The more advanced protections are called *security checks*. A security check is a more rigorous, algorithmic inspection of a request for specific patterns or types of behavior that might indicate an attack or constitute a threat to your protected web sites and web services. It can, for example, identify a request that attempts to perform a certain type of operation that might breach security, or a response that includes sensitive private information such as a social security number or credit card number. During configuration, you specify the security checks that are appropriate for the web servers and content that you need to protect. The security checks are restrictive. Many of them can block legitimate requests and responses if you do not add the appropriate exceptions (*relaxations*) when configuring them. Identifying the needed exceptions is not difficult if you use the adaptive learning feature, which observes normal use of your web site and creates recommended exceptions.

The application firewall can be installed as either a Layer 3 network device or a Layer 2 network bridge between your servers and your users, usually behind your company's router or firewall. It must be installed in a location where it can intercept traffic between the web servers that you want to protect and the hub or switch through which users access those web servers. You then configure the network to send requests to the application firewall instead of directly to your web servers, and responses to the application firewall instead of directly to your users. The application firewall filters that traffic before forwarding it to its final destination, using both its internal rule set and your additions and modifications. It blocks or renders harmless any activity that it detects as harmful, and then forwards the remaining traffic to the web server. The following figure provides an overview of the filtering process.

Note: The figure omits the application of a policy to incoming traffic. It illustrates a security configuration in which the policy is to process all requests. Also, in this configuration, a signatures object has been configured and associated with the profile, and security checks have been configured in the profile.

Figure 1. A Flowchart of Application Firewall Filtering



As the figure shows, when a user requests a URL on a protected web site, the application firewall first examines the request to ensure that it does not match a signature. If the request matches a signature, the application firewall either displays the *error object* (a web page that is located on the application firewall appliance and which you can configure by using the imports feature) or forwards the request to the designated error URL (the *error page*). Signatures do not require as many resources as do security checks, so detecting and stopping attacks that are detected by a signature before running any of the security checks reduces the load on the server.

If a request passes signature inspection, the application firewall applies the request security checks that have been enabled. The request security checks verify that the request is appropriate for your web site or web service and does not contain material that might

pose a threat. For example, security checks examine the request for signs indicating that it might be of an unexpected type, request unexpected content, or contain unexpected and possibly malicious web form data, SQL commands, or scripts. If the request fails a security check, the application firewall either sanitizes the request and then sends it back to the NetScaler appliance (or NetScaler virtual appliance), or displays the error object. If the request passes the security checks, it is sent back to the NetScaler appliance, which completes any other processing and forwards the request to the protected web server.

When the web site or web service sends a response to the user, the application firewall applies the response security checks that have been enabled. The response security checks examine the response for leaks of sensitive private information, signs of web site defacement, or other content that should not be present. If the response fails a security check, the application firewall either removes the content that should not be present or blocks the response. If the response passes the security checks, it is sent back to the NetScaler appliance, which forwards it to the user.

Application Firewall Features

The basic application firewall features are policies, profiles, and signatures, which provide a hybrid security model as described in "Known Web Attacks," "Unknown Web Attacks," and "How the Application Firewall Works." Of special note is the learning feature, which observes traffic to your protected applications and recommends appropriate configuration settings for certain security checks.

The imports feature manages files that you upload to the application firewall. These files are then used by the application firewall in various security checks, or when responding to a connection that matches a security check.

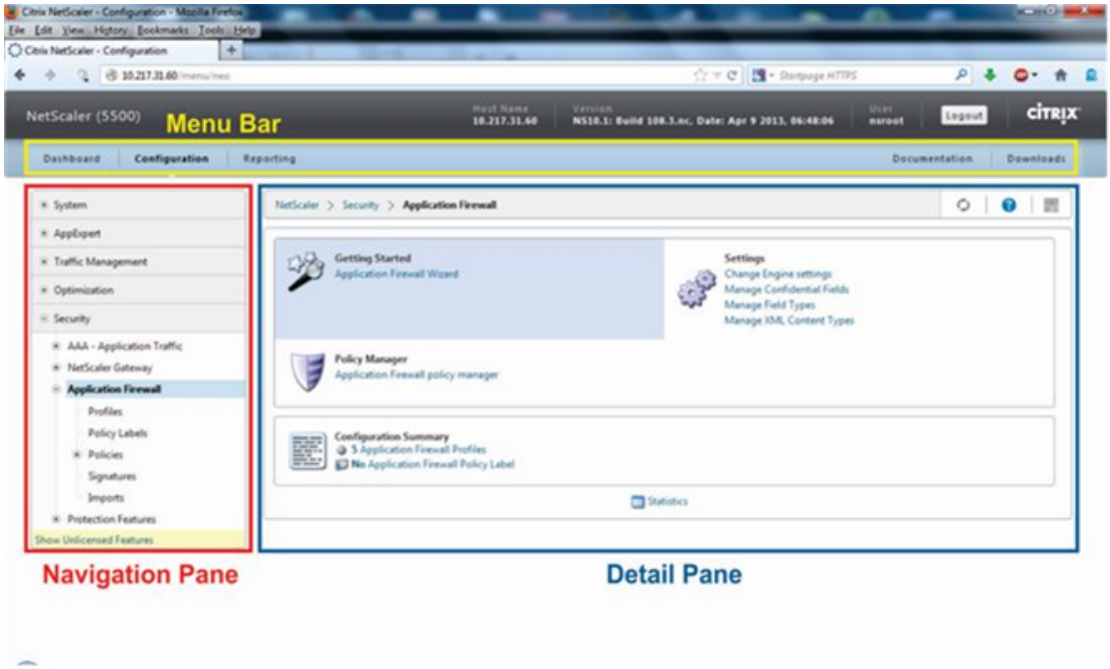
You can use the logs, statistics, and reports features to evaluate the performance of the application firewall and identify possible needs for additional protections.

The Application Firewall User Interfaces

All models in the Citrix NetScaler Application Delivery product line can be configured and managed from the Citrix NetScaler command line interface or the web-based configuration utility. However, the configuration utility provides a more complete interface. Not all application firewall configuration tasks can be performed at the command line. Also, the configuration utility provides access to a wizard that reduces the complexity of configuring the application firewall. Unlike most wizards, the application firewall wizard can serve as your primary interface to the application firewall.

The command line interface is a modified UNIX shell based on the FreeBSD `bash` shell. To configure the application firewall from the command line interface, you type commands at the prompt and press the Enter key, just as you do with any other Unix shell. For instructions for using the command line interface, see "Command Reference."

Figure 1 shows the navigation pane expanded to display the application firewall screens, and in the detail pane the main application firewall screen.



The configuration utility has two main areas on all screens. The panel on the left, called the *Navigation Pane*, contains a navigation tree, with which you navigate to the screens on which you configure the features that are installed on your appliance. The screens to which you navigate appear to the right of the Navigation Pane, in the *details pane*.

When you access the configuration utility, the details pane displays the System Overview screen, as shown in Figure 1. If, in the navigation pane, you click plus sign next to the application firewall folder, the Application Firewall node *expands* to include the main application firewall elements that you can configure. If you click the first element, Profiles, the details pane displays the configured profiles, if any profiles have been configured. At the bottom of the details pane, you can click Add to configure a new profile. Other buttons at the bottom of the details pane are grayed out until you select an existing profile.

Screens for the other elements work in the same way.

If, instead of expanding the application firewall node, you click the node itself, the details pane displays different options, one of which is the application firewall wizard. Citrix recommends that you use the wizard for initial configuration, and many users use it almost exclusively. It includes most of the functionality that is available elsewhere in the configuration utility.

For information and instructions on accessing the configuration utility, see "Citrix NetScaler Getting Started Guide."

Configuring the Application Firewall

You can configure the Citrix Application Firewall using any of the following methods:

- **Application Firewall Wizard.** A dialog box consisting of a series of screens that step you through the configuration process.
- **Citrix Web Interface AppExpert Template.** A NetScaler AppExpert template (a set of configuration settings) that are designed to provide appropriate protection for web sites. This AppExpert template contains appropriate Application Firewall configuration settings for protecting many web sites.
- **Citrix NetScaler Configuration Utility.** The NetScaler web-based configuration interface.
- **Citrix NetScaler Command Line Interface.** The NetScaler command line configuration interface.

Citrix recommends that you use the Application Firewall Wizard. Most users will find it the easiest method to configure the application firewall, and it is designed to prevent mistakes. If you have a new Citrix NetScaler appliance that you will use primarily to protect web sites, you may find the Web Interface AppExpert template a better option because it provides a good default configuration, not just for the Application Firewall, but for the entire appliance. Both the configuration utility and the command line interface are intended for experienced users, primarily to modify an existing configuration or use advanced options.

The Application Firewall Wizard

The application firewall wizard is a dialog box that consists of several screens that prompt you to configure each part of a simple configuration. The application firewall then creates the appropriate configuration elements from the information that you give it. This is the simplest and, for most purposes, the best way to configure the application firewall.

To use the wizard, connect to the configuration utility with the browser of your choice. When the connection is established, verify that the application firewall is enabled, and then run the application firewall wizard, which prompts you for configuration information. You do not have to provide all of the requested information the first time you use the wizard. Instead, you can accept default settings, perform a few relatively straightforward configuration tasks to enable important features, and then allow the application firewall to collect important information to help you complete the configuration.

For example, when the wizard prompts you to specify a rule for selecting the traffic to be processed, you can accept the default, which selects all traffic. When it presents you with a list of signatures, you can enable the appropriate categories of signatures and turn on the collection of statistics for those signatures. For this initial configuration, you can skip the advanced protections (*security checks*). The wizard automatically creates the appropriate policy, signatures object, and profile (collectively, the *security configuration*) , and binds the policy to global. The application firewall then begins filtering connections to your protected web sites, logging any connections that match one or more of the signatures that

you enabled, and collecting statistics about the connections that each signature matches. After the application firewall processes some traffic, you can run the wizard again and examine the logs and statistics to see if any of the signatures that you have enabled are matching legitimate traffic. After determining which signatures are identifying the traffic that you want to block, you can enable blocking for those signatures. If your web site or web service is not complex, does not use SQL, and does not have access to sensitive private information, this basic security configuration will probably provide adequate protection.

You may need additional protection if, for example, your web site is dynamic. Content that uses scripts may need protection against cross-site scripting attacks. Web content that uses SQL—such as shopping carts, many blogs, and most content management systems—may need protection against SQL injection attacks. Web sites and web services that collect sensitive private information such as social security numbers or credit card numbers may require protection against unintentional exposure of that information. Certain types of web-server or XML-server software may require protection from types of attacks tailored to that software. Another consideration is that specific elements of your web sites or web services may require different protection than do other elements. Examining the application firewall logs and statistics can help you identify the additional protections that you might need.

After deciding which advanced protections are needed for your web sites and web services, you can run the wizard again to configure those protections. Certain security checks require that you enter exceptions (*relaxations*) to prevent the check from blocking legitimate traffic. You can do so manually, but it is usually easier to enable the adaptive learning feature and allow it to recommend the necessary relaxations. You can use the wizard as many times as necessary to enhance your basic security configuration and/or create additional security configurations.

The wizard automates some tasks that you would have to perform manually if you did not use the wizard. It automatically creates a policy, a signatures object, and a profile, and assigns them the name that you provided when you were prompted for the name of your configuration. The wizard also adds your advanced-protection settings to the profile, binds the signatures object to the profile, associates the profile with the policy, and puts the policy into effect by binding it to Global.

A few tasks cannot be performed in the wizard. You cannot use the wizard to bind a policy to a bind point other than Global. If you want the profile to apply to only a specific part of your configuration, you must manually configure the binding. You cannot configure the engine settings or certain other global configuration options in the wizard. While you can configure any of the advanced protection settings in the wizard, if you want to modify a specific setting in a single security check, it may be easier to do so on the manual configuration screens in the configuration utility.

For more information on using the Application Firewall Wizard, see "The Application Firewall Wizard."

The Citrix Web Interface AppExpert Template

AppExpert Templates are a different and simpler approach to configuring and managing complex enterprise applications. The AppExpert display in the configuration utility consists of a table. Applications are listed in the left-most column, with the NetScaler features that are applicable to that application appearing each in its own column to the right. (In the AppExpert interface, those features that are associated with an application are called *application units*.) In the AppExpert interface, you configure the interesting traffic for each application, and turn on rules for compression, caching, rewrite, filtering, responder and the application firewall, instead of having to configure each feature individually.

The Web Interface AppExpert Template contains rules for the following application firewall signatures and security checks:

- "**Deny URL check.**" Detects connections to content that is known to pose a security risk, or to any other URLs that you designate.
- "**Buffer Overflow check.**" Detects attempts to cause a buffer overflow on a protected web server.
- "**Cookie Consistency check.**" Detects malicious modifications to cookies set by a protected web site.
- "**Form Field Consistency check.**" Detects modifications to the structure of a web form on a protected web site.
- "**CSRF Form Tagging check.**" Detects cross-site request forgery attacks.
- "**Field Formats check.**" Detects inappropriate information uploaded in web forms on a protected web site.
- "**HTML SQL Injection check.**" Detects attempts to inject unauthorized SQL code.
- "**HTML Cross-Site Scripting check.**" Detects cross-site scripting attacks.

For information on installing and using an AppExpert Template, see "AppExpert Applications and Templates."

The Citrix NetScaler Configuration Utility

The NetScaler configuration utility is a web-based interface that provides access to all configuration options for the application firewall feature, including advanced configuration and management options that are not available from any other configuration tool or interface. Specifically, many advanced Signatures options can be configured only in the configuration utility. You can review recommendations generated by the learning feature only in the configuration utility. You can bind policies to a bind point other than Global only in the configuration utility.

For a description of the configuration utility, see "The Application Firewall User Interfaces." For more information on using the configuration utility to configure the application firewall, see "Manual Configuration By Using the Configuration Utility."

For instructions on configuring the application firewall by using the configuration utility, see "Manual Configuration By Using the Configuration Utility." For information on the Citrix NetScaler Configuration Utility, see "The Application Firewall User Interfaces."

The Citrix NetScaler Command Line Interface

The Citrix NetScaler command line interface is a modified UNIX shell based on the FreeBSD `bash` shell. To configure the Application Firewall from the command line interface, you type commands at the prompt and press the Enter key, just as you do with any other Unix shell. You can configure most parameters and options for the application firewall by using the NetScaler command line. Exceptions are the signatures feature, many of whose options can be configured only by using the configuration utility or the Application Firewall wizard, and the learning feature, whose recommendations can only be reviewed in the configuration utility.

For instructions on configuring the application firewall by using the NetScaler command line, see "Manual Configuration By Using the Command Line Interface."

Enabling the Application Firewall

Before you can create an application firewall security configuration, you must make sure that the application firewall feature is enabled.

- If you are configuring a dedicated Citrix Application Firewall appliance, the feature is already enabled. You do not have to perform either of the procedures described here.
- If you have a Citrix NetScaler appliance but have not previously configured the application firewall, you need to enable the application firewall feature before you configure it.
- If you are upgrading a NetScaler appliance from a previous version of the NetScaler operating system to the current version, you may need to enable the application firewall feature before you configure it.
- If you are installing a new application firewall appliance or NetScaler appliance, you do not need to perform this procedure.

Note: If you are upgrading a NetScaler appliance or NetScaler virtual appliance from a previous version, you may need to update the licenses on your appliance before you can enable this feature.

You can enable the application firewall by using the NetScaler command line or the configuration utility.

To enable the application firewall by using the command line interface

At the command prompt, type:

enable ns feature **AppFW**

To enable the application firewall by using the configuration utility

1. In the navigation pane, expand System and click Settings.
2. In the Settings pane, under Modes & Features, click basic features.
3. In the Configure Basic Features dialog box, select the Application Firewall check box.
4. Click OK.

The Application Firewall Wizard

Unlike most wizards, the Application Firewall wizard is designed not just to simplify the initial configuration process, but also to modify previously created configurations and to maintain your Application Firewall setup. A typical user runs the wizard multiple times, skipping some of the screens each time.

Opening the Wizard

To run the Application Firewall wizard, first open the configuration utility. Next, in the navigation pane, expand Application Firewall, and then in the details pane click Application Firewall Wizard. (For more information about the configuration utility, see "The Application Firewall User Interfaces.") Then:

1. In the navigation pane, click Application Firewall.
2. In the details pane, under Getting Started, click Application Firewall Wizard. The first screen of the wizard appears.
3. To advance to the next screen, click Next.

The Wizard Screens

The Application Firewall wizard displays the following screens, in the following order:

1. **Introduction screen.** Provides an introduction to the Application Firewall wizard. There is nothing that you can configure on this screen.
2. **Specify Name screen.** On this screen, when creating a new security configuration, you specify the name that the wizard is to assign to the configuration. The name can begin with a letter, number, or the underscore symbol, and can consist of from 1 to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) symbols. Choose a name that makes it easy for others to tell what content your new security configuration protects.

   Note: Because the wizard uses this name for both the policy and the profile, it is limited to 31 characters. Manually created policies can have names up to 127 characters in length.

   When creating an existing configuration, you select Modify Existing Configuration and then, in the Name drop-down list, select the name of the existing configuration that you want to modify.

   Note: Only policies that are bound to global or to a bind point appear in this list; you cannot modify an unbound policy by using the Application Firewall wizard. You must either manually bind it to Global or a bind point, or modify it manually. (For manual modification, in the configuration utility's Application Firewall --> Policies --> Firewall pane, select the policy and click Open).

You also select a profile type on this screen. The profile type determines the types of advanced protection (*security checks*) that can be configured. Because certain kinds of content are not vulnerable to certain types of security threats, restricting the list of available checks saves time during configuration. The types of Application Firewall profiles are:

- **Web Application (HTML).** Any HTML-based Web site that does not use XML or Web 2.0 technologies.
- **XML Application (XML, SOAP).** Any XML-based Web service.
- **Web 2.0 Application (HTML, XML, REST).** Any Web 2.0 site that combines HTML and XML-based content, such as an ATOM-based site, a blog, an RSS feed, or a wiki.

Note: If you are unsure which type of content is used on your Web site, you can choose Web 2.0 Application to ensure that you protect all types of Web application content.

3. **Specify Rule screen.** On this screen, you specify the policy rule (*expression*) that defines the traffic to be examined by this security configuration. If you are creating an initial configuration to protect your Web sites and Web services, you can simply accept the default value, `true`, which selects all web traffic .

   If you want this security configuration to examine, not all HTTP traffic that is routed through the appliance, but specific traffic, you can write a policy rule specifying the traffic that you want it to examine. Rules are written in Citrix NetScaler expressions language, which is a fully functional object-oriented programming language.

   - For a simple description of using the NetScaler expressions syntax to create Application Firewall rules, and a list of useful rules, see "Firewall Policies."
   - For a detailed explanation of how to create policy rules in NetScaler expressions syntax, see "Policies and Expressions."

   Note: In addition to the default expressions syntax, for backward compatibility the NetScaler operating system supports the NetScaler classic expressions syntax on NetScaler Classic and nCore appliances and virtual appliances. Classic expressions are not supported on NetScaler Cluster appliances and virtual appliances. Current users who want to migrate their existing configurations to the NetScaler cluster must migrate any policies that contain classic expressions to the default expressions syntax.

4. **Select Signature Protections screen.** On this screen, you select the categories of signatures that you want to use to protect your web sites and web services. The default categories are:

   - **CGI.** Protection against attacks on web sites that use CGI scripts in any language, including PERL scripts, Unix shell scripts, and Python scripts.
   - **Cold Fusion.** Protection against attacks on web sites that use the Adobe Systems® ColdFusion® Web development platform.
   - **FrontPage.** Protection against attacks on web sites that use the Microsoft® FrontPage® Web development platform.

- **PHP.** Protection against attacks on web sites that use the PHP open-source Web development scripting language.
- **Client side.** Protection against attacks on client-side tools used to access your protected web sites, such as Microsoft Internet Explorer, Mozilla Firefox, the Opera browser, and the Adobe Acrobat Reader.
- **Microsoft IIS.** Protection against attacks on Web sites that run the Microsoft Internet Information Server (IIS).
- **Miscellaneous.** Protection against attacks on other server-side tools, such as Web servers and database servers.

If you are creating a new security configuration, the signature categories that you select are enabled, and by default they are recorded in a new signatures object. The new signatures object is assigned the same name that you entered on the Specify name screen as the name of the security configuration.

If you have previously configured signatures objects and want to use one of them as the signatures object associated with the security configuration that you are creating, click Select Existing Signature and select a signatures object from the Signatures list.

If you are modifying an existing security configuration, you can click Select Existing Signature and assign a different signatures object to the security configuration.

5. **Select Signature Actions screen.** On this screen, you select the actions associated with the signature categories that you selected on the Select signature protections screen. If you are creating an initial configuration, you might want to accept the defaults, which enable the Log and Stats actions but not the Block action. You can decide later, after reviewing the collected logs and statistics, which signatures you should use to block traffic, and then enable the Block action for those signatures. Signatures are designed to catch specific known attacks on your web sites, and therefore they have extremely low false positive rates. However, with any new configuration, you should probably observe how the settings you chose are working before you use them to block traffic.

   If you select More for one of the signature categories, the Configure Actions for Signatures dialog box appears. Its contents are the same as the contents of the Modify Signatures Object dialog box, as described in "To Configure a Signatures Object."

   If the signatures object has already logged connections, you can click Logs to display the Syslog Viewer with the logs, as described in "Logs, Statistics, and Reports." If a signature is blocking legitimate access to your protected web site or web service, you can create and implement a relaxation for that signature by selecting a log that shows the unwanted blocking, and then clicking Deploy.

6. **Select Advanced Protections screen.** On this screen, you choose the advanced protections (also called *security checks* or simply *checks*) that you want to use to protect your web sites and web services. The checks are divided into categories. Which categories are available (and which checks are available within a category) depends on the profile type that you chose on the Specify Name screen. All checks are available for Web 2.0 Application profiles. If you chose that profile type, the Select advanced protections screen displays the following categories of security checks:

   - Top--level protections (Some checks appear at the top level, not in any category.)
   - Data Leak Prevention Protections

- Advanced Form Protections
- URL Protections
- XML Protections

To display the individual checks in a category, click the icon to the left of the category. To apply a security check to your filtered data, select the check box next to the name of the security check. For descriptions of the security checks see "Advanced Protections" and its subtopics.

7. **Select Advanced Actions screen.** On this screen, you configure the actions for the advanced protections that you have enabled.

   Note: If no advanced protections are enabled, the Wizard skips the Advanced Actions screen and goes directly to the Summary screen.

   The actions that you can configure are:

   - **Block.** Block connections that match the signature. Disabled by default.
   - **Log.** Log connections that match the signature for later analysis. Enabled by default.
   - **Stats.** Maintain statistics, for each signature, that show how many connections it matched and provide certain other information about the types of connections that were blocked. Disabled by default.
   - **Learn.** Observe traffic to this Web site or Web service, and use connections that repeatedly violate this check to generate recommended exceptions to the check, or new rules for the check. Available only for some checks.

   To enable or disable an action for a check, in the list, select or clear the check box for that action to the right of that check.

   To configure other parameters for those checks that have them, in the list, click the blue chevron to the far right of that check. In the dialog box that appears, configure the parameters. These vary from check to check. You can also select a check and, at the bottom of the dialog box, click Open to display a dialog box for modifying any of the options for that check. These dialog boxes also vary from check to check. Most of them include a Checks tab and a General tab. If the check supports relaxations, the Checks tab includes an Add button, which opens yet another dialog box, in which you can specify a relaxation for the check. A relaxation is a rule for exempting specified traffic from the check.

   For information about the settings available for a check, see the detailed description of that check.

   To review the recommendations generated by the learning engine for a specific check, select that check and then click Learned Violations to open the Manage Learned Rules dialog box for that check. For more information on how learning works and how to configure exceptions (relaxations) or deploy learned rules for a check, see "Manual Configuration By Using the Configuration Utility" under To configure and use the learning feature

   To view all logs for a specific check, select that check, and then click Logs to display the Syslog Viewer, as described in "Logs, Statistics, and Reports." If a security check is

blocking legitimate access to your protected web site or web service, you can create and implement a relaxation for that security check by selecting a log that shows the unwanted blocking, and then clicking Deploy.

8. **Summary screen.** On this screen, you review your configuration choices to verify that they are what you want. If you want to make changes, you click Back until you have returned to the appropriate screen, and make your changes. If the configuration is as you want it, you click Finish to save it , and then click Exit to close the Application Firewall wizard.

Following are four procedures that show how to perform specific types of configuration by using the Application Firewall wizard.

To configure the Application Firewall: Initial Configuration

1. In the navigation pane, click Application Firewall.
2. In the details pane, under Getting Started, click Application Firewall Wizard.
3. On the Application Firewall wizard, Introduction screen, in the lower right-hand corner, click Next.
4. On the Specify Name screen, in the Name text box, type a name for your new security configuration, and from the Type drop-down list, select the type of security configuration. Then, click Next.
5. On the Specify Rule screen, click Next again.

   Note: The default rule, `true`, protects all Web traffic that is sent via your NetScaler appliance or virtual appliances. You can create specific security configurations to protect specific parts of your Web sites or Web applications later.
6. On the Select Signature Protections screen, select check boxes to specify the groups of signatures that are appropriate for protecting the content on your protected web sites, and then click Next.

   For more information about signatures, see "Signatures."
7. On the Select Signature Actions screen, select or clear the associated check boxes to choose the signature actions that you want for each signature category that you selected in the previous step, and then click Next.
8. On the Select Advanced Protections screen, click Next again.

   You typically do not need to configure the security checks during initial configuration.
9. On the Summary screen, review your choices to verify that they are what you want. Then, click Finish, or click Back to return to a previous screen and make changes. When you are finished, click Exit to close the Application Firewall wizard.

To configure the Application Firewall: Enabling Blocking for Signatures

1. In the navigation pane, click Application Firewall.
2. In the details pane, under Getting Started, click Application Firewall Wizard.
3. On the Application Firewall wizard, Introduction screen, in the lower right-hand corner, click Next.
4. On the Specify Name screen, select Modify Existing Configuration and, in the Name drop-down list, choose the security configuration that you created during simple configuration, and then click Next.
5. In the Specify Rule screen, click Next again.
6. In the Select Signature Protections screen, click Next again.
7. In the Select Signature Actions screen, enable blocking for your chosen signatures by selecting the Block check box to the left of each of those signature.

   For more information about which signatures to consider for blocking and how to determine when you can safely enable blocking for a signature, see "Signatures."
8. In the Select advanced protections screen, click Next.
9. On the Summary screen, review your choices to verify that they appear correct. Then, click Finish, or click Back to return to the Select Signature Actions screen and make changes. When you are finished, click Exit to close the Application Firewall wizard.

To configure the Application Firewall: Enabling and Configuring advanced protection

1. In the navigation pane, click Application Firewall.
2. In the details pane, under Getting Started, click Application Firewall Wizard.
3. On the Application Firewall wizard, Introduction screen, in the lower right-hand corner, click Next.
4. On the Specify Name screen, select Modify Existing Configuration and, in the Name drop-down list, choose the security configuration that you created during simple configuration. Then, click Next.
5. On the Specify Rule screen, click Next again.
6. On the Select Signature Protections screen, click Next.
7. On the Select Signature Actions screen, click Next again.
8. On the Select advanced protections screen, select the check box beside each security check that you want to enable, and then click Next.

   For information about the security checks, see "Advanced Protections" and its subtopics.
9. On the Select Deep Actions screen, select check boxes to specify the actions that you want the Application Firewall to perform for each security check, and then click Next.

   For general information about the actions, see "Advanced Protections" and its subtopics. For information about the learning feature, which is available for some security checks, see "To configure and use the Learning feature."
10. On the Summary screen, review your choices to verify that they appear correct. Then, click Finish, or click Back to return to the Select Signature Actions screen and make changes. When you are finished, click Exit to close the Application Firewall wizard.

To configure the Application Firewall: Creating A Policy

The following procedure describes how to use the Application Firewall wizard to create a specialized security configuration to protect only specific content. In this case, you create a new security configuration instead of modifying the initial configuration. This type of security configuration requires a custom rule, so that the policy applies the configuration to only the selected Web traffic.

1. In the navigation pane, click Application Firewall.
2. In the details pane, under Getting Started, click Application Firewall Wizard.
3. On the Application Firewall wizard, Introduction screen, in the lower right-hand corner, click Next.

4. On the Specify Name screen, type a name for your new security configuration in the Name text box, select the type of security configuration from the Type drop-down list, and then click Next.

5. On the Specify Rule screen, enter a rule that matches only that content that you want this Web application to protect, and then click Next.

   For a description of policies and policy rules, see "Policies."

6. On the Select Signature Protections screen, choose the appropriate groups of signatures to protect the content on your protected web sites by selecting the check box beside each group of signatures, and then click Next.

   For detailed information about signatures, see "Signatures."

7. On the Select Signature Actions screen, select or clear the associated check boxes to choose the signature actions that you want for each signature category that you selected in the previous step, and then click Next. For a detailed description of actions, see "Signatures."

8. In the Select Advanced Protections screen, select the check box beside each security check that you want to enable, and then click Next.

   For detailed information about the security checks, see "Advanced Protections" and its subtopics.

9. In the Select Advanced Actions screen, select check boxes to specify the actions that you want the Application Firewall to perform for each security check. Then, click Next.

   For information about each security check to help you determine which actions to enable, see the Advanced Protections section.

10. On the Summary screen, review your choices to verify that they appear correct. Then, click Finish, or click Back to return to the Select Signature Actions screen and make changes. When you are finished, click Exit to close the wizard.

Manual Configuration

If you want to bind a profile to a bind point other than Global, you must manually configure the binding. Also, certain security checks require that you either manually enter the necessary exceptions or enable the learning feature to generate the exceptions that your Web sites and Web services need. Some of these tasks cannot be performed by using the application firewall wizard.

If you are familiar with how the application firewall works and prefer manual configuration, you can manually configure a signatures object and a profile, associate the signatures object with the profile, create a policy with a rule that matches the web traffic that you want to configure, and associate the policy with the profile. You then bind the policy to Global, or to a bind point, to put it into effect, and you have created a complete security configuration.

For manual configuration, you can use the configuration utility (a graphical interface) or the command line. Citrix recommends that you use the configuration utility. Not all configuration tasks can be performed at the command line. Certain tasks, such as enabling signatures and reviewing learned data, must be done in the configuration utility. Most other tasks are easier to perform in the configuration utility.

Manual Configuration By Using the Configuration Utility

If you need to configure the Application Firewall feature manually, Citrix recommends that you use the configuration utility. For a description of the configuration utility, see "The Application Firewall User Interfaces."

To create and configure a signatures object

Before you can configure the signatures, you must create a new signatures object from the appropriate default signatures object template. Assign the copy a new name, and then configure the copy. You cannot configure or modify the default signatures objects directly. The following procedure provides basic instructions for configuring a signatures object. For more detailed instructions, see "Manually Configuring the Signatures Feature." If you need to create your own, user defined signatures, see "The Signatures Editor."

1. In the navigation pane, expand Application Firewall, and then select Signatures.
2. In the details pane, select the signatures object that you want to use as a template, and then click Add.

   Your choices are:

   - *** Default Signatures.** Contains the signatures rules, the SQL injection rules, and the cross-site scripting rules.
   - *** XPath Injection.** Contains all of the items in the * Default Signatures, and in addition contains the XPath injection rules.
3. In the Add Signatures Object dialog box, type a name for your new signatures object, click OK, and then click Close. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), and underscore (_) symbols.
4. Select the signatures object that you created, and then click Open.
5. In the Modify Signatures Object dialog box, set the Display Filter Criteria options at the left to display the filter items that you want to configure.

   As you modify these options, the results that you specify are displayed in the Filtered Results window at the right. For more information about the categories of signatures, see "Signatures."
6. In the Filtered Results area, configure the settings for a signature by selecting and clearing the appropriate check boxes.
7. When finished, finished, click Close.

To create an application firewall profile by using the configuration utility

Creating an application firewall profile requires that you specify only a few configuration details.

1. In the navigation pane, expand Application Firewall, and then select Profiles.
2. In the details pane, click Add.
3. In the Create Application Firewall Profile dialog box, type a name for your profile.

   The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) symbols.
4. Choose the profile type from the drop-down list.

   The profile types are HTML (for HTML-based Web sites), XML (for XML-based Web services) and Web 2.0 (for blogs, RSS feeds, wikis, and other sites that contain both HTML and XML).

   Note: If you are unsure what types of content your profile will protect, you can choose Web 2.0 to make the full range of Application Firewall security checks available to protect your Web site.
5. If you plan to use the learning feature or to enable and configure a large number of advanced protections, select Advanced. Otherwise, select Basic.

   You probably should use the learning feature if you plan to configure either of the SQL injection checks, either of the cross-site scripting checks, any check that provides protection against Web form attacks, or the cookie consistency check. Unless you include the proper exceptions for your protected Web sites when configuring these checks, they can block legitimate traffic. Anticipating all of the necessary exceptions without creating any that are too broad is difficult. The learning feature makes this task much easier.
6. Click Create, and then click Close.

To configure an application firewall profile by using the configuration utility

1. Navigate to Application Firewall > Profiles.
2. In the details pane, select the profile that you want to configure, and then click Open.
3. In the Configure Application Firewall Profile dialog box, on the Security Checks tab, configure the security checks.
   - To enable or disable an action for a check, in the list, select or clear the check box for that action.
   - To configure other parameters for those checks that have them, in the list, click the blue chevron to the far right of that check. In the dialog box that appears, configure the parameters. These vary from check to check.

     You can also select a check and, at the bottom of the dialog box, click Open to display the Configure Relaxation dialog box or Configure Rule dialog box for that check. These dialog boxes also vary from check to check. Most of them include a Checks tab and a General tab. If the check supports relaxations or user-defined rules, the Checks tab includes an Add button, which opens yet another dialog box, in which you can specify a relaxation or rule for the check. (A relaxation is a rule for exempting specified traffic from the check.) If relaxations have already been configured, you can select one and click Open to modify it.

     For more information about the Configure Relaxation or Configure Rule dialog boxes, see "Configuring an Application Firewall Rule or Relaxation."
   - To review learned exceptions or rules for a check, select the check, and then click Learned Violations. In the Manage Learned Rules dialog box, select each learned exception or rule in turn.
     - To edit the exception or rule, and then add it to the list, click Edit & Deploy.
     - To accept the exception or rule without modification, click Deploy.
     - To remove the exception or rule from the list, click Skip.
   - To refresh the list of exceptions or rules to be reviewed, click Refresh.
   - To open the Learning Visualizer and use it to review learned rules, click Visualizer.
   - To review the log entries for connections that matched a check, select the check, and then click Logs. You can use this information to determine which checks are matching attacks, so that you can enable blocking for those checks. You can also use this information to determine which checks are matching legitimate traffic, so that you can configure an appropriate exemption to allow those legitimate connections. For more information about the logs, see "Logs, Statistics, and Reports."
   - To completely disable a check, in the list, clear all of the check boxes to the right of that check.
4. On the Settings tab, configure the profile settings.

- To associate the profile with the set of signatures that you previously created and configured, under Common Settings, choose that set of signatures in the Signatures drop-down list.

  Note: You may need to use the scroll bar on the right of the dialog box to scroll down to display the Common Settings section.

- To configure an HTML or XML Error Object, select the object from the appropriate drop-down list.

  Note: You must first upload the error object that you want to use in the Imports pane. For more information about importing error objects, see "Imports."

- To configure the default XML Content Type, type the content type string directly into the Default Request and Default Response text boxes, or click Manage Allowed Content Types to manage the list of allowed content types. ">>More...."

5. If you want to use the learning feature, click Learning, and configure the learning settings for the profile, as described in "Configuring and Using the Learning Feature".

6. Click OK to save your changes and return to the Profiles pane.

Configuring an Application Firewall Rule or Relaxation

You configure two different types of information in this dialog box, depending upon which security check you are configuring. In the majority of cases, you configure an exception (or *relaxation*) to the security check. If you are configuring the Deny URL check or the Field Formats check, you configure an addition (or *rule*). The process for either of these is the same.

To configure a relaxation or rule by using the configuration utility

1. Navigate to Application Firewall > Profiles.

2. In the Profiles pane, select the profile you want to configure, and then click Open.

3. In the Configure Application Firewall Profile dialog box, click the Security Checks tab. The Security Checks tab contains the list of application firewall security checks.

4. In the Security Checks window, click the check that you want to configure, and then click Open. The Modify Check dialog box for the check that you chose is displayed, with the Checks tab selected. The Checks tab contains a list of existing relaxations or rules for this check. The list might be empty if you have not either manually added any relaxations or approved any relaxations that were recommended by the learning engine. Beneath the list is a row of buttons that allow you to add, modify, delete, enable, or disable the relaxations on the list.

5. To add or modify a relaxation or a rule, do one of the following:

   - To add a new relaxation, click Add.

   - To modify an existing relaxation, select the relaxation that you want to modify, and then click Open.

   The Add Check Relaxation or Modify Check Relaxation dialog box for the selected check is displayed. Except for the title, these dialog boxes are identical.

6. Fill in the dialog box as described below. The dialog boxes for each check are different; the list below covers all elements that might appear in any dialog box.

   - **Enabled check box**—Select to place this relaxation or rule in active use; clear to deactivate it.

   - **Attachment Content Type**—The Content-Type attribute of an XML attachment. In the text area, enter a regular expression that matches the Content-Type attribute of the XML attachments to allow.

   - **Action URL**—In the text area, enter a PCRE-format regular expression that defines the URL to which data entered into the web form is delivered.

   - **Cookie**—In the text area, enter a PCRE-format regular expression that defines the cookie.

   - **Field Name**—A web form field name element may be labeled Field Name, Form Field, or another similar name. In the text area, enter a PCRE-format regular expression that defines the name of the form field.

   - **Form Origin URL**—In the text area, enter a PCRE-format regular expression that defines the URL that hosts the web form.

   - **Form Action URL**—In the text area, enter a PCRE-format regular expression that defines the URL to which data entered into the web form is delivered.

   - **Name**—An XML element or attribute name. In the text area, enter a PCRE-format regular expression that defines the name of the element or attribute.

- **URL**—A URL element may be labeled Action URL, Deny URL, Form Action URL, Form Origin URL, Start URL, or simply URL. In the text area, enter a PCRE-format regular expression that defines the URL.
- **Format**—The format section contains multiple settings that include list boxes and text boxes. Any of the following can appear:
  - **Type**—Select a field type in the Type drop-down list. To add a new field type definition, click Manage—
  - **Minimum Length**—Type a positive integer that represents the minimum length in characters if you want to force users to fill in this field. Default: 0 (Allows field to be left blank.)
  - **Maximum length**—To limit the length of data in this field, type a positive integer that represents the maximum length in characters. Default: 65535
- **Location**—Choose the element of the request that your relaxation will apply to from the drop-down list. For HTML security checks, the choices are:
  - `FORMFIELD`—Form fields in web forms.
  - `HEADER`—Request headers.
  - `COOKIE`—Set-Cookie headers.

  For XML security checks, the choices are:
  - `ELEMENT`—XML element.
  - `ATTRIBUE`—XML attribute.
- **Maximum Attachment Size**—The maximum size in bytes allowed for an XML attachment.
- **Comments**—In the text area, type a comment. Optional.

Note: For any element that requires a regular expression, you can type the regular expression, use the Regex Tokens menu to insert regular expression elements and symbols directly into the text box, or click Regex Editor to open the Add Regular Expression dialog box, and use it to construct the expression.

7. To remove a relaxation or rule, select it, and then click Remove.
8. To enable a relaxation or rule, select it, and then click Enable.
9. To disable a relaxation or rule, select it, and then click Disable.
10. To configure the settings and relationships of all existing relaxations in an integrated interactive graphic display, click Visualizer, and use the display tools.

    Note: The Visualizer button does not appear on all check relaxation dialog boxes.
11. To review learned rules for this check, click Learning and perform the steps in "To configure and use the Learning feature."
12. Click OK.

To configure the Learning feature by using the configuration utility

1. In the navigation pane, expand Application Firewall, and then select Profiles.
2. In the Profiles pane, select the profile, and then click Open.
3. Click the Learning tab. At the top of the Learning tab is list of the security checks that are available in the current profile and that support the learning feature.
4. To configure the learning thresholds, select a security check, and then type the appropriate values in the following text boxes:
   - **Minimum number threshold.** Depending on which security check's learning settings you are configuring, the minimum number threshold might refer to the minimum number of total user sessions that must be observed, the minimum number of requests that must be observed, or the minimum number of times a specific form field must be observed, before a learned relaxation is generated. Default: 1
   - **Percentage of times threshold.** Depending on which security check's learning settings you are configuring, the percentage of times threshold might refer to the percentage of total observed user sessions that violated the security check, the percentage of requests, or the percentage of times a form field matched a particular field type, before a learned relaxation is generated. Default: 0
5. To remove all learned data and reset the learning feature, so that it must start its observations again from the beginning, click Remove All Learned Data.

   Note: This button removes only learned recommendations that have not been reviewed and either approved or skipped. It does not remove learned relaxations that have been accepted and deployed.
6. Click Close to return to the Configure Application Firewall Profile dialog box.
7. Click Close to close the Configure Application Firewall Profile dialog box, and return to the Application Firewall Profile screen.

To create and configure a policy by using the configuration utility

1. Navigate to Application Firewall > Policies.
2. In the details pane, do one of the following:
   - To create a new firewall policy, click Add. The Create Application Firewall Policy is displayed.
   - To edit an existing firewall policy, select the policy, and then click Open. The Configure Application Firewall Policy is displayed.
3. If you are creating a new firewall policy, in the Create Application Firewall Policy dialog box, Policy Name text box, type a name for your new policy.

   The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 128 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) symbols.

   If you are configuring an existing firewall policy, this field is read-only. You cannot modify it.
4. Select the profile that you want to associate with this policy from the Profile drop-down list. You can create a new profile to associate with your policy by clicking New, and you can modify an existing profile by clicking Modify.
5. In the Expression text area, create a rule for your policy.
   - You can type a rule directly into the text area.
   - You can click Prefix to select the first term for your rule, and follow the prompts. See "To Create an Application Firewall Rule (Expression)" for a complete description of this process.
   - You can click Add to open the Add Expression dialog box, and use it to construct the rule. See "The Add Expression Dialog Box" for a complete description of this process.
6. Click Create or OK, and then click Close.

To create or configure an Application Firewall rule (expression)

The policy rule, also called the *expression*, defines the web traffic that the application firewall filters by using the profile associated with the policy. Like other NetScaler policy rules (or *expressions*), application firewall rules use NetScaler expressions syntax. This syntax is powerful, flexible, and extensible. It is too complex to describe completely in this set of instructions. You can use the following procedure to create a simple firewall policy rule, or you can read it as an overview of the policy creation process.

1. If you have not already done so, navigate to the appropriate location in the Application Firewall wizard or the NetScaler configuration utility to create your policy rule:

- If you are configuring a policy in the Application Firewall wizard, in the navigation pane, click Application Firewall, then in the details pane click Application Firewall Wizard, and then navigate to the Specify Rule screen.

- If you are configuring a policy manually, in the navigation pane, expand Application Firewall, then Policies, and then Firewall. In the details pane, to create a new policy, click Add. To modify an existing policy, select the policy, and then click Open.

2. On the Specify Rule screen, the Create Application Firewall Profile dialog box, or the Configure Application Firewall Profile dialog box, click Prefix, and then choose the prefix for your expression from the drop-down list. Your choices are:

   - **HTTP.** The HTTP protocol. Choose this if you want to examine some aspect of the request that pertains to the HTTP protocol.

   - **SYS.** The protected Web site(s). Choose this if you want to examine some aspect of the request that pertains to the recipient of the request.

   - **CLIENT.** The computer that sent the request. Choose this if you want to examine some aspect of the sender of the request.

   - **SERVER.** The computer to which the request was sent. Choose this if you want to examine some aspect of the recipient of the request.

   After you choose a prefix, the application firewall displays a two-part prompt window that displays the possible next choices at the top, and a brief explanation of what the selected choice means at the bottom.

3. Choose your next term.

   If you chose HTTP as your prefix, your only choice is REQ, which specifies the Request/Response pair. (The application firewall operates on the request and response as a unit instead of on each separately.) If you chose another prefix, your choices are more varied. For help on a specific choice, click that choice once to display information about it in the lower prompt window.

   When you have decided which term you want, double-click it to insert it into the Expression window.

4. Type a period after the term you just chose. You are then prompted to choose your next term, as described in the previous step. When a term requires that you type a value, fill in the appropriate value. For example, if you choose `HTTP.REQ.HEADER("")`, type the header name between the quotation marks.

5. Continue choosing terms from the prompts and filling in any values that are needed, until your expression is finished.

   Following are some examples of expressions for specific purposes.

   - **Specific web host.** To match traffic from a particular web host:

     HTTP.REQ.HEADER("Host").EQ("shopping.example.com")

     For `shopping.example.com`, substitute the name of the web host that you want to match.

- **Specific web folder or directory.** To match traffic from a particular folder or directory on a Web host:

  HTTP.REQ.URL.STARTSWITH("https//www.example.com/folder")

  For `www.example.com`, substitute the name of the web host. For `folder`, substitute the folder or path to the content that you want to match. For example, if your shopping cart is in a folder called `/solutions/orders`, you substitute that string for folder.

- **Specific type of content: GIF images.** To match GIF format images:

  HTTP.REQ.URL.ENDSWITH(".gif")

  To match other format images, substitute another string in place of `.gif`.

- **Specific type of content: scripts.** To match all CGI scripts located in the `CGI-BIN` directory:

  HTTP.REQ.URL.STARTSWITH("https//www.example.com/CGI-BIN")

  To match all JavaScripts with `.js` extensions:

  HTTP.REQ.URL.ENDSWITH(".js")

  For more information about creating policy expressions, see "Policies and Expressions."

Note: If you use the command line to configure a policy, remember to escape any double quotation marks within NetScaler expressions. For example, the following expression is correct if entered in the configuration utility:

HTTP.REQ.HEADER("Host").EQ("shopping.example.com")

If entered at the command line, however, you must type this instead:

HTTP.REQ.HEADER(\"Host\").EQ(\"shopping.example.com\")

To add a firewall rule (expression) by using the Add Expression dialog box

The Add Expression dialog box (also referred to as the *Expression Editor*) helps users who are not familiar with the NetScaler expressions language to construct a policy that matches the traffic that they want to filter.

1. If you have not already done so, navigate to the appropriate location in the Application Firewall wizard or the NetScaler configuration utility:

- If you are configuring a policy in the Application Firewall wizard, in the navigation pane, click Application Firewall, then in the details pane click Application Firewall Wizard, and then navigate to the Specify Rule screen.

- If you are configuring a policy manually, in the navigation pane, expand Application Firewall, then Policies, and then Firewall. In the details pane, to create a new policy, click Add. To modify an existing policy, select the policy, and then click Open.

2. On the Specify Rule screen, in the Create Application Firewall Profile dialog box, or in the Configure Application Firewall Profile dialog box, click Add.

3. In the Add Expression dialog box, in the Construct Expression area, in the first list box, choose one of the following prefixes:

   - **HTTP.** The HTTP protocol. Choose this if you want to examine some aspect of the request that pertains to the HTTP protocol. The default choice.

   - **SYS.** The protected Web site(s). Choose this if you want to examine some aspect of the request that pertains to the recipient of the request.

   - **CLIENT.** The computer that sent the request. Choose this if you want to examine some aspect of the sender of the request.

   - **SERVER.** The computer to which the request was sent. Choose this if you want to examine some aspect of the recipient of the request.

4. In the second list box, choose your next term. The available terms differ depending on the choice you made in the previous step, because the dialog box automatically adjusts the list to contain only those terms that are valid for the context. For example, if you selected HTTP in the previous list box, the only choice is REQ, for requests. Because the application firewall treats requests and associated responses as a single unit and filters both, you do not need to specific responses separately. After you choose your second term, a third list box appears to the right of the second. The Help window displays a description of the second term, and the Preview Expression window displays your expression.

5. In the third list box, choose the next term. A new list box appears to the right, and the Help window changes to display a description of the new term. The Preview Expression window updates to display the expression as you have specified it to that point.

6. Continue choosing terms, and when prompted filling in arguments, until your expression is complete. If you make a mistake or want to change your expression after you have already selected a term, you can simply choose another term. The expression is modified, and any arguments or additional terms that you added after the term that you modified are cleared.

7. When you have finished constructing your expression, click OK to close the Add Expression dialog box. Your expression is inserted into the Expression text area.

To bind an application firewall policy by using the configuration utility

1. In the navigation pane, expand Application Firewall, then Policies, and then select Firewall Policies.

2. In the details pane, click Policy Manager.

3. In the Application Firewall Policy Manager dialog box, choose the bind point to which you want to bind the policy. The choices are:

   - **Override Global.** Policies that are bound to this bind point process all traffic from all interfaces on the NetScaler appliance, and are applied before any other policies.

   - **LB Virtual Server.** Policies that are bound to a load balancing virtual server are applied only to traffic that is processed by that load balancing virtual server, and are applied before any Default Global policies. After selecting LB Virtual Server, you must also select the specific load balancing virtual server to which you want to bind this policy.

   - **CS Virtual Server.** Policies that are bound to a content switching virtual server are applied only to traffic that is processed by that content switching virtual server, and are applied before any Default Global policies. After selecting CS Virtual Server, you must also select the specific content switching virtual server to which you want to bind this policy.

   - **Default Global.** Policies that are bound to this bind point process all traffic from all interfaces on the NetScaler appliance.

   - **Policy Label.** Policies that are bound to a policy label process traffic that the policy label routes to them. The policy label controls the order in which policies are applied to this traffic.
4. Select Insert Policy to insert a new row and display a drop-down list with all available, unbound application firewall policies.

5. Select the policy you want to bind, or select New Policy to create a new policy. The policy that you selected or created is inserted into the list of globally bound application firewall policies.

6. Make any additional adjustments to the binding.

   - To modify the policy priority, click the field to enable it, and then type a new priority. You can also select Regenerate Priorities to renumber the priorities evenly.

   - To modify the policy expression, double click that field to open the Configure Application Firewall Policy dialog box, where you can edit the policy expression.

   - To set the Goto Expression, double click field in the Goto Expression column heading to display the drop-down list, where you can choose an expression.

   - To set the Invoke option, double click field in the Invoke column heading to display the drop-down list, where you can choose an expression
7. Repeat steps 3 through 6 to add any additional application firewall policies you want to globally bind.

8. Click OK. A message appears in the status bar, stating that the policy has been successfully bound.

Manual Configuration By Using the Command Line Interface

You can configure many application firewall features from the NetScaler command line. There are important exceptions, however. You cannot enable signatures from the command line. There are over 1,000 default signatures in seven categories; the task is simply too complex for the command line interface. You can configure the check actions and parameters for security checks from the command line, but cannot enter manual relaxations. While you can configure the adaptive learning feature and enable learning from the command line, you cannot review learned relaxations or learned rules and approve or skip them. The command line interface is intended for advanced users who are thoroughly familiar with the NetScaler appliance and the application firewall feature.

To manually configure the Application Firewall by using the NetScaler command line, use a telnet or secure shell client of your choice to log on to the NetScaler command line.

To create a profile by using the command line interface

At the command prompt, type the following commands:

- add appfw profile <name> [-defaults (**basic** | **advanced**)]
- set appfw profile <name> -type (**HTML** | **XML** | **HTML XML**)
- save ns config

Example

The following example adds a profile named `pr-basic`, with basic defaults, and assigns a profile type of `HTML`. This is the appropriate initial configuration for a profile to protect an HTML Web site.

```
add appfw profile pr-basic -defaults basic
set appfw profile pr-basic -type HTML
save ns config
```

Parameters for Creating a Profile

name (Profile Name)

A name for the profile. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) symbols.

defaults (Defaults)

You can choose one of two default configurations when you create a profile: Basic or Advanced. A profile created with basic defaults should protect most Web sites while requiring little additional configuration. A profile created with advanced defaults is intended to protect more complex Web sites requiring additional configuration. You can modify either type of default configuration.

type (Profile Type)

The type of content that the profile will protect. There are three types of profile: **HTML** (`HTML`), **XML** (`XML`), or **Web 2.0** (`HTML XML`). If you are unsure what types of content your profile will protect, you can specify Web 2.0 to make the full range of Application Firewall security checks available to protect your Web site.

To configure a profile by using the command line interface

At the command prompt, type the following commands:

- set appfw profile <name> <arg1> [<arg2> ...] where <arg1> represents a parameter and <arg2> represents either another parameter or the value to assign to the parameter represented by <arg1>. For descriptions of the parameters to use when configuring specific security checks, see Advanced Protections and its subtopics. For descriptions of the other parameters, see "Parameters for Creating a Profile."
- save ns config

Example

The following example shows how to configure an HTML profile created with basic defaults to begin protecting a simple HTML-based Web site. This example turns on logging and maintenance of statistics for most security checks, but enables blocking only for those checks that have extremely low false positive rates and require no special configuration. It also turns on transformation of unsafe HTML and unsafe SQL, which prevents attacks but does not block requests to your Web sites. With logging and statistics enabled, you can later review the logs to determine whether to enable blocking for a specific security check.

```
set appfw profile -startURLAction log stats
set appfw profile -denyURLAction block log stats
set appfw profile -cookieConsistencyAction log stats
set appfw profile -crossSiteScriptingAction log stats
set appfw profile -crossSiteScriptingTransformUnsafeHTML ON
set appfw profile -fieldConsistencyAction log stats
set appfw profile -SQLInjectionAction log stats
set appfw profile -SQLInjectionTransformSpecialChars ON
set appfw profile -SQLInjectionOnlyCheckFieldsWithSQLChars ON
set appfw profile -SQLInjectionParseComments checkall
set appfw profile -fieldFormatAction log stats
set appfw profile -bufferOverflowAction block log stats
set appfw profile -CSRFtagAction log stats
```

save ns config

To create and configure a policy

At the command prompt, type the following commands:

- add appfw policy <name> <rule> <profile>
- save ns config

Example

The following example adds a policy named `pl-blog`, with a rule that intercepts all traffic to or from the host `blog.example.com`, and associates that policy with the profile `pr-blog`. This is an appropriate policy to protect a blog hosted on a specific hostname.

```
add appfw policy pl-blog "HTTP.REQ.HOSTNAME.DOMAIN.EQ("blog.example.com")" pr-blog
```

Parameters for creating and configuring a policy

name

A name for your policy. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 128 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols.

rule

A policy rule, or expression, in NetScaler expressions language. For a short description and some useful examples of Application Firewall rules, see "Manually Configuring Firewall Policies." For a complete description of the NetScaler expressions language, see "Introduction to Policies and Expressions."

profile

The name of the profile that you previously created.

To bind an Application Firewall policy

At the command prompt, type the following commands:

- bind appfw global <policyName> <priority>
- save ns config

Example

The following example binds the policy named `pl-blog` and assigns it a priority of `10`.

```
bind appfw global pl-blog 10
save ns config
```

Signatures

The application firewall signatures function provides specific, configurable rules that protect your web sites against known attacks. A signature represents a pattern that is a component of a known attack on an operating system, a web server, a web site, an XML-based web service, or any other server that is connected to a web site or web service. A signature can be used to check either requests or responses. A signature can consist of a literal string or a PCRE-compliant regular expression.

To specify how the application firewall is to use signatures, you configure a signatures object, which specifies the signatures to apply to your traffic and the actions to be taken when the signatures match the traffic. A signatures object also contains the SQL injection and cross-site scripting patterns, and may also contain XPath injection patterns. These patterns are not actually signatures but are used by some of the advanced protection checks. The SQL Injection and Cross-Site Scripting patterns contain the SQL special symbols and keywords, the cross-site scripting allowed tags and attributes, and the denied patterns for the HTML and XML SQL Injection and Cross-Site Scripting checks. The XPath injection patterns contain the XPath (*XML Path Language*) denied patterns.

Note: If you use the wizard to configure signatures, the signatures object is created automatically.

The application firewall examines requests to your protected web sites and web services to determine whether a request matches a signature. Matching requests are handled as you specify when configuring the Signatures actions. By default, matching requests are logged so that you can examine them later. If you enabled blocking, the application firewall displays an error page or error object. If you enabled statistics, the application firewall also includes the request in the statistics that it maintains about requests that match an application firewall signature or security check.

If you want to configure signatures manually, you must create a signatures object from a template or import a signatures object file. There are two default templates that you can use: the *Default Signatures template and the *Xpath Injection template. The *Default Signatures template contains over 1,000 signatures, in addition to the complete list of SQL injection and cross-site scripting allowed and denied patterns. The *Xpath Injection template contains all of those, and in addition contains 57 Xpath keywords and special strings.

In addition to using its native signatures format, the application firewall can create a signatures object by using a built-in template for any supported external signatures format, or by importing an external signatures file in a supported format. The supported formats are as follows:

- **Cenzic**—Signatures files, produced by Cenzic products, that use Cenzic Hailstorm technology.
- **IBM AppScan**—Signatures files produced by IBM AppScan Enterprise and IBM AppScan Standard.
- **Qualys**—Qualys WAS signatures files produced by QualysGuard products. Only Qualys WAS 1.0 files are supported for importing as signatures. WAS 2.0 is not supported.

Note: Qualys classifies a single SQL special character in a URL as a security threat, even when no SQL keywords are present. The SQL injection check does not consider the presence of a single SQL special character a threat unless an SQL keyword is present. For that reason, a Qualys scanner continues to report such requests as containing SQL injection vulnerabilities, but the application firewall does not detect or block these requests because they pose no actual threat to your protected web sites and web services.

- **Trend Micro**—Signatures files produced by the Trend Micro Vulnerability Scanner (TMVS).

- **Whitehat**—WASC 1.0, WASC 2.0, and best practices signatures produced by Whitehat Sentinel products.

  WASC signatures include information about many vulnerabilities. The application firewall generates blocking signatures from all WASC vulnerabilities. However, only certain vulnerabilities are appropriate for the web application firewall environment. For a list of appropriate Whitehat signatures, see Whitehat WASC Signature Types for WAF Use.

Once you have created a signatures object, you can configure all parts of it, including the signatures rules, the XML SQL Injection and Cross-Site Scripting rules, and the Xpath injection rules. You can manually create and modify your own custom signatures in the signatures editor. You can also add new SQL injection, cross-site scripting, and XPath injection patterns, modify existing patterns, and remove patterns.

Regardless of whether you use the wizard for initial configuration or configure your signatures object manually, you should regularly apply the Citrix updates to keep your signatures current. Citrix regularly updates the default application firewall signatures. You can apply those updates manually, or you can enable automatic signature updates so that the application firewall can update the signatures from the Cloud-based application firewall updates service. You can obtain the correct URL for either type of updates from your Citrix service representative or reseller.

Manually Configuring the Signatures Feature

To use signatures to protect your web sites, you must review the rules, and enable and configure the ones that you want to apply. The rules are disabled by default. Citrix recommends that you enable all rules that are applicable to the type of content that your web site uses.

To manually configure the signatures feature, use a browser to connect to the configuration utility. Then, create a signatures object from a built-in template, an existing signatures object, or by importing a file. Next, configure the new signatures object.

Note: The following procedures do not address adding user-defined signatures to a signatures object. To create your own signatures, see "The Signatures Editor."

Adding a New Signatures Object

You can add a new signatures object to the application firewall by:

- Copying either a built-in template or an existing signatures object.
- Importing a signatures object from an external file.

To create a signatures object from a template

1. Navigate to Application Firewall > Signatures.
2. In the details pane, select the signatures object that you want to use as a template.

   Your choices are:

   - *** Default Signatures.** Contains the signatures rules, the SQL injection rules, and the cross-site scripting rules.
   - *** XPath Injection.** Contains everything that is in the *** Default Signatures** template, and also contains the XPath injection rules.
   - **Any existing signatures object.**
3. Click Add.
4. In the Add Signatures Object dialog box, type a name for your new signatures object, and then click OK. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), and underscore (_) symbols.
5. Click Close.

To create a signatures object by importing a file

1. Navigate to Application Firewall > Signatures.
2. In the details pane, click Add.
3. In the Add Signatures Object dialog box, select the External Format tab.
4. Choose the external format file that you want to use to create your new signatures object.
   - To import a native NetScaler format signatures object file, in the Import section select either Import from Local File or Import from URL, then type or browse to the path or URL to the file.
   - To import a Cenzic, IBM AppScan, Qualys, or Whitehat format file, in the XSLT section select Use Built-in XSLT File, Use Local File, or Reference from URL. Next, if you chose Use Built-in XSLT File, select the appropriate file format from the drop-down list. If you chose Use Local File or Reference from URL, then type or browse to the path or URL to the file.
5. Click Add, and then click Close.

Configuring or Modifying a Signatures Object

You configure a signatures object after creating it, or modify an existing signatures object, to enable or disable signature categories or specific signatures, and configure how the application firewall responds when a signature matches a connection.

To configure or modify a signatures object

1. Navigate to Application Firewall > Signatures.
2. In the details pane, select the signatures object that you want to configure, and then click Open.
3. In the Modify Signatures Object dialog box, set the Display Filter Criteria options at the left to display the filter items that you want to configure.

   As you modify these options, the results that you requested are displayed in the Filtered Results window at the right.

   - To display only selected categories of signatures, check or clear the appropriate signature-category check boxes. The signature categories are:

Name	Type of Attack that this Signature Protects Against
cgi	CGI scripts. Includes Perl and UNIX shell scripts.
client	Browsers and other clients.
coldfusion	Web sites that use the Adobe Systems ColdFusion application server.
frontpage	Web sites that use Microsoft's FrontPage server.
iis	Web sites that use the Microsoft Internet Information Server (IIS).
misc	Miscellaneous attacks.
php	Web sites that use PHP

   - To display only signatures that have specific check actions enabled, select the ON check box for each of those actions, clear the ON check boxes for the other actions, and clear all of the OFF check boxes. To display only signatures that have a specific check action disabled, select their respective OFF check boxes and clear all of the ON check boxes. To display signatures regardless of whether they have a check action enabled or disabled, select or clear both the ON and the OFF check boxes for that action. The check actions are:

Criterion	Description
Enabled	The signature is enabled. The application firewall checks only for signatures that are enabled when it processes traffic.
Block	Connections that match this signature are blocked.
Log	A log entry is produced for any connection that matches this signature.
Stats	The application firewall includes any connection that matches this signature in the statistics that it generates for that check.

   - To display only signatures that contain a specific string, type the string into the text box under the filter criteria, and then click Search.
   - To reset all display filter criteria to the default settings and display all signatures, click Show All.

4. For information about a specific signature, select the signature, and then click the blue double arrow to the left of the Category field. The Signature Rule Vulnerability Detail message box appears. It contains information about the purpose of the signature and provides links to external web-based information about the vulnerability or vulnerabilities that this signature addresses. To access an external link, click the blue double arrow to the left of the description of that link.

5. Configure the settings for a signature by selecting the appropriate check boxes.

6. If you want to add a local signature rule to the signatures object, or modify an existing local signature rule, see "The Signatures Editor."

7. If you have no need for SQL injection, cross-site scripting, or Xpath injection patterns, click OK, and then click Close. Otherwise, in the lower left-hand corner of the details pane, click Manage SQL/XSS Patterns.

8. In the Manage SQL/XSS Patterns dialog box, Filtered Results window, navigate to the pattern category and pattern that you want to configure. For information about the SQL injection patterns, see "HTML SQL Injection Check." For information about the cross-site scripting patterns, see "HTML Cross-Site Scripting Check."

9. To add a new pattern:

    a. Select the branch to which you want to add the new pattern.

    b. Click the Add button directly below the lower section of the Filtered Results window.

    c. In the Create Signature Item dialog box, fill in the Element text box with the pattern that you want to add. If you are adding a transformation pattern to the transform rules branch, under Elements, fill in the From text box with the pattern that you want to change and the To text box with the pattern to which you want to change the previous pattern.

    d. Click OK.

10. To modify an existing pattern:

    a. In the Filtered Results window, select the branch that contains the pattern that you want to modify.

    b. In the detail window beneath the Filtered Results window, select the pattern that you want to modify.

    c. Click Modify.

    d. In the Modify Signature Item dialog box, Element text box, modify the pattern. If you are modifying a transformation pattern, you can modify either or both patterns under Elements, in the From and the To text boxes.

    e. Click OK.

11. To remove a pattern, select the pattern that you want to remove, then click the Remove button below the details pane beneath the Filtered Results window. When prompted, confirm your choice by clicking Close.

12. To add the patterns category to the XSS branch:

a. Select the branch to which you want to add the patterns category.

b. Click the Add button directly below the Filtered Results window.

Note: Currently you can add only one category, named patterns, to the XSS branch, so after you click Add, you must accept the default choice, which is `patterns`.

c. Click OK.

13. To remove a branch, select that branch, and then click the Remove button directly below the Filtered Results window. When prompted, confirm your choice by clicking OK.

Note: If you remove a default branch, you remove all of the patterns in that branch. Doing so can disable the security checks that use that information.

14. When you are finished modifying the SQL injection, cross-site scripting, and XPath injection patterns, click OK, and then click Close to return to the Modify Signatures Object dialog box.

15. Click OK at any point to save your changes, and when you are finished configuring the signatures object, click Close.

Updating a Signatures Object

You should update your signatures objects frequently to ensure that your application firewall is providing protection against current threats. You should regularly update both the default application firewall signatures and any signatures that you import from a supported vulnerability scanning tool.

Citrix regularly updates the default signatures for the application firewall. You can update the default signatures manually or automatically. In either case, ask your Citrix representative or Citrix reseller for the URL to access the updates. You can enable automatic updates of the Citrix native format signatures in the "Engine Settings" and "Signature Auto Update Settings" dialog box.

Most makers of vulnerability scanning tools regularly update the tools. Most web sites also change frequently. You should update your tool and rescan your web sites regularly, exporting the resulting signatures to a file and importing them into your application firewall configuration.

Note: When you update the application firewall signatures from the NetScaler command line, you must first update the deafult signatures, and then issue additional update commands to update each custom signatures file that is based on the default signatures. If you do not update the default signatures first, a version mismatch error prevents updating of the custom signatures files.

To update a signatures object from a Citrix format file by using the configuration utility

1. Navigate to Application Firewall > Signatures.
2. In the details pane, select the signatures object that you want to update.
3. In the Action drop-down list, select Merge.
4. In the Update Signatures Object dialog box, choose one of the following options.
   - **Import from URL**—Choose this option if you download signature updates from a web URL.
   - **Import from Local File**—Choose this option if you import signature updates from a file on your local hard drive, network hard drive, or other storage device.
5. In the text area, type the URL, or type or browse to the local file.
6. Click Update. The update file is imported, and the Update Signatures dialog box changes to a format nearly identical to that of the Modify Signatures Object dialog box, which is described in "Configuring or Modifying a Signatures Object" and "To configure or modify a signatures object." The Update Signatures Object dialog box displays all branches with new or modified signature rules, SQL injection or cross-site scripting patterns, and XPath injection patterns if there are any.
7. Review and configure the new and modified signatures.
8. When you are finished, click OK, and then click Close.

To import and update signatures from a vulnerability scanning tool

1. Navigate to Application Firewall > Signatures.
2. In the details pane, select the signatures object that you want to update, and then click Update.
3. In the Update Signatures Object dialog box, on the External Format tab, Import section, choose one of the following options.
   - **Import from URL**—Choose this option if you download signature updates from a Web URL.
   - **Import from Local File**—Choose this option if you import signature updates from a file on your local or a network hard drive or other storage device.
4. In the text area, type the URL, or browse or type the path to the local file.
5. In the XSLT section, choose one of the following options.
   - **Use Built-in XSLT File**—Choose this option if you want to use a built-in XSLT files.
   - **Use Local File**—Choose this option to use an XSLT file on your local computer.
   - **Reference from URL**—Choose this option to import an XSLT file from a web URL.
6. If you chose Use Built-in XSLT File, in the Built-In XSLT drop-down list choose the built-in XSLT file that you want to use.
   - To use the Cenzic XSLT file, select Cenzic.
   - To use the IBM AppScan Standard XSLT file, select IBM AppScan Standard.
   - To use the IBM AppScan Enterprise XSLT file, select IBM AppScan Enterprise.
   - To use the Qualys XSLT file, select Qualys.
   - To use the Trend Microsystems XSLT file, select Trend Micro.
   - To use the Whitehat XSLT file, select Whitehat.
7. Click Update. The update file is imported, and the Update Signatures dialog box changes to a format nearly identical to that of the Modify Signatures Object dialog box, which is described in "Configuring or Modifying a Signatures Object." The Update Signatures Object dialog box displays all branches with new or modified signature rules, SQL injection or cross-site scripting patterns, and XPath injection patterns if there are any.
8. Review and configure the new and modified signatures.
9. When you are finished, click OK, and then click Close.

Updating a Signatures Object from a Citrix Format File

Citrix regularly updates the signatures for the Application Firewall. You should regularly update the signatures on your Application Firewall to ensure that your Application Firewall is using the most current list. Ask your Citrix representative or Citrix reseller for the URL to access the updates.

To update a signatures object from a Citrix format file by using the command line

At the command prompt, type the following commands:

- update appfw signatures <name> [-mergeDefault]
- save ns config

To update a signatures object from a Citrix format file by using the configuration utility

1. Navigate to Application Firewall > Signatures.
2. In the details pane, select the signatures object that you want to update.
3. In the Action drop-down list, select Merge.
4. In the Update Signatures Object dialog box, choose one of the following options.
   - **Import from URL**—Choose this option if you download signature updates from a web URL.
   - **Import from Local File**—Choose this option if you import signature updates from a file on your local hard drive, network hard drive, or other storage device.
5. In the text area, type the URL, or type or browse to the local file.
6. Click Update. The update file is imported, and the Update Signatures dialog box changes to a format nearly identical to that of the Modify Signatures Object dialog box, which is described in "Configuring or Modifying a Signatures Object" and "To configure or modify a signatures object." The Update Signatures Object dialog box displays all branches with new or modified signature rules, SQL injection or cross-site scripting patterns, and XPath injection patterns if there are any.
7. Review and configure the new and modified signatures.
8. When you are finished, click OK, and then click Close.

Updating a Signatures Object from a Supported Vulnerability Scanning Tool

Note: Before you update a signatures object from a file, you must create the file by exporting signatures from the vulnerability scanning tool.

To import and update signatures from a vulnerability scanning tool

1. Navigate to Application Firewall > Signatures.
2. In the details pane, select the signatures object that you want to update, and then click Update.
3. In the Update Signatures Object dialog box, on the External Format tab, Import section, choose one of the following options.
   - **Import from URL**—Choose this option if you download signature updates from a Web URL.
   - **Import from Local File**—Choose this option if you import signature updates from a file on your local or a network hard drive or other storage device.
4. In the text area, type the URL, or browse or type the path to the local file.
5. In the XSLT section, choose one of the following options.
   - **Use Built-in XSLT File**—Choose this option if you want to use a built-in XSLT files.
   - **Use Local File**—Choose this option to use an XSLT file on your local computer.
   - **Reference from URL**—Choose this option to import an XSLT file from a web URL.
6. If you chose Use Built-in XSLT File, in the Built-In XSLT drop-down list choose the built-in XSLT file that you want to use.
   - To use the Cenzic XSLT file, select Cenzic.
   - To use the IBM AppScan Standard XSLT file, select IBM AppScan Standard.
   - To use the IBM AppScan Enterprise XSLT file, select IBM AppScan Enterprise.
   - To use the Qualys XSLT file, select Qualys.
   - To use the Trend Microsystems XSLT file, select Trend Micro.
   - To use the Whitehat XSLT file, select Whitehat.
7. Click Update. The update file is imported, and the Update Signatures dialog box changes to a format nearly identical to that of the Modify Signatures Object dialog box, which is described in "Configuring or Modifying a Signatures Object." The Update Signatures Object dialog box displays all branches with new or modified signature rules, SQL injection or cross-site scripting patterns, and XPath injection patterns if there are any.
8. Review and configure the new and modified signatures.
9. When you are finished, click OK, and then click Close.

Exporting a Signatures Object to a File

You export a signatures object to a file so that you can import it to another application firewall.

To export a signatures object to a file

1. Navigate to Application Firewall > Signatures.
2. In the details pane, select the signatures object that you want to configure.
3. In the Actions drop-down list, select Export.
4. In the Export Signatures Object dialog box, Local File text box, type the path and name of the file to which you want to export the signatures object, or use the Browse dialog to designate a path and name.
5. Click OK.

The Signatures Editor

You can use the signatures editor, which is available in the configuration utility, to add a new user-defined (*local*) signature rule to an existing signatures object, or to modify a previously configured local signature rule. Except that it is defined by the user (you), a local signature rule has the same attributes as a default signature rule from Citrix, and it functions in the same way. You enable or disable it, and configure the signature actions for it, just as you do for a default signature.

Add a local rule if you need to protect your web sites and services from a known attack that the existing signatures do not match. For example, you might discover a new type of attack and determine its characteristics by examining the logs on your web server, or you might obtain third-party information about a new type of attack.

At the heart of a signature rule are the rule *patterns*, which collectively describe the characteristics of the attack that the rule is designed to match. Each pattern can consist of a simple string, a PCRE-format regular expression, or the built-in SQL injection or cross-site scripting patterns.

You might want to modify a signature rule by adding a new pattern or modifying an existing pattern to match an attack. For example, you might find out about changes to an attack, or you might determine a better pattern by examining the logs on your web server, or from third-party information.

Parameters for the Signature Editor

Actions

The Enabled, Block, Log, and Stats check boxes. Select or clear the check boxes as appropriate to configure what the Application Firewall does when the signature rule is matched.

- To enable the signature rule, select Enabled.
- To enable blocking for the signature rule, select Block.
- To enable logging for the signature rule, select Log.
- To enable maintaining of statistics for the signature rule, select Stats.

Category

The category in which the signature rule is included. Assigning a signature to a category enables you to configure it and other signatures in that category as a group, which can significantly speed up the configuration process when you want to configure many signature rules in the same way.

LogString

A brief string (a few words or a short sentence) that describes the attack that this signature rule matches. This string is used when logging a match to the NetScaler log.

Comment

A longer description of the attack and the signature rule, with information that another user who is configuring this signature object would need to know. Optional.

Patterns

The patterns that describe the characteristics of the attack that this signature rule should match. Patterns can be fixed strings, PCRE-format regular expressions, or the built-in SQL injection or cross-site scripting patterns. See "Signature Rule Patterns" for more information.

Note: If a signature rule has more than one pattern, a match does not occur unless all of the patterns match the data to which the rule is compared. If either of two patterns can define an attack, but both would not necessarily be present, you should create two signature rules.

To add or modify a local signature rule by using the Signatures Editor

1. Navigate to Application Firewall > Signatures.
2. In the details pane, select the signatures object that you want to edit, and then click Open.
3. In the Modify Signatures Object dialog box, in the middle of the screen beneath the Filtered Results window, do one of the following:.
   - To add a new local signature rule, click Add.
   - To modify an existing local signature rule, select that rule, and then click Open.
4. In the Add Local Signature Rule or the Modify Local Signature Rule dialog box, configure the actions for a signature by selecting the appropriate check boxes.
   - **Enabled.** Enables the new signature rule. If you do not select this, this new signature rule is added to your configuration, but is inactive.
   - **Block.** Blocks connections that violate this signature rule.
   - **Log.** Logs violations of this signature rule to the NetScaler log.
   - **Stats.** Includes violations of this signature rule in the statistics.
   - **Strip.** Removes comments from the request or response before applying the signature rule.
   - **Remove.** Strips information that matches the signature rule from the response. (Applies only to response rules.)
   - **X-Out.** Masks information that matches the signature rule with the letter X. (Applies only to response rules.)
   - **Allow Duplicates.** Allows duplicates of this signature rule in this signatures object.
5. Choose a category for the new signature rule from the Category drop-down list.

   You can also create a new category by clicking the icon to the right of the list and using the Add Signature Rule Category dialog box to add a new category to the list, The rule you are modifying is automatically added to the new category. For instructions, see "To add a signature rule category."
6. In the **LogString** text box, type a brief description of the signature rule to be used in the logs.
7. In the **Comment** text box, type a comment. (Optional)
8. Click More..., and modify the advanced options.
   a. To strip HTML comments before applying this signature rule, in the Strip Comments drop-down list choose All or Exclude Script Tag.

b. To set CSRF Referer Header checking, in the CSRF Referer Header checking radio button array, select either the If Present or Always radio button.

c. To manually modify the Rule ID assigned to this local signature rule, modify the number in the Rule ID text box. The ID must be a positive integer between 1000000 and 1999999 that has not already been assigned to a local signature rule.

d. To assign a version number to the new signature rule, modify the number in the Version Number text box.

e. To assign a Source ID, modify the string in the Source ID text box.

f. To specify the source, choose Local or Snort from the Source drop-down list, or click the Add icon to the right of the list and add a new source.

g. To assign a harm score to violations of this local signature rule, type a number between 1 and 10 in the Harm Score text box.

h. To assign a severity rating to this local signature rule, in the Severity drop-down list choose High, Medium, or Low, or click the Add icon to the right of the list and add a new severity rating.

i. To assign a violation type to this local signature rule, in the Type drop-down list choose Vulnerable or Warning, or click the Add icon to the right of the list and add a new violation type.

9. In the **Patterns** list, add or edit a pattern.

   · To add a pattern, click Add. In the Create New Signature Rule Pattern dialog box, add one or more patterns for your signature rule, and then click OK.

   · To edit a pattern, select the pattern, and then click Open. In the Edit Signature Rule Pattern dialog box, modify the pattern, and then click OK.

   For more information about adding or editing patterns, see "Signature Rule Patterns."

10. Click OK.

To add a signature rule category

Putting signature rules into a category enables you to configure the actions for a group of signatures instead of for each individual signature. You might want to do so for the following reasons:

- **Ease of selection.** For example, assume that all of signature rules in a particular group protect against attacks on a specific type of web server software or technology. If your protected web sites use that software or technology, you want to enable them all. If they do not, you do not want to enable any of them.
- **Ease of initial configuration.** It is easiest to set defaults for a group of signatures as a category, instead of one-by-one. You can then make any changes to individual signatures as needed.
- **Ease of ongoing configuration.** It is easier to configure signatures if you can display only those that meet specific criteria, such as belonging to a specific category.

1. Navigate to Application Firewall > Signatures.
2. In the details pane, select that signatures object that you want to configure, and then click Open.
3. In the Modify Signatures Object dialog box, in the middle of the screen, beneath the Filtered Results window, click Add.
4. In the Add Local Signature Rule dialog box, click the icon to the right of the Category drop-down list.
5. In the Add Signature Rule Category dialog box, New Category text box, type a name for your new signature category. The name can consist of from one to 64 characters.
6. Click **OK**.

Signature Rule Patterns

You can add a new pattern to a signature rule or modify an existing pattern of a signature rule to specify a string or expression that characterizes an aspect of the attack that the signature matches. To determine which patterns an attack exhibits, you can examine the logs on your web server, use a tool to observe connection data in real time, or obtain the string or expression from a third-party report about the attack.

Caution: Any new pattern that you add to a signature rule is in an AND relationship with the existing patterns. Do not add a new pattern to an existing signature rule if you do not want a potential attack to have to match all of the patterns in order to match the signature.

Each pattern can consist of a simple string, a PCRE-format regular expression, or the built-in SQL injection or cross-site scripting pattern. Before you attempt to add a pattern that is based on a regular expression, you should make sure that you understand PCRE-format regular expressions. PCRE expressions are complex and powerful; if you do not understand how they work, you can unintentionally create a pattern that matches something that you did not want (a *false positive*) or that fails to match something that you did want (a *false negative*).

If you are not already familiar with PCRE-format regular expressions, you can use the following resources to learn the basics, or for help with some specific issue:

- *"Mastering Regular Expressions"*, Third Edition. Copyright (c) 2006 by Jeffrey Friedl. O'Reilly Media, ISBN: 9780596528126
- *"Regular Expressions Cookbook"*. Copyright (c) 2009 by Jan Goyvaerts and Steven Levithan. O'Reilly Media, ISBN: 9780596520687
- **PCRE Man page/Specification** (text/official): "http://www.pcre.org/pcre.txt"
- **PCRE Man Page/Specification** (html/gammon.edu.au): "http://www.gammon.com.au/pcre/index.html"
- **Wikipedia PCRE entry**: "http://en.wikipedia.org/wiki/PCRE"
- **PCRE Mailing List** (run by exim.org): "http://lists.exim.org/mailman/listinfo/pcre-dev"

If you need to encode non-ASCII characters in a PCRE-format regular expression, the NetScaler platform supports encoding of hexadecimal UTF-8 codes. For more information, see "PCRE Character Encoding Format."

To configure a signature rule pattern

1. Navigate to Application Firewall > Signatures.
2. In the details pane, select that signatures object that you want to configure, and then click **Open**.
3. In the Modify Signatures Object dialog box, in the middle of the screen beneath the Filtered Results window, either click Add to create a signature rule, or select an existing signature rule and click Open.

   Note: You can modify only signature rules that you added. You cannot modify the default signature rules.

   Depending on your action, either the Add Local Signature Rule or the Modify Local Signature Rule dialog box appears. Both dialog boxes have the same contents.
4. Under the Patterns window in the dialog box that you opened, either click Add to add a new pattern, or select an existing pattern from the list beneath the Add button and click Open. Depending on your action, either the Create New Signature Rule Pattern or the Edit Signature Rule Pattern dialog box appears. Both dialog boxes have the same contents.
5. In the Pattern Type drop-down list, choose the type of connection that the pattern is intended to match.

   - If the pattern is intended to match request elements or features, such as injected SQL code, attacks on web forms, cross-site scripts, or inappropriate URLs, choose **Request**.
   - If the pattern is intended to match response elements or features, such as credit card numbers or safe objects, choose **Response**.
6. In the Location area, define the elements to examine with this pattern.

   The Location area describes what elements of the HTTP request or response to examine for this pattern. The choices that appear in the Location area depend upon the chosen pattern type. If you chose `Request` as the pattern type, items relevant to HTTP requests appear; if you chose `Response`, items relevant to HTTP responses appear.

   In addition, as you choose a value from the Area drop-down list, the remaining parts of the Location area change interactively. Following are all configuration items that might appear in this section.

   Area

   Drop-down list of elements that describe a particular portion of the HTTP connection. The choices are as follows:

   - **HTTP_ANY**. All parts of the HTTP connection.
   - **HTTP_COOKIE**. All cookies in the HTTP request headers after any cookie transformations are performed.

     Note: Does not search HTTP response "Set-Cookie:" headers.

- **HTTP_FORM_FIELD**. Form fields and their contents, after URL decoding, percent decoding, and removal of excess whitespace. You can use the `<Location>` tag to further restrict the list of form field names to be searched.
- **HTTP_HEADER**. The value portions of the HTTP header after any cross-site scripting or URL decoding transformations.
- **HTTP_METHOD**. The HTTP request method.
- **HTTP_ORIGIN_URL**. The origin URL of a web form.
- **HTTP_POST_BODY**. The HTTP post body and the web form data that it contains.
- **HTTP_RAW_COOKIE**. All HTTP request cookie, including the "Cookie:" name portion.

  Note: Does not search HTTP response "Set-Cookie:" headers.
- **HTTP_RAW_HEADER**. The entire HTTP header, with individual headers separated by linefeed characters (`\n`) or carriage return/line-feed strings (`\r\n`).
- **HTTP_RAW_RESP_HEADER**. The entire response header, including the name and value parts of the response header after URL transformation has been done, and the complete response status. As with HTTP_RAW_HEADER, individual headers are separated by linefeed characters (`\n`) or carriage return/line-feed strings (`\r\n`).
- **HTTP_RAW_SET_COOKIE**. The entire Set-Cookie header after any URL transformations have been performed.

  Note: URL transformation can change both the domain and path parts of the Set-Cookie header.
- **HTTP_RAW_URL**. The entire request URL before any URL transformations are performed, including any query or fragment parts.
- **HTTP_RESP_HEADER**. The value part of the complete response headers after any URL transformations have been performed.
- **HTTP_RESP_BODY**. The HTTP response body.
- **HTTP_SET_COOKIE**. All "Set-Cookie" headers in the HTTP response headers.
- **HTTP_STATUS_CODE**. The HTTP status code.
- **HTTP_STATUS_MESSAGE**. The HTTP status message.
- **HTTP_URL**. The value portion of the URL in the HTTP headers, excluding any query or fragment ports, after conversion to the UTF-* character set, URL decoding, stripping of whitespace, and conversion of relative URLs to absolute. Does not include HTML entity decoding.

URL

Examines any URLs found in the elements specified by the Area setting.

- To enable, select the Enabled check box.
- To search for a literal string in a URL, type the string in the text area.
- To search for a pattern defined by a regular expression, select the Is Regular Expression check box, and then type the regular expression in the text area. Use the **Regex Tokens** to insert common regular expression elements at the cursor, or the Regex Editor for more assistance in constructing the regular expression that you want.

Field Name

Examines any form field names found in the elements specified by the Area selection.

- To enable, select the Enabled check box.
- To search for a literal string in a form field, type the string in the text area.
- To search for a pattern defined by a regular expression, select the **Is Regular Expression** check box, and then type the regular expression in the text area. Use the **Regex Tokens** to insert common regular expression elements at the cursor, or the Regex Editor for more assistance in constructing the regular expression that you want.

7. In the Pattern area, define the pattern. A pattern is a literal string or PCRE-format regular expression that defines the pattern that you want to match. The Pattern area contains the following elements:

Match

A drop-down list of search methods that you can use for the signature. This list differs depending on whether the pattern type is Request or Response.

Request Match Types

- **Literal**. A literal string.
- **PCRE**. A PCRE-format regular expression.

  NOTE: When you choose PCRE, the regular expression tools beneath the Pattern window are enabled. These tools are not useful for most other types of patterns.
- **Injection**. Directs the application firewall to look for injected SQL in the specified location. The Pattern window disappears, because the application firewall already has the patterns for SQL injection.
- **CrossSiteScripting**. Directs the application firewall to look for cross-site scripts in the specified location. The Pattern window disappears, because the application firewall already has the patterns for cross-site scripts.
- **Expression**. An expression in the NetScaler default expressions language. This is the same expressions language that is used to create application firewall policies and other policies on the NetScaler appliance. Although the NetScaler expressions language was originally developed for policy rules, it is a highly flexible general purpose language that can also be used to define a signature pattern.

When you choose Expression, the NetScaler Expression Editor appears beneath Pattern window. For more information about the Expression Editor and instructions on how to use it, see "To add a firewall rule (expression) by using the Add Expression dialog box." For more information about NetScaler expressions, see "Policies and Expressions."

Response Match Types

- **Literal**. A literal string.
- **PCRE**. A PCRE-format regular expression.

  NOTE: When you choose PCRE, the regular expression tools beneath the Pattern window are enabled. These tools are not useful for most other types of patterns.
- **Credit Card**. A built-in pattern to match one of the six supported types of credit card number.

Note: The Expression match type is not available for Response-side signatures.

Pattern Window (unlabeled)

In this window, type the pattern that you want to match, and fill in any additional data.

- **Literal.** Type the string you want to search for in the text area.
- **PCRE.** Type the regular expression in the text area. Use the **Regex Editor** for more assistance in constructing the regular expression that you want, or the Regex Tokens to insert common regular expression elements at the cursor. To enable UTF-8 characters, click UTF-8.
- **Expression.** Type the NetScaler advanced expression in the text area. Use Prefix to choose the first term in your expression, or Operator to insert common operators at the cursor. Click **Add** to open the Add Expression dialog box for more assistance in constructing the regular expression that you want. Click Evaluate to open the Advanced Expression Evaluator to help determine what effect your expression has.
- **Offset.** The number of characters to skip over before starting to match on this pattern. You use this field to start examining a string at some point other than the first character.
- **Depth.** How many characters from the starting point to examine for matches. You use this field to limit searches of a large string to a specific number of characters.
- **Min-Length.** The string to be searched must be at least the specified number of bytes in length. Shorter strings are not matched.
- **Max-Length.** The string to be searched must be no longer than the specified number of bytes in length. Longer strings are not matched.
- **Search method.** A check box labeled fastmatch. You can enable fastmatch only for a literal pattern, to improve performance.

8. Click OK.

9. Repeat the previous four steps to add or modify additional patterns.

10. When finished adding or modifying patterns, click OK to save your changes and return to the Signatures pane.

Caution: Until you click **OK** in the **Add Local Signature Rule** or **Modify Local Signature Rule** dialog box, your changes are not saved. Do not close either of these dialog boxes without clicking **OK** unless you want to discard your changes.

Advanced Protections

The application firewall advanced protections (*security checks*) are a set of filters designed to catch complex or unknown attacks on your protected web sites and web services. The security checks use heuristics, positive security, and other techniques to detect attacks that may not be detected by signatures alone. You configure the security checks by creating and configuring an application firewall *profile*, which is a collection of user-defined settings that tell the application firewall which security checks to use and how to handle a request or response that fails a security check. A profile is associated with a *signatures object* and with a *policy* to create a security configuration.

The application firewall provides twenty security checks, which differ widely in the types of attacks that they target and how complex they are to configure. The security checks are organized into the following categories:

- **Common security checks.** Checks that apply to any aspect of web security that either does not involve content or is equally applicable to all types of content.
- **HTML security checks.** Checks that examine HTML requests and responses. These checks apply to HTML-based web sites and to the HTML portions of Web 2.0 sites, which contain mixed HTML and XML content.
- **XML security checks.** Checks that examine XML requests and responses. These checks apply to XML-based web services and to the XML portions of Web 2.0 sites.

The security checks protect against a wide range of types of attack, including attacks on operation system and web server software vulnerabilities, SQL database vulnerabilities, errors in the design and coding of web sites and web services, and failures to secure sites that host or can access sensitive information.

All security checks have a set of configuration options, the check actions, which control how the application firewall handles a connection that matches a check. Three check actions are available for all security checks. They are:

- **Block.** Block connections that match the signature. Disabled by default.
- **Log.** Log connections that match the signature, for later analysis. Enabled by default.
- **Stats.** Maintain statistics, for each signature, that show how many connections it matched and provide certain other information about the types of connections that were blocked. Disabled by default.

A fourth check action, **Learn**, is available for more than half of the check actions. It observes traffic to a protected Web site or web service and uses connections that repeatedly violate the security check to generate recommended exceptions (*relaxations*) to the check, or new rules for the check. In addition to the check actions, certain security checks have parameters that control the rules that the check uses to determine which connections violate that check, or that configure the application firewall's response to connections that violate the check. These parameters are different for each check, and they are described in the documentation for each check.

To configure security checks, you can use the application firewall wizard, as described in "The Application Firewall Wizard," or you can configure the security checks manually, as described in "Manual Configuration By Using the Configuration Utility." Some tasks, such as manually entering relaxations or rules or reviewing learned data, can be done only by using the configuration utility, not the command line. Using the wizard is usually best configuration method, but in some cases manual configuration might be easier if you are thoroughly familiar with it and simply want to adjust the configuration for a single security check.

Regardless of which method you use to configure the security checks, each security check requires that certain tasks be performed. Many checks require that you specify exceptions (*relaxations*) to prevent blocking of legitimate traffic before you enable blocking for that security check. You can do this manually, by observing the log entries after a certain amount of traffic has been filtered and then creating the necessary exceptions. However, it is usually much easier to enable the learning feature and let it observe the traffic and recommend the necessary exceptions.

Top-Level Advanced Protections

Four of the advanced protections are especially effective against common types of Web attacks, and are therefore more commonly used than any of the others. They are:

- **HTML Cross-Site Scripting.** Examines requests and responses for scripts that attempt to access or modify content on a different Web site than the one on which the script is located. When this check finds such a script, it either renders the script harmless before forwarding the request or response to its destination, or it blocks the connection.

- **HTML SQL Injection.** Examines requests that contain form field data for attempts to inject SQL commands into an SQL database. When this check detects injected SQL code, it either blocks the request or renders the injected SQL code harmless before forwarding the request to the Web server.

  Note: If both of the following conditions apply to your configuration, you should make certain that your Application Firewall is correctly configured:

  - If you enable the HTML Cross-Site Scripting check or the HTML SQL Injection check (or both), and

  - Your protected Web sites accept file uploads or contain Web forms that can contain large POST body data.

  For more information about configuring the Application Firewall to handle this case, see "Configuring the Application Firewall."

- **Buffer Overflow.** Examines requests to detect attempts to cause a buffer overflow on the Web server.

- **Cookie Consistency.** Examines cookies returned with user requests to verify that they match the cookies your Web server set for that user. If a modified cookie is found, it is stripped from the request before the request is forwarded to the Web server.

The Buffer Overflow check is simple; you can usually enable blocking for it immediately. The other three top-level checks are considerably more complex and require configuration before you can safely use them to block traffic. Citrix strongly recommends that, rather than attempting to configure these checks manually, you enable the learning feature and allow it to generate the necessary exceptions.

HTML Cross-Site Scripting Check

HTML Cross-Site Scripting Check

The HTML Cross-Site Scripting check examines both the headers and the POST bodies of user requests for possible cross-site scripting attacks. If it finds a cross-site script, it either modifies (*transforms*) the request to render the attack harmless, or blocks the request.

To prevent misuse of the scripts on your protected web sites to breach security on your web sites, the HTML Cross-Site Scripting check blocks scripts that violate the *same origin rule*, which states that scripts should not access or modify content on any server but the server on which they are located. Any script that violates the same origin rule is called a cross-site script, and the practice of using scripts to access or modify content on another server is called cross-site scripting. The reason cross-site scripting is a security issue is that a web server that allows cross-site scripting can be attacked with a script that is not on that web server, but on a different web server, such as one owned and controlled by the attacker.

Unfortunately, many companies have a large installed base of JavaScript-enhanced web content that violates the same origin rule. If you enable the HTML Cross-Site Scripting check on such a site, you have to generate the appropriate exceptions so that the check does not block legitimate activity.

If you use the wizard or the configuration utility, in the Modify HTML Cross-Site Scripting Check dialog box, on the General tab you can enable or disable the Block, Log, Learn, and Statistics actions, and in addition the following parameters:

- **Transform.** If enabled, the application firewall makes the following changes to requests that match the HTML Cross-Site Scripting check:
  - Left angle bracket (<) to HTML character entity equivalent (<)
  - Right angle bracket (>) to HTML character entity equivalent (>)

  This ensures that browsers do not interpret unsafe html tags, such as `<script>`, and thereby execute malicious code. If you enable both request-header checking and transformation, any special characters found in request headers are also modified as described above. If scripts on your protected web site contain cross-site scripting features, but your web site does not rely upon those scripts to operate correctly, you can safely disable blocking and enable transformation. This configuration ensures that no legitimate web traffic is blocked, while stopping any potential cross-site scripting attacks.

- **Check complete URLs.** If checking of complete URLs is enabled, the application firewall examines entire URLs for HTML cross-site scripting attacks instead of checking just the query portions of URLs.

- **Check Request headers.** If Request header checking is enabled, the application firewall examines the headers of requests for HTML cross-site scripting attacks, instead of just URLs.

If you use the command-line interface, you can enter the following commands to configure the HTML Cross-Site Scripting Check:

- set appfw profile <name> -crossSiteScriptingAction [**block**] [**learn**] [**log**] [**stats**] [**none**]
- set appfw profile <name> -crossSiteScriptingTransformUnsafeHTML ([**ON**] | [**OFF**])
- set appfw profile <name> -crossSiteScriptingCheckCompleteURLs ([**ON**] | [**OFF**])

To specify relaxations for the HTML Cross-Site Scripting check, you must use the configuration utility. On the Checks tab of the Modify HTML Cross-Site Scripting Check dialog box, click Add to open the Add HTML Cross-Site Scripting Check Relaxation dialog box, or select an existing relaxation and click Open to open the Modify HTML Cross-Site Scripting Check Relaxation dialog box. Either dialog box provides the same options for configuring a relaxation, as described in "Manual Configuration By Using the Configuration Utility."

Following are examples of HTML Cross-Site Scripting check relaxations:

Web Form Field Expressions

- **Logon Fields.** The following expression exempts all fields beginning with the string `logon_` followed by a string of upper- and lower-case letters or numbers that is at least two characters long and no more than fifteen characters long:

  ^logon_[0-9A-Za-z]{2,15}$

- **Name Fields.** The following expression exempts form fields with names beginning with `Name_` followed by a string beginning with a letter or number and consisting of from one to twenty letters, numbers, or the apostrophe or hyphen symbol:

  ^Name_[0-9A-Za-z][0-9A-Za-z'-]{0,20}$

- **Name Fields (Special Characters).** If your web site has Turkish-speaking customers whose first names may contain special characters, you might have a form field that begins with the string Turkish-Name_ on their logon page. In addition, the customers may use the same special characters in their names. The special characters in both of these strings must be represented as encoded UTF-8 strings. The following expression exempts form fields beginning with Turkish-Name_ and containing Turkish special characters:

  ^T\xC3\xBCrk\xC3\xA7e-Name_([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])+$

  Note: See "PCRE Character Encoding Format" for a complete description of supported special characters and how to encode them properly.

- **Session-ID Fields.** The following expression exempts all fields beginning with the string `sessionid-` followed by a ten-digit number:

  ^sessionid-[0-9]{10,10}$

URL Expressions

- **URLs using JavaScript.** You can use a single expression to exempt all URLs that end with a filename that follows a specified pattern. The following expression exempts all URLs that end with the string `query_` followed by a string of upper- and lower-case letters or numbers that is at least two characters long and no more than forty characters long, and ending with the string `.js`:

query_[0-9A-Za-z]{2,40}[.]js$

- **URLs containing a Specified String.** You can use an expression to exempt all URLs that contain a specific string. The following expression exempts all URLs that contain the string `prodinfo`:

  ^https?://(([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|\\x[0-9A-Fa-f][0-9A-Fa-f]+[.])+[a-z]{2,6}/[^<>?]*\?prodinfo[^<>?]*$

  In the above expression , each character class has been grouped with the string `\\x[0-9A-Fa-f][0-9A-Fa-f]`, which matches all properly constructed character encoding strings but does not allow stray backslash characters that are not associated with a UTF-8 character encoding string. The double backslash (\\) is an escaped backslash, which tells the application firewall to interpret it as a literal backslash. If you included only one backslash, the application firewall would interpret the following left square bracket ([) as a literal character instead of as the opening of a character class, which would break the expression.

Caution: Regular expressions are powerful. Especially if you are not thoroughly familiar with PCRE-format regular expressions, double-check any regular expressions you write. Make sure that they define exactly the URL you want to add as an exception, and nothing else. Careless use of wildcards, and especially of the dot-asterisk (`.*`) metacharacter/wildcard combination, can have results you do not want or expect, such as blocking access to web content that you did not intend to block or allowing an attack that the HTML Cross-Site Scripting check would otherwise have blocked.

HTML SQL Injection Check

The HTML SQL Injection check provides special defenses against injection of unauthorized SQL code that might break security. It examines both the headers and the POST bodies of requests for injected SQL code. If the application firewall detects unauthorized SQL code in a user request, it either transforms the request, to render the SQL code inactive, or blocks the request.

Many web applications have web forms that use SQL to communicate with relational database servers. Often, the scripts that pass web form information to the database do not validate the information provided by the user before sending it to the database. Malicious code or a hacker can use the insecure web form to send SQL commands to the web server.

Note: To prevent blocking of legitimate requests, this check ignores cookies that were set by the server, even if they contain elements that the Cookie Consistency Check would otherwise block.

If you use the wizard or the configuration utility, in the Modify Cookie Consistency Check dialog box, on the General tab you can enable or disable the Block, Log, Statistics, and Learn actions, and the following actions:

- **Transform.** Make the following changes to requests that match the HTML SQL Injection check:
  - Single straight quote (') to double straight quote (")
  - Backslash (\) to double backslash (\\).
  - Semicolon (;) is dropped completely.

  These three characters (*special strings*) are necessary to issue commands to an SQL server. Unless an SQL command is prefaced with a special string, most SQL servers ignore that command. For this reason, the changes that the application firewall performs when transformation is enabled prevent an attacker from injecting active SQL. After these changes are made, it is safe to forward the request to your protected web site. When web forms on your protected web site may legitimately contain SQL special strings, but the web form does not rely upon the special strings to operate correctly, you can disable blocking and enable transformation to prevent blocking of legitimate web form data without reducing the protection that the application firewall provides to your protected web sites.

  Note: You normally enable either transformation or blocking, but not both. If you have blocking enabled, enabling transformation is redundant because the application firewall already blocks access to requests that contain injected SQL.

- **Restrict checks to fields containing SQL special characters.** If you configure the application firewall to check only fields that contain SQL special strings, the application firewall skips web form fields that do not contain special characters. Since most SQL servers do not process SQL commands that are not preceded by a special character, enabling this parameter can significantly reduce the load on the application firewall and speed up processing without placing your protected web sites at risk.

- **SQL comments handling.** By default, the application firewall checks all SQL comments for injected SQL commands. Many SQL servers ignore anything in a comment, however, even if it is preceded by an SQL special character. For faster processing, if your SQL server ignores comments, you can configure the application firewall to skip comments when examining requests for injected SQL. The SQL comments handling options are:
  - **ANSI.** Skip ANSI-format SQL comments, which are normally used by UNIX-based SQL databases.
  - **Nested.** Skip nested SQL comments, which are normally used by Microsoft SQL Server.
  - **ANSI/Nested.** Skip comments that adhere to both the ANSI and nested SQL comment standards. Comments that match only the ANSI standard, or only the nested standard, are still checked for injected SQL.

    Caution: In most cases, you should not choose the Nested or the ANSI/Nested option unless your back-end database runs on Microsoft SQL Server. Most other types of SQL server software do not recognize nested comments. If nested comments appear in a request directed to another type of SQL server, they may indicate an attempt to breach security on that server.
  - **Check all Comments.** Check the entire request for injected SQL, without skipping anything. The default setting.
- **Check Request headers.** Examine the headers of requests for HTML SQL Injection attacks, instead of just URLs.

  Caution: If you enable both request header checking and transformation, any SQL special characters found in headers are also transformed. The Accept, Accept-Charset, Accept-Encoding, Accept-Language, Expect, and User-Agent headers normally contain semicolons (;), so enabling both Request header checking and transformation simultaneously may cause errors.

If you use the command-line interface, you can enter the following commands to configure the HTML SQL Injection Check:

- set appfw profile <name> -SQLInjectionAction [**block**] [**learn**] [**log**] [**stats**] [**none**]
- set appfw profile <name> -SQLInjectionTransformSpecialChars ([**ON**] | [**OFF**])
- set appfw profile <name> -SQLInjectionOnlyCheckFieldsWithSQLChars ([**ON**]|[**OFF**])
- set appfw profile <name> -SQLInjectionParseComments ([**checkall**] | [**ansi**|**nested**] | [**ansinested**])

To specify relaxations for the HTML SQL Injection check, you must use the configuration utility. On the Checks tab of the Modify HTML SQL Injection Check dialog box, click Add to open the Add HTML SQL Injection Check Relaxation dialog box, or select an existing relaxation and click Open to open the Modify HTML SQL Injection Check Relaxation dialog box. Either dialog box provides the same options for configuring a relaxation, as described in "Manual Configuration By Using the Configuration Utility."

Following are examples of HTML SQL Injection check relaxations:

Web Form Field Name Expressions

- **Logon Fields.** The following expression exempts all fields beginning with the string `logon_` followed by a string of letters or numbers that is at least two characters long and no more than fifteen characters long:

  ^logon_[0-9A-Za-z]{2,15}$

- **Name Fields.** The following expression exempts form fields with names beginning with `Name_` followed by a string beginning with a letter or number and consisting of from one to twenty letters, numbers, or the apostrophe or hyphen symbol:

  ^Name_[0-9A-Za-z][0-9A-Za-z'-]{0,20}$

- **Name Fields (Special Characters).** If your web site has Turkish-speaking customers whose first names may contain special characters, you might have a form field that begins with the string Turkish-Name_ on their logon page. In addition, the customers may use the same special characters in their names. The special characters in both of these strings must be represented as encoded UTF-8 strings. The following expression exempts form fields beginning with Turkish-Name_ and containing Turkish special characters:

  ^T\xC3\xBCrk\xC3\xA7e-Name_([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])+$

  Note: See "PCRE Character Encoding Format" for a complete description of supported special characters and how to encode them properly.

- **Session-ID Fields.** The following expression exempts all fields beginning with the string `sessionid-` followed by a ten-digit number:

  ^sessionid-[0-9]{10,10}$

Action URL Expressions

- **URLs using JavaScript.** You can use a single expression to exempt all URLs that end with a filename that follows a specified pattern. The following expression exempts all URLs that end with the string `query_` followed by a string of upper- and lower-case letters or numbers that is at least two characters long and no more than forty characters long, and that end with the string `.js`:

  query_[0-9A-Za-z]{2,40}[.]js$

- **URLs containing a Specified String.** You can use an expression to exempt all URLs that contain a specific string. The following expression exempts all URLs that contain the string `prodinfo`:

  ^https?://(([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|\\x[0-9A-Fa-f][0-9A-Fa-f]+[.])+[a-z]{2,6}/[^<>?]*\?prodinfo[^<>?]*$

  In the expression above, each character class has been grouped with the string `\\x[0-9A-Fa-f][0-9A-Fa-f]`, which matches all properly constructed character

encoding strings but does not allow stray backslash characters that are not associated with a UTF-8 character encoding string. The double backslash (\\) is an escaped backslash, which tells the application firewall to interpret it as a literal backslash. If you included only one backslash, the application firewall would interpret the following left square bracket ([) as a literal character instead of as the opening of a character class, which would break the expression.

Caution: Regular expressions are powerful. Especially if you are not thoroughly familiar with PCRE-format regular expressions, double-check any regular expressions you write. Make sure that they define exactly the URL that you want to add as an exception, and nothing else. Careless use of wildcards, and especially of the dot-asterisk (`.*`) metacharacter/wildcard combination, can have results that you do not want, such as blocking access to web content that you did not intend to block or allowing an attack that the HTML SQL Injection check would otherwise have blocked.

Buffer Overflow Check

The Buffer Overflow check detects attempts to cause a buffer overflow on the web server. If the application firewall detects a URL, cookie or header longer than the specified maximum length in a request, it blocks that request because it might be an attempt to cause a buffer overflow.

The Buffer Overflow check prevents attacks against insecure operating-system or web-server software that can crash or behave unpredictably when it receives a data string that is larger than it can handle. Proper programming techniques prevent buffer overflows by checking incoming data and either rejecting or truncating overlong strings. Many programs, however, do not check all incoming data and are therefore vulnerable to buffer overflows. This issue especially affects older versions of web-server software and operating systems, many of which are still in use.

If you use the wizard or the configuration utility, in the Modify Buffer Overflow Check dialog box, on the General tab you can enable or disable the Block, Log, and Statistics actions. On the Checks tab, you can set the following parameters:

- **Maximum URL Length.** The maximum length the application firewall allows in a requested URL. Requests with longer URLs are blocked. Possible Values: 0-65536. Default: 1024
- **Maximum Cookie Length.** The maximum length the application firewall allows for an individual cookie in a request. Longer cookies are stripped from requests before those requests are forwarded to your protected web server. Possible Values: 0-65536. Default: 4096
- **Maximum Header Length.** The maximum length the application firewall allows for HTTP headers. Requests with longer headers are blocked. Possible Values: 0-65536. Default: 4096

If you use the command-line interface, you can add the following Buffer Overflow Check arguments to the set appfwl profile <profileName> command:

- -bufferOverflowAction [**block**] [**log**| [**stats**]
- -bufferOverflowMaxURLLength <positiveInteger>
- -bufferOverflowMaxCookieLength <positiveInteger>
- -bufferOverflowMaxHeaderLength <positiveInteger>

Cookie Consistency Check

The Cookie Consistency check examines cookies returned by users, to verify that they match the cookies that your web site set for that user. If a modified cookie is found, it is stripped from the request before the request is forwarded to the web server. You can also configure the Cookie Consistency check to transform all of the server cookies that it processes, by encrypting the cookies, proxying the cookies, or adding flags to the cookies. This check applies to requests and responses.

An attacker would normally modify a cookie to gain access to sensitive private information by posing as a previously authenticated user, or to cause a buffer overflow. The Buffer Overflow check protects against attempts to cause a buffer overflow by using a very long cookie. The Cookie Consistency check focuses on the first scenario.

If you use the wizard or the configuration utility, in the Modify Cookie Consistency Check dialog box, on the General tab you can enable or disable the following actions:

- Block
- Log
- Learn
- Statistics
- Transform. If enabled, the Transform action modifies all cookies as specified in the following settings:
    - **Encrypt Server Cookies.** Encrypt cookies set by your web server, except for any listed in the Cookie Consistency check relaxation list, before forwarding the response to the client. Encrypted cookies are decrypted when the client sends a subsequent request, and the decrypted cookies are reinserted into the request before it is forwarded to the protected web server. Specify one of the following types of encryption:
        - **None.** Do not encrypt or decrypt cookies. The default.
        - **Decrypt only.** Decrypt encrypted cookies only. Do not encrypt cookies.
        - **Encrypt session only.** Encrypt session cookies only. Do not encrypt persistent cookies. Decrypt any encrypted cookies.
        - **Encrypt all.** Encrypt both session and persistent cookies. Decrypt any encrypted cookies.

          Note: When encrypting cookies, the application firewall adds the **HttpOnly** flag to the cookie. This flag prevents scripts from accessing and parsing the cookie. The flag therefore prevents a script-based virus or trojan from accessing a decrypted cookie and using that information to breach security. This is done regardless of the Flags to Add in Cookies parameter settings, which are handled independently of the Encrypt Server Cookies parameter

settings.

- **Proxy Server Cookies.** Proxy all non-persistent (*session*) cookies set by your web server, except for any listed in the Cookie Consistency check relaxation list. Cookies are proxied by using the existing application firewall session cookie. The application firewall strips session cookies set by the protected web server and saves them locally before forwarding the response to the client. When the client sends a subsequent request, the application firewall reinserts the session cookies into the request before forwarding it to the protected web server. Specify one of the following settings:
  - **None.** Do not proxy cookies. The default.
  - **Session only.** Proxy session cookies only. Do not proxy persistent cookies.

    Note: If you disable cookie proxying after having enabled it (set this value to None after it was set to Session only), cookie proxying is maintained for sessions that were established before you disabled it. You can therefore safely disable this feature while the application firewall is processing user sessions.
- **Flags to Add in Cookies**. Add flags to cookies during transformation. Specify one of the following settings:
  - **None.** Do not add flags to cookies. The default.
  - **HTTP only.** Add the HttpOnly flag to all cookies. Browsers that support the HttpOnly flag do not allow scripts to access cookies that have this flag set.
  - **Secure**. Add the Secure flag to cookies that are to be sent only over an SSL connection. Browsers that support the Secure flag do not send the flagged cookies over an insecure connection.
  - **All.** Add the HttpOnly flag to all cookies, and the Secure flag to cookies that are to be sent only over an SSL connection.

If you use the command-line interface, you can enter the following commands to configure the Cookie Consistency Check:

- set appfw profile <name> -cookieConsistencyAction [**block**] [**learn**] [**log**] [**stats**] [**none**]
- set appfw profile <name> -cookieTransforms ([**ON**] | [**OFF**])
- set appfw profile <name> -cookieEncryption ([**none**] | [**decryptOnly**] | [**encryptSession**] | [**encryptAll**])
- set appfw profile <name> -cookieProxying ([**none**] | [**sessionOnly**])
- set appfw profile <name> -addCookieFlags ([**none**] | [**httpOnly**] | [**secure**] | [**all**])

To specify relaxations for the Cookie Consistency check, you must use the configuration utility. On the Checks tab of the Modify Cookie Consistency Check dialog box, click Add to open the Add Cookie Consistency Check Relaxation dialog box, or select an existing relaxation and click Open to open the Modify Cookie Consistency Check Relaxation dialog box. Either dialog box provides the same options for configuring a relaxation, as described in "Manual Configuration By Using the Configuration Utility."

Following are examples of Cookie Consistency check relaxations:

- **Logon Fields.** The following expression exempts all form fields beginning with the string `logon_` followed by a string of letters or numbers that is at least two characters long and no more than fifteen characters long:

  ```
  ^logon_[0-9A-Za-z]{2,15}$
  ```

- **Logon Fields (special characters).** The following expression exempts all form fields beginning with the string `türkçe-logon_` followed by a string of letters or numbers that is at least two characters long and no more than fifteen characters long:

  ```
  ^t\xC3\xBCrk\xC3\xA7e-logon_[0-9A-Za-z]{2,15}$
  ```

  Note: The special characters in that string must be represented as encoded UTF-8 strings. See "PCRE Character Encoding Format" for a complete description of supported special characters and how to encode them properly.

- **Arbitrary strings.** Allow cookies that contain the string `sc-item_`, followed by the ID of an item that the user has added to his shopping cart ([0-9A-Za-z]+), a second underscore (_), and finally the number of these items he wants ([1-9][0-9]?), to be user-modifiable:

  ```
  ^sc-item_[0-9A-Za-z]+_[1-9][0-9]?$
  ```

Caution: Regular expressions are powerful. Especially if you are not thoroughly familiar with PCRE-format regular expressions, double-check any regular expressions you write. Make sure that they define exactly the URL you want to add as an exception, and nothing else. Careless use of wildcards, and especially of the dot-asterisk (`.*`) metacharacter/wildcard combination, can have results you do not want or expect, such as blocking access to web content that you did not intend to block or allowing an attack that the Cookie Consistency check would otherwise have blocked.

Data Leak Prevention Checks

The data-leak-prevention checks filter responses to prevent leaks of sensitive information, such as credit card numbers and social security numbers, to unauthorized recipients.

Credit Card Check

The Credit Card check provides special handling for credit card numbers. A web application does not usually send a credit card number in a response to a user request, even when the user supplies a credit card number in the request. The application firewall examines web server responses, including headers, for credit card numbers. If it finds a credit card number in the response, and the administrator has not configured it to allow credit card numbers to be sent, it responds in one of two ways:

- It blocks the response.
- It replaces all but the final group of digits in the credit card with x's. For example, a credit card number of 9876-5432-1234-5678 would be rendered xxxx-xxxx-xxxx-5678.

The Credit Card check prevents attackers from exploiting a security flaw in your web server software or on your web site to obtain credit card numbers of your customers. If your web sites do not have access to credit card information, you do not need to configure this check. If you have a shopping cart or other application that can access credit card numbers, or your web sites have access to database servers that contain credit card numbers, you should configure protection for each type of credit card that you accept.

Note: A web site that does not access an SQL database usually does not have access to sensitive private information such as credit card numbers.

If you use the wizard or the configuration utility, in the Credit Card Check dialog box, on the General tab you can enable or disable the Block, Log, and Statistics actions, and the following actions:

- **X-Out.** Mask any credit card number detected in a response by replacing each digit, except the digits in the final group, with the letter "X."
- **Maximum credit cards allowed per page.** Allow up to the specified number of credit card numbers per page in responses without masking the credit card numbers or blocking the response. The Maximum is set to zero (0) by default. Web pages do not usually contain unmasked credit card numbers, but occasionally a web page might legitimately contain a credit card number or even a list of credit card numbers. To allow one or more credit card numbers to appear in a web page before masking the numbers or blocking the response, change the value in the "Maximum credit cards allowed per page" text box to the number of credit cards that you want to allow.

To configure the types of credit cards to be protected, in the Modify Credit Card Check dialog box, select each credit card type that you want to protect, and then click Protect. If you want to cancel protection for a credit card type, select that credit card type and then click Unprotect. You can hold down your Shift or Ctrl key while choosing credit card types, and then enable or disable several credit card types at once by clicking the Protect or Unprotect button while multiple credit card types are selected.

If you use the command-line interface, you can enter the following commands to configure the Credit Card Check:

- set appfw profile <name> -creditCardAction [**block**] [**log**] [**stats**] [**none**]

- set appfw profile <name> -creditCard (**VISA** | **MASTERCARD** | **DISCOVER** | **AMEX** | **JCB** | **DINERSCLUB**)
- set appfw profile <name> -creditCardMaxAllowed <integer>
- set appfw profile <name> -creditCardXOut ([**ON**] | [**OFF**])

Safe Object Check

The Safe Object check provides user-configurable protection for sensitive business information, such as customer numbers, order numbers, and country-specific or region-specific telephone numbers or postal codes. A user-defined regular expression or custom plug-in tells the application firewall the format of this information and defines the rules to be used to protect it. If a string in a user request matches a safe object definition, the application firewall either blocks the response, masks the protected information, or removes the protected information from the response before sending it to the user, depending on how you configured that particular safe object rule.

The Safe Object check prevents attackers from exploiting a security flaw in your web server software or on your web site to obtain sensitive private information, such as company credit card numbers or social security numbers. If your web sites do not have access to these types of information, you do not need to configure this check. If you have a shopping cart or other application that can access such information, or your web sites have access to database servers that contain such information, you should configure protection for each type of sensitive private information that you handle and store.

Note: A web site that does not access an SQL database usually does not have access to sensitive private information.

The Safe Object Check dialog box is unlike that for any other check. Each safe object expression that you create is the equivalent of a separate security check, similar to the Credit Card check, for that type of information. If you use the wizard or the configuration utility, you add a new expression by clicking Add and configuring the expression in the Add Safe Object dialog box. You modify an existing expression by selecting it, then clicking Open, and then configuring the expression in the Modify Safe Object dialog box.

In the Safe Object dialog box for each safe object expression, you can configure the following:

- **Safe Object Name.** A name for your new safe object. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 255 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols.

- **Actions.** Enable or disable the Block, Log, and Statistics actions, and the following actions:

    - **X-Out.** Mask any information that matches the safe object expression with the letter “X”.

    - **Remove.** Remove any information that matches the safe object expression.
- **Regular Expression.** Enter a PCRE-compatible regular expression that defines the safe object. You can create the regular expression in one of three ways: by typing the regular expression directly into the text box, by using the **Regex Tokens** menu to enter regular expression elements and symbols directly into the text box, or by opening the Regular Expressions Editor and using it to construct the expression. The regular expression must consist of ASCII characters only. Do not cut and paste characters that are not part of the basic 128-character ASCII set. If you want to include non-ASCII characters, you must manually type those characters in PCRE hexadecimal character

encoding format.

Note: Do not use start anchors (^) at the beginning of Safe Object expressions, or end anchors ($) at the end of Safe Object expressions. These PCRE entities are not supported in Safe Object expressions, and if used, will cause your expression not to match what it was intended to match.

- **Maximum Match Length.** Enter a positive integer that represents the maximum length of the string that you want to match. For example, if you want to match U.S. social security numbers, enter the number eleven (11) in this field. That allows your regular expression to match a string with nine numerals and two hyphens. If you want to match California driver's license numbers, enter the number eight (8).

Caution: If you do not enter a maximum match length in this field, the application firewall uses a default value of one (1) when filtering for strings that match your safe object expressions. As a result, most safe object expressions fail to match their target strings.

You cannot use the command-line interface to configure the Safe Object check. You must configure it by using either the application firewall wizard or the configuration utility.

Following are examples of Safe Object check regular expressions:

- Look for strings that appear to be U.S. social security numbers, which consist of three numerals (the first of which must not be zero), followed by a hyphen, followed by two more numerals, followed by a second hyphen, and ending with a string of four more numerals:

  [1-9][0-9]{2,2}-[0-9]{2,2}-[0-9]{4,4}

- Look for strings that appear to be California driver's license IDs, which start with a letter and are followed by a string of exactly seven numerals:

  [A-Za-z][0-9]{7,7}

- Look for strings that appear to be Example Manufacturing customer IDs which, consist of a string of five hexadecimal characters (all the numerals and the letters A through F), followed by a hyphen, followed by a three-letter code, followed by a second hyphen, and ending with a string of ten numerals:

  [0-9A-Fa-f]{5,5}-[A-Za-z]{3,3}-[0-9]{10,10}

Caution: Regular expressions are powerful. Especially if you are not thoroughly familiar with PCRE-format regular expressions, double-check any regular expressions you write to ensure that they define exactly the type of string you want to add as a safe object definition, and nothing else. Careless use of wildcards, and especially of the dot-asterisk (.*) metacharacter/wildcard combination, can have results you did not want or expect, such as blocking access to web content that you did not intend to block.

Advanced Form Protection Checks

The advanced Form Protection checks examine web form data to prevent attackers from compromising your system by modifying the web forms on your web sites or sending unexpected types and quantities of data to your web site in a form.

Field Formats Check

The Field Formats check verifies the data that users send to your web sites in a web form. It examines both the length and type of data to ensure that it is appropriate for the form field in which it appears. If the application firewall detects inappropriate web form data in a user request, it blocks the request. This check applies to HTML requests only. It does not apply to XML requests.

By preventing an attacker from sending inappropriate web form data to your web site, the Field Formats check prevents certain types of attacks on your web site and database servers. For example, if a particular field expects the user to enter a phone number, the Field Formats check examines the user's response to ensure that the data matches the format for a phone number. If a particular field expects a first name, the Field Formats check ensures that the data in that field is of a type and length appropriate for a first name. It does the same thing for each form field that you configure it to protect.

The Field Formats check provides a different type of protection than does the Form Field Consistency check. The Form Field Consistency check verifies that the structure of the web forms returned by users is intact, that data format restrictions configured in the HTML are respected, and that data in hidden fields has not been modified. It can do this without any specific knowledge about your web forms other than what it derives from the web form itself. The Field Formats check verifies that the data in each form field matches the specific formatting restrictions that you configured manually, or that the learning feature generated and you approved. In other words, the Form Field Consistency check enforces general web form security, while the Field Formats check enforces the specific rules that you set for your web forms.

Before it can protect your web forms, the Field Formats check requires that you configure the application firewall to recognize the type and length of data expected in each form field on each web form that you want to protect.

If you use the wizard or the configuration utility, in the Modify Field Formats Check dialog box, on the General tab you can enable or disable the Block, Log, Learn, and Statistics actions and the following parameters:

- **Field Type.** Assign a default field type to form fields in web forms that do not have a field type. This parameter is not set by default. You can assign any field type that is defined on your application firewall as the default field type.

  Caution: If you set a restrictive default field type and do not disable blocking until you are certain that the field types assigned to your form fields are correct, users may be unable to use your web forms.

- **Minimum Length.** The default minimum data length assigned to form fields in web forms that do not have an explicit setting. This parameter is set to 0 by default, which allows the user to leave the field blank. Any higher setting forces users to fill in the field.

- **Maximum Length.** The default maximum data length assigned to form fields in web forms that do not have an explicit setting. This parameter is set to 65535 by default.

If you use the command-line interface, you can enter the following commands to configure the Field Formats Check:

- set appfw profile <name> -fieldFormatAction [**block**] [**learn**] [**log**] [**stats**] [**none**]
- set appfw profile <name> -defaultFieldFormatType <string>
- set appfw profile <name> -defaultFieldFormatMinLength <integer>
- set appfw profile <name> -defaultFieldFormatMaxLength <integer>

To specify relaxations for the Field Formats check, you must use the configuration utility. On the Checks tab of the Modify Field Formats Check dialog box, click Add to open the Add Field Formats Check Relaxation dialog box, or select an existing relaxation and click Open to open the Modify Field Formats Check Relaxation dialog box. Either dialog box provides the same options for configuring a relaxation, as described in "Manual Configuration By Using the Configuration Utility."

Following are examples of Field Formats check relaxations:

- Choose form fields with the name FirstName:

  ^FirstName$

- Choose form fields with names that begin with Name_ and are followed by a string beginning with a letter or number and consisting of from one to twenty letters, numbers, or the apostrophe or hyphen symbol:

  ^Name_[0-9A-Za-z][0-9A-Za-z'-]{0,20}$

- Choose form fields with names that begin with Turkish-FirstName_ and are otherwise the same as the previous expression, except that they can contain Turkish special characters throughout:

  ^T\xC3\xBCrk\xC3\xA7e-FirstName_([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])+$

  Note: See "PCRE Character Encoding Format" for a complete description of supported special characters and how to encode them properly.

- Choose form field names that begin with a letter or number, consist of a combination of letters and/or numbers only, and that contain the string Num anywhere in the string:

  ^[0-9A-Za-z]*Num[0-9A-Za-z]*$

Form Field Consistency Check

The Form Field Consistency check examines the web forms returned by users of your web site, and verifies that web forms were not modified inappropriately by the client. This check applies only to HTML requests that contain a web form, with or without data. It does not apply to XML requests.

The Form Field Consistency check prevents clients from making unauthorized changes to the structure of the web forms on your web site when they are filling out a web form and submitting data by using that form. It also ensures that the data a user submits meets the HTML restrictions for length and type, and that data in hidden fields is not modified. This prevents an attacker from tampering with a web form and using the modified form to gain unauthorized access to web site, redirect the output of a contact form that uses an insecure script and thereby send unsolicited bulk email, or exploit a vulnerability in your web server software to gain control of the web server or the underlying operating system. Web forms are a weak link on many web sites and attract a wide range of attacks.

The Form Field Consistency check verifies all of the following:

- If a field is sent to the user, the check ensures that it is returned by the user.
- The check enforces HTML field lengths and types.

  Note: The Form Field Consistency check enforces HTML restrictions on data type and length but does not otherwise validate the data in web forms. You can use the Field Formats check to set up rules that validate data returned in specific form fields on your web forms.
- If your web server does not send a field to the user, the check does not allow the user to add that field and return data in it.
- If a field is a read-only or hidden field, the check verifies that the data has not changed.
- If a field is a list box or radio button field, the check verifies that the data in the response corresponds to one of the values in that field.

If a web form returned by a user violates one or more of the Form Field consistency checks, and you have not configured the application firewall to allow that web form to violate the Form Field Consistency checks, the request is blocked.

If you use the wizard or the configuration utility, in the Modify Form Field Consistency Check dialog box, on the General tab you can enable or disable the Block, Log, Learn, and Statistics actions.

You also configure Sessionless Field Consistency in the General tab. If Sessionless Field Consistency is enabled, the application firewall checks only the web form structure, dispensing with those parts of the Form Field Consistency check that depend upon maintaining session information. This can speed the Form Field Consistency check with little security penalty for web sites that use many forms. To use Sessionless Field Consistency on all web forms, select On. To use it only for forms submitted with the HTTP POST method, select postOnly

If you use the command-line interface, you can enter the following command to configure the Form Field Consistency Check:

- set appfw profile <name> -fieldConsistencyAction [**block**] [**learn**] [**log**] [**stats**] [**none**]

To specify relaxations for the Form Field Consistency check, you must use the configuration utility. On the Checks tab of the Modify Form Field Consistency Check dialog box, click Add to open the Add Form Field Consistency Check Relaxation dialog box, or select an existing relaxation and click Open to open the Modify Form Field Consistency Check Relaxation dialog box. Either dialog box provides the same options for configuring a relaxation, as described in "Manual Configuration By Using the Configuration Utility."

Following are examples of Form Field Consistency check relaxations:

Form Field Names

- Choose form fields with the name UserType:

  ^UserType$

- Choose form fields with names that begin with UserType_ and are followed by a string that begins with a letter or number and consists of from one to twenty-one letters, numbers, or the apostrophe or hyphen symbol:

  ^UserType_[0-9A-Za-z][0-9A-Za-z'-]{0,20}$

- Choose form fields with names that begin with Turkish-UserType_ and are otherwise the same as the previous expression, except that they can contain Turkish special characters throughout:

  ^T\xC3\xBCrk\xC3\xA7e-UserType_([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])+$

  Note: See "PCRE Character Encoding Format" for a complete description of supported special characters and how to encode them properly.

- Choose form field names that begin with a letter or number, consist of a combination of letters and/or numbers only, and that contain the string Num anywhere in the string:

  ^[0-9A-Za-z]*Num[0-9A-Za-z]*$

Form Field Action URLs

- Choose URLs beginning with http://www.example.com/search.pl? and containing any string after the query except for a new query:

  ^http://www[.]example[.]com/search[.]pl\?[^?]*$

- Choose URLs that begin with http://www.example-español.com and have paths and filenames that consist of upper-case and lower-case letters, numbers, non-ASCII special characters, and selected symbols in the path. The ñ character and any other special characters are represented as encoded UTF-8 strings containing the hexadecimal code assigned to each special character in the UTF-8 charset:

  ^http://www[.]example-espa\xC3\xB1ol[.]com/(([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|\\x[0-9A-Fa-f][0-9A-Fa-f])*/)*([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])

```
([0-9A-Za-z_-]|\\x[0-9A-Fa-f][0-9A-Fa-f])*[.](asp|htp|php|s?html?)$
```

Note: See "PCRE Character Encoding Format" for a complete description of supported special characters and how to encode them properly.

- Choose all URLs that contain the string /search.cgi?:

```
^[^?<>]*/search[.]cgi\?[^?<>]*$
```

Caution: Regular expressions are powerful. Especially if you are not thoroughly familiar with PCRE-format regular expressions, double-check any regular expressions you write. Make sure that they define exactly the URL you want to add as an exception, and nothing else. Careless use of wildcards, and especially of the dot-asterisk (`.*`) metacharacter/wildcard combination, can have results you do not want or expect, such as blocking access to web content that you did not intend to block or allowing an attack that the Cookie Consistency check would otherwise have blocked.

CSRF Form Tagging Check

The CSRF Form Tagging check tags each web form sent by a protected web site to users with a unique and unpredictable FormID, and then examines the web forms returned by users to ensure that the supplied FormID is correct. This check protects against Cross Site Request Forgery (CSRF) attacks. This check applies only to HTML requests that contain a web form, with or without data. It does not apply to XML requests.

The CSRF Form Tagging check prevents attackers from using their own web forms to send high volume form responses with data to your protected web sites. This check requires relatively little CPU processing capacity compared to certain other security checks that analyze web forms in depth. It is therefore able to handle high volume attacks without seriously degrading the performance of the protected web site or the application firewall itself.

Before you enable the CSRF Form Tagging check, you should be aware of the following:

- You need to enable form tagging. The CSRF check depends on form tagging and does not work without it.
- You should disable the Citrix NetScaler Integrated Caching feature for all web pages containing forms that are protected by that profile. The Integrated Caching feature and CSRF form tagging are not compatible.
- You should consider enabling Referer checking. Referer checking is part of the Start URL check, but it prevents cross-site request forgeries, not Start URL violations. Referer checking also puts less load on the CPU than does the CSRF Form Tagging check. If a request violates Referer checking, it is immediately blocked, so the CSRF Form Tagging check is not invoked.
- The CSRF Form Tagging check does not work with web forms that use different domains in the form-origin URL and form-action URL. For example, CSRF Form Tagging cannot protect a web form with a form-origin URL of `http://www.example.com/` and a form action URL of `http://www.example.org/form.pl`, because `example.com` and `example.org` are different domains.

If you use the wizard or the configuration utility, in the Modify CSRF Form Tagging Check dialog box, on the General tab you can enable or disable the Block, Log, Learn and Statistics actions.

If you use the command-line interface, you can enter the following command to configure the CSRF Form Tagging Check:

- set appfw profile <name> -fieldConsistencyAction [**block**] [**log**] [**learn**] [**stats**] [**none**]

To specify relaxations for the CSRF Form Tagging check, you must use the configuration utility. On the Checks tab of the Modify CSRF Form Tagging Check dialog box, click Add to open the Add CSRF Form Tagging Check Relaxation dialog box, or select an existing relaxation and click Open to open the Modify CSRF Form Tagging Check Relaxation dialog box. Either dialog box provides the same options for configuring a relaxation, as described in "Manual Configuration By Using the Configuration Utility."

Following are examples of CSRF Form Tagging check relaxations:

Note: The following expressions are URL expressions that can be used in both the Form Origin URL and Form Action URL roles.

- Choose URLs beginning with http://www.example.com/search.pl? and containing any string after the query, except for a new query:

  ^http://www[.]example[.]com/search[.]pl\?[^?]*$

- Choose URLs that begin with http://www.example-español.com and have paths and filenames that consist of upper-case and lower-case letters, numbers, non-ASCII special characters, and selected symbols in the path. The ñ character and any other special characters are represented as encoded UTF-8 strings containing the hexadecimal code assigned to each special character in the UTF-8 charset:

  ^http://www[.]example-espa\xC3\xB1ol[.]com/(([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|\\x[0-9A-Fa-f][0-9A-Fa-f])*/)*([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|\\x[0-9A-Fa-f][0-9A-Fa-f])*[.](asp|htp|php|s?html?)$

  Note: See "PCRE Character Encoding Format" for a complete description of supported special characters and how to encode them properly.

- Choose all URLs that contain the string /search.cgi?:

  ^[^?<>]*/search[.]cgi\?[^?<>]*$

Caution: Regular expressions are powerful. Especially if you are not thoroughly familiar with PCRE-format regular expressions, double-check any regular expressions you write. Make sure that they define exactly the URL that you want to add as an exception, and nothing else. Careless use of wildcards, and especially of the dot-asterisk (.*) metacharacter/wildcard combination, can have results you do not want, such as blocking access to web content that you did not intend to block or allowing an attack that the check would otherwise have blocked.

Deny URL Check

The Deny URL check examines and blocks connections to URLs that are commonly accessed by hackers and malicious code. This check contains a list of URLs that are common targets of hackers or malicious code and that rarely if ever appear in legitimate requests. You can also add URLs or URL patterns to the list. The Deny URL check prevents attacks against various security weaknesses known to exist in web server software or on many web sites.

The Deny URL check takes priority over the Start URL check, and thus denies malicious connection attempts even when a Start URL relaxation would normally allow a request to proceed.

If you use the wizard or the configuration utility, in the Modify Deny URL Check dialog box, on the General tab you can enable or disable the Block, Log, and Statistics actions.

If you use the command-line interface, you can enter the following command to configure the Deny URL Check:

- set appfw profile <name> -denyURLAction [**block**] [**log**] [**stats**] [**none**]

To create and configure your own deny URLs, you must use the configuration utility. On the Checks tab of the Modify Deny URL Check dialog box, click Add to open the Add Deny URL dialog box, or select an existing user-defined deny URL and click Open to open the Modify Deny URLdialog box. Either dialog box provides the same options for creating and configuring a deny URL, as described in "Manual Configuration By Using the Configuration Utility."

Following are examples of Deny URL expressions:

- Do not allow users to access the image server at `images.example.com` directly:

  ^http://images[.]example[.]com$

- Do not allow users to access CGI (`.cgi`) or PERL (`.pl`) scripts directly:

  ^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]*/)*
  [0-9A-Za-z][0-9A-Za-z_.-]*[.](cgi|pl)$

- Here is the same deny URL, modified to support non-ASCII characters:

  ^http://www[.]example[.]com/(([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])
  ([0-9A-Za-z_-]|\\x[0-9A-Fa-f][0-9A-Fa-f])*/)*([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])
  ([0-9A-Za-z_-]|\\x[0-9A-Fa-f][0-9A-Fa-f])*[.](cgi|pl)$

  Note: See "PCRE Character Encoding Format" for a complete description of supported special characters and how to encode them properly.

Caution: Regular expressions are powerful. Especially if you are not thoroughly familiar with PCRE-format regular expressions, double-check any regular expressions you write. Make sure that they define exactly the URL or pattern that you want to block, and nothing else. Careless use of wildcards, and especially of the dot-asterisk (`.*`) metacharacter/wildcard combination, can have results that you do not want, such as

blocking access to web content that you did not intend to block.

URL Protection Checks

The URL Protection checks examine request URLs to prevent attackers from aggressively attempting to access multiple URLs (*forceful browsing*) or using a URL to trigger a known security vulnerability in web server software or web site scripts.

Start URL Check

The Start URL check examines the URLs in incoming requests and blocks the connection attempt if the URL does not meet the specified criteria. To meet the criteria, the URL must match an entry in the Start URL list, unless the Enforce URL Closure parameter is enabled. If you enable this parameter, a user who clicks a link on your Web site is connected to the target of that link.

The primary purpose of the Start URL check is to prevent repeated attempts to access random URLs on a Web site, (*forceful browsing*). Forceful browsing can be used to trigger a buffer overflow, find content that users were not intended to access directly, or find a back door into secure areas of your Web server.

If you use the wizard or the configuration utility, in the Modify Start URL Check dialog box, on the General tab you can enable or disable Block, Log, Statistics, Learn actions, and the following parameters:

- **Enforce URL Closure.** Allow users to access any web page on your web site by clicking a hyperlink on any other page on your web site. Users can navigate to any page on your web site that can be reached from the home page or any designated start page by clicking hyperlinks.

  Note: The URL closure feature allows any query string to be appended to and sent with the action URL of a web form submitted by using the HTTP GET method. If your protected web sites use forms to access an SQL database, make sure that you have the SQL injection check enabled and properly configured.

- **Sessionless URL Closure.** From the client's point of view, this type of URL closure functions in exactly the same way as standard, session-aware URL Closure, but uses a token embedded in the URL instead of a cookie to track the user's activity, which consumes considerably fewer resources.

  Note: When enabling sessionless (Sessionless URL Closure), you must also enable regular URL closure (Enforce URL Closure) or sessionless URL closure does not work.

- **Validate Referer Header.** Verify that the Referer header in a request that contains web form data from your protected web site instead of another web site. This action verifies that your web site, not an outside attacker, is the source of the web form. Doing so protects against cross-site request forgeries (CSRF) without requiring form tagging, which is more CPU-intensive than header checks. The application firewall can handle the HTTP Referer header in one of the following three ways, depending on which option you select in the drop-down list:

  - **Off.** Do not validate the Referer header.

  - **If-Present.** Validate the Referer header if a Referer header exists. If an invalid Referer header is found, the request generates a referer-header violation. If no Referer header exists, the request does not generate a referer-header violation. This option enables the application firewall to perform Referer header validation on requests that contain a Referer header, but not block requests from users whose browsers do not set the Referer header or who use web proxies or filters that remove that header.

- **Always.** Always validate the Referer header. If there is no Referer header, or if the Referer header is invalid, the request generates a referer-header violation.

Note: Although the referer header check and Start URL security check share the same action settings, it is possible to violate the referer header check without violating the Start URL check. The difference is visible in the logs, which log referer header check violations separately from Start URL check violations.

One Start URL setting, Exempt Closure URLs from Security Checks, is not configured in the Modify Start URL Check dialog box, but in the Settings tab of the Configure Application Firewall Profile dialog box. If enabled, this setting directs the application firewall not to run further security checks on URLs that meet the URL Closure criteria.

If you use the command-line interface, you can enter the following commands to configure the Start URL Check:

- set appfw profile <name> -startURLAction [**block**] [**learn**] [**log**] [**stats**] [**none**]
- set appfw profile <name> -startURLClosure ([**ON**] | [**OFF**])
- set appfw profile <name> -sessionlessURLClosure ([**ON**] | [**OFF**])
- set appfw profile <name> -exemptClosureURLsFromSecurityChecks ([**ON**] | [**OFF**])
- set appfw profile <name> -RefererHeaderCheck ([**none**] | [**if-present**] | [**always**])

To specify relaxations for the Start URL check, you must use the configuration utility. On the Checks tab of the Modify Start URL Check dialog box, click Add to open the Add Start URL Check Relaxation dialog box, or select an existing relaxation and click Open to open the Modify Start URL Check Relaxation dialog box. Either dialog box provides the same options for configuring a relaxation, as described in "Manual Configuration By Using the Configuration Utility."

Following are examples of Start URL check relaxations:

- Allow users to access the home page at `www.example.com`:

  ^http://www[.]example[.]com$

- Allow users to access all static HTML (`.htm` and `.html`), server-parsed HTML (`.htp` and `.shtml`), PHP (`.php`), and Microsoft ASP (`.asp`) format web pages at `www.example.com`:

  ^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]*/)*
  [0-9A-Za-z][0-9A-Za-z_.-]*[.](asp|htp|php|s?html?)$

- Allow users to access web pages with pathnames or file names that contain non-ASCII characters at `www.example-español.com`:

  ^http://www[.]example-espa\xC3\xB1ol[.]com/(([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|\\x
  ([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|\\x[0-9A-Fa-f][0-9A-Fa-f])*[.](asp|htp|php|s?html?)

Note: In the above expression, each character class has been grouped with the string `\\x[0-9A-Fa-f][0-9A-Fa-f]`, which matches all properly-constructed character encoding strings but does not allow stray backslash characters that are not associated with a UTF-8 character encoding string. The double backslash (\\) is an escaped backslash, which tells the application firewall to interpret it as a literal backslash. If you included only one backslash, the application firewall would instead interpret the following left square bracket ([) as a literal character instead of the opening of a character class, which would break the expression. See "PCRE Character Encoding Format" for a complete description of supported special characters and how to encode them properly.

- Allow users to access all GIF (`.gif`), JPEG (`.jpg` and `.jpeg`), and PNG (`.png`) format graphics at `www.example.com`:

  ^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]*/)*
  [0-9A-Za-z][0-9A-Za-z_.-]*[.](gif|jpe?g|png)$

- Allow users to access CGI (`.cgi`) and PERL (`.pl`) scripts, but only in the CGI-BIN directory:

  ^http://www[.]example[.]com/CGI-BIN/[0-9A-Za-z][0-9A-Za-z_.-]*[.](cgi|pl)$

- Allow users to access Microsoft Office and other document files in the `docsarchive` directory:

  ^http://www[.]example[.]com/docsarchive/[0-9A-Za-z][0-9A-Za-z_-.]*[.](doc|xls|pdf|ppt)$

Caution: Regular expressions are powerful. Especially if you are not thoroughly familiar with PCRE-format regular expressions, double-check any regular expressions that you write. Make sure that they define exactly the URL you want to add as an exception, and nothing else. Careless use of wildcards, and especially of the dot-asterisk (`.*`) metacharacter/wildcard combination, can have results you do not want, such as blocking access to web content that you did not intend to block or allowing an attack that the Start URL check would otherwise have blocked.

Deny URL Check

The Deny URL check examines and blocks connections to URLs that are commonly accessed by hackers and malicious code. This check contains a list of URLs that are common targets of hackers or malicious code and that rarely if ever appear in legitimate requests. You can also add URLs or URL patterns to the list. The Deny URL check prevents attacks against various security weaknesses known to exist in web server software or on many web sites.

The Deny URL check takes priority over the Start URL check, and thus denies malicious connection attempts even when a Start URL relaxation would normally allow a request to proceed.

If you use the wizard or the configuration utility, in the Modify Deny URL Check dialog box, on the General tab you can enable or disable the Block, Log, and Statistics actions.

If you use the command-line interface, you can enter the following command to configure the Deny URL Check:

- set appfw profile <name> -denyURLAction [**block**] [**log**] [**stats**] [**none**]

To create and configure your own deny URLs, you must use the configuration utility. On the Checks tab of the Modify Deny URL Check dialog box, click Add to open the Add Deny URL dialog box, or select an existing user-defined deny URL and click Open to open the Modify Deny URLdialog box. Either dialog box provides the same options for creating and configuring a deny URL, as described in "Manual Configuration By Using the Configuration Utility."

Following are examples of Deny URL expressions:

- Do not allow users to access the image server at `images.example.com` directly:

  ^http://images[.]example[.]com$

- Do not allow users to access CGI (`.cgi`) or PERL (`.pl`) scripts directly:

  ^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]*/)*
  [0-9A-Za-z][0-9A-Za-z_.-]*[.](cgi|pl)$

- Here is the same deny URL, modified to support non-ASCII characters:

  ^http://www[.]example[.]com/(([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])
  ([0-9A-Za-z_-]|\\x[0-9A-Fa-f][0-9A-Fa-f])*/)*([0-9A-Za-z]|\\x[0-9A-Fa-f][0-9A-Fa-f])
  ([0-9A-Za-z_-]|\\x[0-9A-Fa-f][0-9A-Fa-f])*[.](cgi|pl)$

  Note: See "PCRE Character Encoding Format" for a complete description of supported special characters and how to encode them properly.

Caution: Regular expressions are powerful. Especially if you are not thoroughly familiar with PCRE-format regular expressions, double-check any regular expressions you write. Make sure that they define exactly the URL or pattern that you want to block, and nothing else. Careless use of wildcards, and especially of the dot-asterisk (`.*`) metacharacter/wildcard combination, can have results that you do not want, such as

blocking access to web content that you did not intend to block.

XML Protection Checks

The XML Protection checks examine requests for XML-based attacks of all types.

Caution: The XML security checks apply only to content that is sent with an HTTP content-type header of text/xml. If the content-type header is missing, or is set to a different value, all XML security checks are bypassed. If you plan to protect XML or Web 2.0 web applications, the webmasters of each web server that hosts those applications should ensure that the proper HTTP content-type header is sent.

XML Format Check

The XML Format check examines the XML format of incoming requests and blocks those requests that are not well formed or that do not meet the criteria in the XML specification for properly-formed XML documents. Some of those criteria are:

- An XML document must contain only properly-encoded Unicode characters that match the Unicode specification.
- No special XML syntax characters—such as < , > and &—can be included in the document except when used in XML markup.
- All begin, end, and empty-element tags must be correctly nested, with none missing or overlapping.
- XML element tags are case-sensitive. All beginning and end tags must match exactly.
- A single root element must contain all the other elements in the XML document.

A document that does not meet the criteria for well-formed XML does not meet the definition of an XML document. Strictly speaking, it is not XML. However, not all XML applications and web services enforce the XML well-formed standard, and not all handle poorly-formed or invalid XML correctly. Inappropriate handling of a poorly-formed XML document can cause security breaches. The purpose of the XML Format check is to prevent a malicious user from using a poorly-formed XML request to breach security on your XML application or web service.

If you use the wizard or the configuration utility, in the Modify XML Format Check dialog box, on the General tab you can enable or disable the Block, Log, and Statistics actions.

If you use the command-line interface, you can enter the following command to configure the XML Format Check:

- set appfw profile <name> -xmlFormatAction [**block**] [**log**] [**stats**] [**none**]

You cannot configure exceptions to the XML Format check. You can only enable or disable it.

XML Denial-of-Service Check

The XML Denial of Service (*XML DoS* or *XDoS*) check examines incoming XML requests to determine whether they match the characteristics of a denial-of-service (DoS) attack, and blocks those requests that do. The purpose of the XML DoS check is to prevent an attacker from using XML requests to launch a denial-of-service attack on your web server or web site.

If you use the wizard or the configuration utility, in the Modify XML Denial-of-Service Check dialog box, on the General tab you can enable or disable the Block, Log, Statistics, and Learn actions:

If you use the command-line interface, you can enter the following command to configure the XML Denial-of-Service check:

- set appfw profile <profileName> -xmlDoSAction [**block**] [**log**] [**learn**] [**stats**] [**none**]

To configure individual XML Denial-of-Service rules, you must use the configuration utility. On the Checks tab of the Modify XML Denial-of-Service Check dialog box, select a rule and click Open to open the Modify XML Denial-of-Service dialog box for that rule. The individual dialog boxes differ for the different rules but are extremely simple. Some only allow you to enable or disable the rule; others allow you to modify a number by typing a new value in a text box.

The individual XML Denial-of-Service rules are:

Maximum Element Depth

Restrict the maximum number of nested levels in each individual element to 256. If this rule is enabled, and the application firewall detects an XML request with an element that has more than the maximum number of allowed levels, it blocks the request. You can modify the maximum number of levels to any value from one (1) to 65,535.

Maximum Element Name Length

Restrict the maximum length of each element name to 128 characters. This includes the name within the expanded namespace, which includes the XML path and element name in the following format:

{http://prefix.example.com/path/}target_page.xml

The user can modify the maximum name length to any value between one (1) character and 65,535.

Maximum # Elements

Restrict the maximum number of any one type of element per XML document to 65,535. You can modify the maximum number of elements to any value between one (1) and 65,535.

Maximum # Element Children

Restrict the maximum number of children (including other elements, character information, and comments) each individual element is allowed to have to 65,535. You can modify the maximum number of element children to any value between one (1) and 65,535.

Maximum # Attributes

Restrict the maximum number of attributes each individual element is allowed to have to 256. You can modify the maximum number of attributes to any value between one (1) and 256.

Maximum Attribute Name Length

Restrict the maximum length of each attribute name to 128 characters. You can modify the maximum attribute name length to any value between one (1) and 2,048.

Maximum Attribute Value Length

Restrict the maximum length of each attribute value to 2048 characters. You can modify the maximum attribute name length to any value between one (1) and 2,048.

Maximum Character Data Length

Restrict the maximum character data length for each element to 65,535. You can modify the length to any value between one (1) and 65,535.

Maximum File Size

Restrict the size of each file to 20 MB. You can modify the maximum file size to any value.

Minimum File Size

Require that each file be at least 9 bytes in length. You can modify the minimum file size to any positive integer representing a number of bytes.

Maximum # Entity Expansions

Limit the number of entity expansions allowed to the specified number. Default: 1024.

Maximum Entity Expansion Depth

Restrict the maximum number of nested entity expansions to no more than the specified number. Default: 32.

Maximum # Namespaces

Limit the number of namespace declarations in an XML document to no more than the specified number. Default: 16.

Maximum Namespace URI Length

Limit the URL length of each namespace declaration to no more than the specified number of characters. Default: 256.

Block Processing Instructions

Block any special processing instructions included in the request. This rule has no user-modifiable values.

Block DTD

Block any document type definitions (*DTD*) included with the request. This rule has no user-modifiable values.

Block External Entities

Block all references to external entities in the request. This rule has no user-modifiable values.

SOAP Array Check

Enable or disable the following SOAP array checks:

- **Maximum SOAP Array Size.** The maximum total size of all SOAP arrays in an XML request before the connection is blocked. You can modify this value. Default: 20000000.
- **Maximum SOAP Array Rank.** The maximum rank or dimensions of any single SOAP array in an XML request before the connection is blocked. You can modify this value. Default: 16.

XML Cross-Site Scripting Check

The XML Cross-Site Scripting check examines both the headers and the bodies of user requests for possible cross-site scripting attacks. If it finds a possible cross-site scripting attack, it blocks the request.

To prevent misuse of the scripts on your protected web services to breach security on your web services, the XML Cross-Site Scripting check blocks scripts that violate the *same origin rule*, which states that scripts should not access or modify content on any server but the server on which they are located. Any script that violates the same origin rule is called a cross-site script, and the practice of using scripts to access or modify content on another server is called cross-site scripting. The reason cross-site scripting is a security issue is that a web server that allows cross-site scripting can be attacked with a script that is not on that web server, but on a different web server, such as one owned and controlled by the attacker.

Unfortunately, many companies have a large installed base of JavaScript-enhanced web content that violates the same origin rule. If you enable the XML Cross-Site Scripting check on such a site, you have to generate the appropriate exceptions so that the check does not block legitimate activity. In addition, to prevent blocking of legitimate requests, this check ignores cookies that were set by the server, even if they contain elements that the Cookie Consistency check would otherwise block. You should keep that in mind when configuring this check.

If you use the wizard or the configuration utility, in the Modify Cookie Consistency Check dialog box, on the General tab you can enable or disable the Block, Log, and Statistics actions, and the following parameters:

- **Transform.** Make the following changes to requests that match the XML Cross-Site Scripting check:
  - Left angle bracket (<) to HTML character entity equivalent (<)
  - Right angle bracket (>) to HTML character entity equivalent (>)

  These changes prevent browsers from interpreting unsafe html tags, such as `<script>`, and thereby executing malicious code. If you enable both request-header checking and transformation, any special characters found in request headers are also modified as described above. If scripts on your protected web site contain cross-site scripting features, but your web site does not rely upon those scripts to operate correctly, you can safely disable blocking and enable transformation. This configuration ensures that no legitimate web traffic is blocked, while stopping any potential cross-site scripting attacks.

- **Check complete URLs.** If checking of complete URLs is enabled, the application firewall examines entire URLs for XML Cross-Site Scripting attacks instead of checking just the query portions of URLs.

- **Check Request headers.** If Request header checking is enabled, the application firewall examines request headers for XML Cross-Site Scripting attacks, instead of examining just URLs.

If you use the command-line interface, you can enter the following commands to configure the XML Cross-Site Scripting Check:

- set appfw profile <name> -crossSiteScriptingAction [**block**] [**learn**] [**log**] [**stats**] [**none**]
- set appfw profile <name> -crossSiteScriptingTransformUnsafeHTML ([**ON**] | [**OFF**])
- set appfw profile <name> -crossSiteScriptingCheckCompleteURLs ([**ON**] | [**OFF**])

To specify relaxations for the XML Cross-Site Scripting check, you must use the configuration utility. On the Checks tab of the Modify XML Cross-Site Scripting Check dialog box, click Add to open the Add XML Cross-Site Scripting Check Relaxation dialog box, or select an existing relaxation and click Open to open the Modify XML Cross-Site Scripting Check Relaxation dialog box. Either dialog box provides the same options for configuring a relaxation, as described in "Manual Configuration By Using the Configuration Utility."

Following are examples of XML Cross-Site Scripting check relaxations:

- **Name element or attribute.** The following expression exempts all elements beginning with the string `name_` followed by a string of upper- and lower-case letters or numbers that is at least two characters long and no more than fifteen characters long:

  ^name_[0-9A-Za-z]{2,15}$

- **URL element or attribute.** The following expression exempts URLs with hostnames of `web.example.com`, with a path up to four levels deep followed by an optional filename and extension, but no HTML or query symbols :

  ^https?://web[.]example[.]com(/[^<>?]{1,30}){0,4}(/[^<>?]{1,30})*$

- **URL element or attribute (special characters).** The following expression exempts URLs with hostnames of `web.türkçe-example.com`, with the same path and file restrictions as above:

  ^https?://web[.]t\xC3\xBCrk\xC3\xA7e-example[.]com(/[^<>?]{1,30}){0,4}(/[^<>?]{1,30})*$

  Note: See "PCRE Character Encoding Format" for a complete description of supported special characters and how to encode them properly.

Caution: Regular expressions are powerful. Especially if you are not thoroughly familiar with PCRE-format regular expressions, double-check any regular expressions you write. Make sure that they define exactly the URL that you want to add as an exception, and nothing else. Careless use of wildcards, and especially of the dot-asterisk (`.*`) metacharacter/wildcard combination, can have results that you do not want, such as blocking access to web content that you did not intend to block or allowing an attack that the XML Cross-Site Scripting check would otherwise have blocked.

XML SQL Injection Check

The XML SQL Injection check examines both the headers and the bodies of user requests for possible XML SQL Injection attacks. If it finds injected SQL, it blocks the request.

To prevent misusing the scripts on your protected web services to breach security on your web services, the XML SQL Injection check blocks scripts that violate the *same origin rule*, which states that scripts should not access or modify content on any server but the server on which they are located. Any script that violates the same origin rule is called a cross-site script, and the practice of using scripts to access or modify content on another server is called XML SQL Injection. The reason XML SQL Injection is a security issue is that a web server that allows XML SQL Injection can be attacked with a script that is not on that web server, but on a different web server, such as one owned and controlled by the attacker.

Unfortunately, many companies have a large installed base of JavaScript-enhanced web content that violates the same origin rule. If you enable the XML SQL Injection check on such a site, you have to generate the appropriate exceptions so that the check does not block legitimate activity. In addition, to prevent blocking of legitimate requests, this check ignores cookies that were set by the server, even if they contain elements that the Cookie Consistency check would otherwise block. You should keep this in mind when configuring this check.

Note: To prevent blocking of legitimate requests, this check ignores cookies that were set by the server, even if they contain elements that the Cookie Consistency check would otherwise block.

If you use the wizard or the configuration utility, in the Modify XML SQL Injection Check dialog box, on the General tab you can enable or disable Block, Log, and Statistics actions, and the following parameters:

- **Restrict checks to fields containing SQL special characters.** If you configure the application firewall to check only fields that contain SQL special strings, the application firewall skips web form fields that do not contain special characters. Since most SQL servers do not process SQL commands that are not preceded by a special character, enabling this parameter can significantly reduce the load on the application firewall and speed up processing without placing your protected web sites at risk.

- **SQL comments handling.** By default, the application firewall checks all SQL comments for injected SQL commands. Many SQL servers ignore anything in a comment, however, even if it is preceded by an SQL special character. For faster processing, if your SQL server ignores comments, you can configure the application firewall to skip comments when examining requests for injected SQL. The SQL comments handling options are:

    - **ANSI.** Skip ANSI-format SQL comments, which are normally used by UNIX-based SQL databases.

    - **Nested.** Skip nested SQL comments, which are normally used by Microsoft SQL Server.

    - **ANSI/Nested.** Skip comments that adhere to both the ANSI and nested SQL comment standards. Comments that match only the ANSI standard, or only the nested standard, are checked for injected SQL.

Caution: In most cases, you should not choose the Nested or the ANSI/Nested option unless your database runs on Microsoft SQL Server. Most other types of SQL server software do not recognize nested comments. If nested comments appear in a request directed to another type of SQL server, they may indicate an attempt to breach security on that server.

- **Check all Comments.** Check the entire request for injected SQL, without skipping anything. The default setting.

- **Check Request headers.** If Request header checking is enabled, the application firewall examines the headers of requests for XML SQL Injection attacks, instead of just URLs.

  Caution: If you enable both request header checking and transformation, any SQL special characters found in headers are also transformed. The Accept, Accept-Charset, Accept-Encoding, Accept-Language, Expect, and User-Agent headers normally contain semicolons (;), so enabling both Request header checking and transformation simultaneously may cause errors.

If you use the command-line interface, you can enter the following commands to configure the XML SQL Injection Check:

- set appfw profile <name> -XMLSQLInjectionAction [**block**] [**learn**] [**log**] [**stats**] [**none**]
- set appfw profile <name> -XMLSQLInjectionOnlyCheckFieldsWithSQLChars (**ON** | **OFF**)]
- set appfw profile <name> -XMLSQLInjectionParseComments ([**checkall**] | [**ansi** | **nested**] | [**ansinested**])

You configure the exceptions to the XML SQL Injection check by opening the Modify XML SQL Injection Check dialog box, Checks tab. An exception can consist of either a literal string or a PCRE-format regular expression. For information about adding, modifying, removing, enabling, or disabling exceptions, see "Manual Configuration By Using the Configuration Utility."

Following are examples of XML SQL Injection check relaxations:

- **Name element or attribute.** The following expression exempts all elements beginning with the string `name_` followed by a string of upper- and lower-case letters or numbers that is at least two characters long and no more than fifteen characters long:

  ```
  ^name_[0-9A-Za-z]{2,15}$
  ```

- **URL element or attribute.** The following expression exempts URLs with hostnames of `web.example.com`, with a path up to four levels deep followed by an optional file name and extension, but no HTML or query symbols :

  ```
  ^https?://web[.]example[.]com(/[^<>?]{1,30}){0,4}(/[^<>?]{1,30})*$
  ```

- **URL element or attribute (special characters).** The following expression exempts URLs with hostnames of `web.türkçe-example.com`, with the same path and file restrictions as above:

^https?://web[.]t\xC3\xBCrk\xC3\xA7e-example[.]com(/[^<>?]{1,30}){0,4}(/[^<>?]{1,30})*$

Note: See "PCRE Character Encoding Format" for a complete description of supported special characters and how to encode them properly.

XML Attachment Check

The XML Attachment check examines incoming requests for malicious attachments, and it blocks those requests that contain attachments that might breach applications security. The purpose of the XML Attachment check is to prevent an attacker from using an XML attachment to breach security on your server.

If you use the wizard or the configuration utility, in the Modify XML Attachment Check dialog box, on the General tab you can enable or disable the Block, Learn, Log, Statistics, and Learn actions:

If you use the command-line interface, you can enter the following command to configure the XML Attachment Check:

- set appfw profile <name> -xmlAttachmentAction [**block**] [**learn**] [**log**] [**stats**] [**none**]

You must configure the other XML Attachment check settings in the configuration utility. In the Modify XML Attachment Check dialog box, on the Checks tab, you can configure the following settings:

- **Maximum Attachment Size.** Allow attachments that are no larger than the maximum attachment size you specify. To enable this option, first select the Enabled check box, and then type the maximum attachment size in bytes in the Size text box.
- **Attachment Content Type.** Allow attachments of the specified content type. To enable this option, first select the Enabled check box, and then enter a regular expression that matches the Content-Type attribute of the attachments that you want to allow.
    - You can type the URL expression directly in the text window. If you do so, you can use the Regex Tokens menu to enter a number of useful regular expressions at the cursor instead of typing them manually.
    - You can click Regex Editor to open the Add Regular Expression dialog box and use it to construct the URL expression.

Web Services Interoperability Check

The Web Services Interoperability (WS-I) check examines both requests and responses for adherence to the WS-I standard, and blocks those requests and responses that do not adhere to this standard. The purpose of the WS-I check is to block requests that might not interact with other XML appropriately. An attacker can use inconsistencies in interoperability to launch an attack on your XML application.

If you use the wizard or the configuration utility, in the Modify Web Services Interoperability Check dialog box, on the General tab you can enable or disable the Block, Log, Statistics, and Learn actions.

If you use the command-line interface, you can enter the following command to configure the Web Services Interoperability check:

- set appfw profile <name> -xmlWSIAction [**block**] [**log**] [**learn**] [**stats**] [**none**]

To configure individual Web Services Interoperability rules, you must use the configuration utility. On the Checks tab of the Modify Web Services Interoperability Check dialog box, select a rule and click Enable or Disable to enable or disable the rule. You can also click Open to open the Web Services Interoperability Detail message box for that rule. The message box displays read-only information about the rule. You cannot modify or make other configuration changes to any of these rules.

XML Message Validation Check

The XML Message Validation check examines requests that contain XML messages to ensure that they are valid. If a request contains an invalid XML message, the application firewall blocks the request. The purpose of the XML Validation check is to prevent an attacker from using specially constructed invalid XML messages to breach the security of your application.

If you use the wizard or the configuration utility, in the Modify XML Message Validation Check dialog box, on the General tab you can enable or disable the Block, Log, and Statistics actions.

If you use the command-line interface, you can enter the following command to configure the XML Message Validation Check:

- set appfw profile <name> -xmlValidationAction [**block**] [**log**] [**stats**] [**none**]

You must use the configuration utility to configure the other XML Validation check settings. In the Modify XML Message Validation Check dialog box, on the Checks tab, you can configure the following settings:

- **XML Message Validation.** Use one of the following options to validate the XML message:
  - **SOAP Envelope.** Validate only the SOAP envelope of XML messages.
  - **WSDL.** Validate XML messages by using an XML SOAP WSDL. If you choose WSDL validation, in the WSDL Object drop-down list you must choose a WSDL. If you want to validate against a WSDL that has not already been imported to the application firewall, you can click the Import button to open the Manage WSDL Imports dialog box and import your WSDL. See "WSDL" for more information.
    - If you want to validate the entire URL, leave the Absolute radio button in the End Point Check button array selected. If you want to validate only the portion of the URL after the host, select the Relative radio button.
    - If you want the application firewall to enforce the WSDL strictly, and not allow any additional XML headers not defined in the WSDL, you must clear the Allow additional headers not defined in the WSDL check box.

      Caution: If you uncheck the Allow Additional Headers not defined in the WSDL check box, and your WSDL does not define all XML headers that your protected XML application or Web 2.0 application expects or that a client sends, you may block legitimate access to your protected service.
  - **XML Schema.** Validate XML messages by using an XML schema. If you choose XML schema validation, in the XML Schema Object drop-down list you must choose an XML schema. If you want to validate against an XML schema that has not already been imported to the application firewall, you can click the Import button to open the Manage XML Schema Imports dialog box and import your WSDL. See "WSDL" for more information.
- **Response Validation.** By default, the application firewall does not attempt to validate responses. If you want to validate responses from your protected application or Web 2.0 site, select the Validate Response check box. When you do, the Reuse the XML Schema

specified in request validation check box and the XML Schema Object drop-down list are activated.

- Check the Reuse XML Schema check box to use the schema you specified for request validation to do response validation as well.

  Note: If you check this check box, the XML Schema Object drop-down list is grayed out.

- If you want to use a different XML schema for response validation, use the XML Schema Object drop-down list to select or upload that XML schema .

XML SOAP Fault Filtering Check

The XML SOAP Fault Filtering check examines responses from your protected web services and filters out XML SOAP faults. This prevents leaking of sensitive information to attackers.

If you use the wizard or the configuration utility, in the Modify XML SOAP Fault Filtering Check dialog box, on the General tab you can enable or disable the Block, Log, and Statistics actions, and the Remove action, which removes SOAP faults before forwarding the response to the user.

If you use the command-line interface, you can enter the following command to configure the XML SOAP Fault Filtering Check:

set appfw profile <name> -XMLSOAPFaultAction [**block**] [**log**] [**stats**] [**none**]

You cannot configure exceptions to the XML SOAP Fault Filtering check. You can only enable or disable it.

Profiles

A profile is a collection of security settings that are used to protect specific types of web content or specific parts of your web site. In a profile, you determine how the application firewall applies each of its filters (or checks) to requests to your web sites, and responses from them. There are three types of profile:

- **HTML.** Protects HTML-based web pages.
- **XML.** Protects XML-based web services and web sites.
- **Web 2.0.** Protects Web 2.0 content that combines HTML and XML content, such as ATOM feeds, blogs, and RSS feeds.

The application firewall has a number of security checks, all of which can be enabled or disabled, and configured in a number of ways in each profile. Each profile also has a number of settings that control how it handles different types of content. Finally, rather than manually configuring all of the security checks, you can enable and configure the learning feature. This feature observes normal traffic to your protected web sites for a period of time, and uses those observations to provide you with a tailored list of recommended exceptions (*relaxations*) to some security checks, and additional rules for other security checks.

During initial configuration, whether by using the Application Firewall Wizard or manually, you create one general purpose profile to protect all content on your web sites that is not covered by a more specific profile. After that, you can create as many specific profiles as you want to protect more specialized content.

The Profiles pane contains the following elements:

Name. Displays all the application firewall profiles configured in the appliance.

Type. Displays the profile type: HTML, XML, or Web 2.0.

Add. "Add a new profile."

Open. "Configure the selected profile's" security checks, settings, and learning.

Remove. Remove the selected profile.

Change Profile Type. "Change the profile type" of the selected profile.

Statistics. View the statistics for the selected profile.

Creating Application Firewall Profiles

Creating an application firewall profile is simple, and requires that you specify only two options. You specify basic or advanced *defaults*, the default configuration for the various security checks and settings that are part of a profile, and choose the profile *type* to match the type of content that the profile is intended to protect.

There are three profile types:

- **HTML.** Protects standard HTML-based web sites.
- **XML.** Protects XML-based web services and web sites.
- **Web 2.0 (HTML XML).** Protects sites that contain both HTML and XML elements, such as ATOM feeds, blogs, and RSS feeds.

An application firewall profile name cannot be the same as the name assigned to any other profile or action in any feature on the NetScaler appliance. Certain action or profile names are assigned to built-in actions or profiles, and can never be used for user profiles. (A complete list of disallowed names can be found in the Application Firewall ProfileSupplemental Information.) If you attempt to create a profile with a name that has already been used for an action or a profile, an error message is displayed and the profile is not created.

To create an application firewall profile by using the command line interface

At the command prompt, type the following commands:

- add appfw profile <name> [-defaults (**basic** | **advanced**)]
- set appfw profile <name> -type (**HTML** | **XML** | **HTML XML**)
- save ns config

Example

The following example adds a profile named `pr-basic`, with basic defaults, and assigns a profile type of `HTML`. This is the appropriate initial configuration for a profile to protect an HTML Web site.

```
add appfw profile pr-basic -defaults basic
set appfw profile pr-basic -type HTML
save ns config
```

Parameters for Creating Application Firewall Profiles

name (Profile Name)

A name for the profile. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) symbols.

defaults (Defaults)

You can choose one of two default configurations when you create a profile: Basic or Advanced. A profile created with basic defaults should protect most Web sites while requiring little additional configuration. A profile created with advanced defaults is intended to protect more complex Web sites requiring additional configuration. You can modify either type of default configuration.

type (Profile Type)

The type of content that the profile will protect. There are three types of profile: **HTML** (HTML), **XML** (XML), or **Web 2.0** (HTML XML). If you are unsure what types of content your profile will protect, you can specify Web 2.0 to make the full range of Application Firewall security checks available to protect your Web site.

To create an application firewall profile by using the configuration utility

Creating an application firewall profile requires that you specify only a few configuration details.

1. In the navigation pane, expand Application Firewall, and then select Profiles.
2. In the details pane, click Add.
3. In the Create Application Firewall Profile dialog box, type a name for your profile.

   The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) symbols.
4. Choose the profile type from the drop-down list.

   The profile types are HTML (for HTML-based Web sites), XML (for XML-based Web services) and Web 2.0 (for blogs, RSS feeds, wikis, and other sites that contain both HTML and XML).

   Note: If you are unsure what types of content your profile will protect, you can choose Web 2.0 to make the full range of Application Firewall security checks available to protect your Web site.
5. If you plan to use the learning feature or to enable and configure a large number of advanced protections, select Advanced. Otherwise, select Basic.

You probably should use the learning feature if you plan to configure either of the SQL injection checks, either of the cross-site scripting checks, any check that provides protection against Web form attacks, or the cookie consistency check. Unless you include the proper exceptions for your protected Web sites when configuring these checks, they can block legitimate traffic. Anticipating all of the necessary exceptions without creating any that are too broad is difficult. The learning feature makes this task much easier.

6. Click Create, and then click Close.

Configuring Application Firewall Profiles

The primary tasks in configuring an application firewall profile are configuring the security checks, which are called *deep protections* or *advanced protections* in the application firewall wizard. In addition, you can configure a number of other settings that control the behavior, not of a single security check, but the application firewall feature.

For more information about the application firewall security checks, see "Advanced Protections."

To configure an application firewall profile by using the command line

At the command prompt, type the following commands:

- set appfw profile <name> <arg1> [<arg2> ...]

  where:

  - <arg1> = a parameter and any associated options.
  - <arg2> = a second parameter and any associated options.
  - ... = additional parameters and options.

  For descriptions of the parameters to use when configuring specific security checks, see "Advanced Protections."

- save ns config

Example

The following example shows how to configure an HTML profile created with basic defaults to begin protecting a simple HTML-based Web site. This example turns on logging and maintenance of statistics for most security checks, but enables blocking only for those checks that have extremely low false positive rates and require no special configuration. It also turns on transformation of unsafe HTML and unsafe SQL, which prevents attacks but does not block requests to your Web sites. With logging and statistics enabled, you can later review the logs to determine whether to enable blocking for a specific security check.

```
set appfw profile -startURLAction log stats
set appfw profile -denyURLAction block log stats
set appfw profile -cookieConsistencyAction log stats
set appfw profile -crossSiteScriptingAction log stats
set appfw profile -crossSiteScriptingTransformUnsafeHTML ON
set appfw profile -fieldConsistencyAction log stats
set appfw profile -SQLInjectionAction log stats
set appfw profile -SQLInjectionTransformSpecialChars ON
```

```
set appfw profile -SQLInjectionOnlyCheckFieldsWithSQLChars ON
set appfw profile -SQLInjectionParseComments checkall
set appfw profile -fieldFormatAction log stats
set appfw profile -bufferOverflowAction block log stats
set appfw profile -CSRFtagAction log stats
save ns config
```

To configure an application firewall profile by using the configuration utility

1. Navigate to Application Firewall > Profiles.
2. In the details pane, select the profile that you want to configure, and then click Open.
3. In the Configure Application Firewall Profile dialog box, on the Security Checks tab, configure the security checks.
   - To enable or disable an action for a check, in the list, select or clear the check box for that action.
   - To configure other parameters for those checks that have them, in the list, click the blue chevron to the far right of that check. In the dialog box that appears, configure the parameters. These vary from check to check.

     You can also select a check and, at the bottom of the dialog box, click Open to display the Configure Relaxation dialog box or Configure Rule dialog box for that check. These dialog boxes also vary from check to check. Most of them include a Checks tab and a General tab. If the check supports relaxations or user-defined rules, the Checks tab includes an Add button, which opens yet another dialog box, in which you can specify a relaxation or rule for the check. (A relaxation is a rule for exempting specified traffic from the check.) If relaxations have already been configured, you can select one and click Open to modify it.

     For more information about the Configure Relaxation or Configure Rule dialog boxes, see "Configuring an Application Firewall Rule or Relaxation."
   - To review learned exceptions or rules for a check, select the check, and then click Learned Violations. In the Manage Learned Rules dialog box, select each learned exception or rule in turn.
     - To edit the exception or rule, and then add it to the list, click Edit & Deploy.
     - To accept the exception or rule without modification, click Deploy.
     - To remove the exception or rule from the list, click Skip.
   - To refresh the list of exceptions or rules to be reviewed, click Refresh.
   - To open the Learning Visualizer and use it to review learned rules, click Visualizer.
   - To review the log entries for connections that matched a check, select the check, and then click Logs. You can use this information to determine which checks are matching attacks, so that you can enable blocking for those checks. You can also use this information to determine which checks are matching legitimate traffic, so that you can configure an appropriate exemption to allow those legitimate connections. For more information about the logs, see "Logs, Statistics, and Reports."
   - To completely disable a check, in the list, clear all of the check boxes to the right of that check.
4. On the Settings tab, configure the profile settings.

- To associate the profile with the set of signatures that you previously created and configured, under Common Settings, choose that set of signatures in the Signatures drop-down list.

  Note: You may need to use the scroll bar on the right of the dialog box to scroll down to display the Common Settings section.

- To configure an HTML or XML Error Object, select the object from the appropriate drop-down list.

  Note: You must first upload the error object that you want to use in the Imports pane. For more information about importing error objects, see "Imports."

- To configure the default XML Content Type, type the content type string directly into the Default Request and Default Response text boxes, or click Manage Allowed Content Types to manage the list of allowed content types. ">>More...."

5. If you want to use the learning feature, click Learning, and configure the learning settings for the profile, as described in "Configuring and Using the Learning Feature".

6. Click OK to save your changes and return to the Profiles pane.

Managing Content Types

Web servers usually add a Content-Type header that contains a MIME/type definition for the type of content in each file that the web server serves to users. Web servers serve many different types of content. For example, standard HTML is assigned the "text/html" MIME type. JPG images are assigned the "image/jpeg" or "image/jpg" content type. A normal web server can serve dozens or hundreds of different types of content, all defined in the Content Type header by an assigned MIME/type.

Many application firewall filtering rules are designed to filter specific types of content. Because filtering rules that apply to one type of content (such as HTML) are often inappropriate when filtering a different type of content (such as images), the application firewall attempts to determine the content type of requests and responses before it filters them. When a web server or browser does not add a Content-Type header to a request or response, the application firewall applies a default content type to the connection and filters the content accordingly.

The default content type is normally "application/octet-stream", the most generic MIME/type definition.This MIME/type is appropriate for any type of content that a web server is likely to serve, but also does not provide much information to the application firewall to allow it to choose appropriate filtering. If a protected web server on your network is configure to add accurate content type headers to the content it serves, or serves only one type of content, you can create a profile for that web server and assign a different default content type to it to improve both the speed and the accuracy of filtering.

You can also configure a list of allowed response content types for a specific profile. When this feature is configured, if the application firewall filters a response that does not match one of the allowed content types, it blocks the response.

Requests must always be of either the "application/x-www-form-urlencoded" or "multipart/form-data" types. The application firewall bypasses any request that has any other content type designated.

Note: You cannot include the "application/x-www-form-urlencoded" or "multipart/form-data" content types on the allowed response content types list.

To set the default request content type by using the command line interface

At the command prompt, type the following commands:

- set appfw profile <name> -requestContentType <type>
- save ns config

Example

The following example sets the "text/html" content type as the default for the specified profile:

```
set appfw profile profile1 -requestContentType "text/html"
save ns config
```

To remove the user-defined default request content type by using the command line interface

At the command prompt, type the following commands:

- unset appfw profile <name> -requestContentType <type>
- save ns config

Example

The following example unsets the default content type of "text/html" for the specified profile, allowing the type to revert to "application/octet-stream":

```
unset appfw profile profile1 -requestContentType "text/html"
save ns config
```

To set the default response content type by using the command line interface

At the command prompt, type the following commands:

- set appfw profile <name> -responseContentType <type>
- save ns config

Example

The following example sets the "text/html" content type as the default for the specified profile:

```
set appfw profile profile1 -responseContentType "text/html"
save ns config
```

To remove the user-defined default response content type by using the command line interface

At the command prompt, type the following commands:

- unset appfw profile <name> -responseContentType <type>
- save ns config

Example

The following example unsets the default content type of "text/html" for the specified profile, allowing the type to revert to "application/octet-stream":

```
unset appfw profile profile1 -responseContentType "text/html"
save ns config
```

To add a content type to the allowed content types list by using the command line interface

At the command prompt, type the following commands:

- bind appfw profile <name> -ContentType <contentTypeName>
- save ns config

Example

The following example adds the "text/shtml" content type to the allowed content types list for the specified profile:

```
bind appfw profile profile1 -contentType "text/shtml"
save ns config
```

To remove a content type from the allowed content types list by using the command line interface

At the command prompt, type the following commands:

- unbind appfw profile <name> -ContentType <contentTypeName>
- save ns config

Example

The following example removes the "text/shtml" content type from the allowed content types list for the specified profile:

```
unbind appfw profile profile1 -contentType "text/shtml"
save ns config
```

To manage the default and allowed content types by using the configuration utility

1. Navigate to Application Firewall > Profiles.
2. In the details pane, select the profile that you want to configure, and then click Open. The Configure Application Firewall Profile dialog box is displayed.
3. In the Configure Application Firewall Profile dialog box, click the Settings tab
4. On the Settings tab, scroll down about halfway to the Content Type area.
5. In the Content Type area, configure the default request or response content type:
   - To configure the default request content type, type the MIME/type definition of the content type you want to use in the Default Request text box.
   - To configure the default response content type, type the MIME/type definition of the content type you want to use in the Default Response text box.
   - To create a new allowed content type, click Add. The Add Allowed Content Type dialog box is displayed.
   - To edit an existing allowed content type, select that content type, and then click Open. The Modify Allowed Content Type dialog box is displayed.
6. To manage the allowed content types, click Manage Allowed Content Types.
7. To add a new content type or modify an existing content type, click Add or Open, and in the Add Allowed Content Type or Modify Allowed Content Type dialog box, do the following steps.
   a. Select/clear the Enabled check box to include the content type in, or exclude it from, the list of allowed content types.
   b. In the Content Type text box, type a regular expression that describes the content type that you want ot add, or change the existing content type regular expression.

      Content types are formatted exactly as MIME type descriptions are.

      Note: You can include any valid MIME type on the allowed contents type list. Since many types of document can contain active content and therefore could potentially contain malicious content, you should exercise caution when adding MIME types to this list.
   c. In the Comments text box, add an optional comment that describes the reason for adding this particular MIME type to the allowed contents type list.
   d. Click Create or OK to save your changes.
8. Click Close to close the Manage Allowed Content Types dialog box and return to the Settings tab.
9. To manage the content types for Safe Commerce, click Manage Content Types for Safe Commerce, fill out the Exclude Content Types from Inspection for Safe Commerce dialog box as described in the previous step and substeps, and then click Close. (The

dialog boxes are nearly identical.)

10. Click OK to save your changes.

Changing an Application Firewall Profile Type

If you chose the wrong profile type for an application firewall profile, or the type of content on the protected web site has changed, you can change the profile type.

Note: When you change the profile type, you lose all configuration settings and learned relaxations or rules for the features that the new profile type does not support. For example, if you change the profile type from Web 2.0 to XML, you lose any configuration options for Start URL, Form Field Consistency Check, and the other HTML-specific security checks. The configuration for any options that is supported by both the old and the new profile types remains unchanged.

To change an application firewall profile type by using the command line interface

At the command prompt, type the following commands:

- set appfw profile <name> -type (**HTML** | **XML** | **HTML XML**)
- save ns config

Example

The following example changes the type of a profile named `pr-basic`, from `HTML` to `HTML XML`, which is equivalent to the Web 2.0 type in the configuration utility.

```
set appfw profile pr-basic -type HTML XML
save ns config
```

To change an application firewall profile type by using the configuration utility.

1. In the navigation pane, expand Application Firewall, and then select Profiles.
2. In the details pane, click Change Profile Type.
3. In the Change Application Firewall Profile Type dialog box, Profile Type drop-down list, select a new profile type.
4. Click OK to save your changes and return to the Profiles pane.

Exporting and Importing an Application Firewall Profile

You can export application firewall profiles to your local computer as files, and import previously exported profile files. You might want to configure a single application firewall in a test bed configuration and then export the profile or profiles so that you can import the profile configuration to your production NetScaler appliances. You might also want to export a profile to back up your configuration before making changes so that you can easily roll the configuration back to a know state if necessary.

To export an application firewall profile by using the command line interface

At the command prompt, type the following command:

archive appfw profile <name> <archivename>

Example

Assuming that your local computer uses the Windows 7 operating system, and you are logged onto your local computer as "administrator", the following example exports a profile named `pr-basic` to the home directory.

```
archive appfw profile pr-basic "c:\users\administrator\pr-basic.tgz"
```

To export an application firewall profile by using the configuration utility

1. Navigate to Application Firewall > Profiles.
2. In the details pane, select a profile to export, and then click Export.
3. Choose the local path and filename for the exported file.
   - You can accept the default choice, which consists of the path to your home directory or folder and a filename of the profile name plus the extension `.tgz`, which indicates a Unix-style `tar` archive that is compressed by `gzip`.
   - You can type a new path and/or file name. The path must exist, and the filename must be a valid filename in your local computer's operating system. If you do not specify the `.tgz` extension, it is added automatically.
   - You can use the Browse dialog to locate the path and save the file under the default filename. (Recommended)
4. Click Export. The profile is exported and saved to your computer under the path and file name that you designated.

To import an application firewall profile by using the command line interface

At the command prompt, type the following command:

restore appfw profile <archivename>

Example

Assuming that your local computer uses the Windows 7 operating system, and you are logged onto your local computer as "administrator", the following example imports a profile named `pr-basic.tgz`, located in the home directory, to the application firewall and installs it as a profile named pr-basic.

restore appfw profile "c:\users\administrator\pr-basic.tgz"

To import an application firewall profile by using the configuration utility

1. Navigate to Application Firewall > Profiles.
2. In the details pane, click Import.
3. Choose the import type.
    - To import from a URL, accept the default selection, Import from URL.
    - To import a local file, select Import from Local File.
4. Specify the location of the profile to be imported.
    - You can type a URL, or a path and/or file name for the profile to be imported. The URL or path and filename must exist.
    - If you are importing a local file, you can use the Browse dialog to locate the path and filename of the profile to be imported. (Recommended)
5. Click Import. The profile is imported and appears in the Profiles pane.

Configuring and Using the Learning Feature

The learning feature is a repetitive pattern filter that observes activity on a web site or application protected by the application firewall, to determine what constitutes normal activity on that web site or application. It then generates a list of suggested rules or exceptions (*relaxations*) for those security checks that include support for the learning feature. Users normally find it easier to configure relaxations by using the learning feature than by entering the necessary relaxations manually.

You perform two different types of activities when using the learning feature. First, you enable and configure the feature to use it. Second, after the feature has been enabled and has processed a certain amount of traffic to your protected web sites, you review the list of suggested rules and relaxations (*learned rules*) and mark each with one of the following designations:

- **Edit & Deploy.** The rule is pulled into the Edit dialog box so that you can modify it, and the modified form is deployed.
- **Deploy.** The unmodified learned rule is placed on the list of rules or relaxations for this security check.
- **Skip.** The learned rule is placed on a list of rules or relaxations that are not deployed, and that should not be learned again.

Although you can use the command line interface for basic configuration of the learning feature, the feature is designed primarily for configuration through the Application Firewall wizard or the configuration utility. You can perform only limited configuration of the learning feature by using the command line.

The wizard integrates configuration of learning features with configuration of the application firewall as a whole, and is therefore the easiest method for configuring this feature on a new NetScaler appliance or when managing a simple application firewall configuration. The configuration utility visualizer and manual interface both provide direct access to all learned rules for all security checks, and are therefore often preferable when you must review learned rules for a large number of security checks.

The learning database is limited to 20 MB in size, which is reached after approximately 2,000 learned rules or relaxations are generated per security check for which learning is enabled. If you do not regularly review and either approve or ignore learned rules and this limit is reached, an error is logged to the NetScaler log and no more learned rules are generated until you review the existing learned rules and relaxations.

If learning stops because the database has reached its size limit, you can restart learning either by reviewing the existing learned rules and relaxations or by resetting the learning data. After learned rules or relaxations are approved or ignored, they are removed from the database. After you reset the learning data, all existing learning data is removed from the database and it is reset to its minimum size. When the database falls below 20 MB in size, learning restarts automatically.

To configure the learning settings by using the command line interface

Specify the application firewall profile to be configured and, for each security check that you want to include in that profile, specify the minimum threshold or the percent threshold. The minimum threshold is an integer representing the minimum number of user sessions that the application firewall must process before it learns a rule or relaxation (default: 1). The percent threshold is an integer representing the percentage of user sessions in which the application firewall must observe a particular pattern (URL, cookie, field, attachment, or rule violation) before it learns a rule or relaxation (default: 0). Use the following commands:

- set appfw learningsettings <profileName> [-startURLMinThreshold <positive_integer>] [-startURLPercentThreshold <positive_integer>] [-cookieConsistencyMinThreshold <positive_integer>] [-cookieConsistencyPercentThreshold <positive_integer>] [-CSRFtagMinThreshold <positive_integer>] [-CSRFtagPercentThreshold <positive_integer>] [-fieldConsistencyMinThreshold <positive_integer>] [-fieldConsistencyPercentThreshold <positive_integer>] [-crossSiteScriptingMinThreshold <positive_integer>] [-crossSiteScriptingPercentThreshold <positive_integer>] [-SQLInjectionMinThreshold <positive_integer>] [-SQLInjectionPercentThreshold <positive_integer>] [-fieldFormatMinThreshold <positive_integer>] [-fieldFormatPercentThreshold <positive_integer>] [-XMLWSIMinThreshold <positive_integer>] [-XMLWSIPercentThreshold <positive_integer>] [-XMLAttachmentMinThreshold <positive_integer>] [-XMLAttachmentPercentThreshold <positive_integer>]

- save ns config

Example

The following example enables and configures the learning settings in the profile pr-basic for the HTML SQL Injection security check. This is an appropriate initial test bed learning configuration, where you have complete control over the traffic that is sent to the application firewall.

```
set appfw learningsettings pr-basic -SQLInjectionMinThreshold 10
set appfw learningsettings pr-basic -SQLInjectionPercentThreshold 70
save ns config
```

To reset learning settings to their defaults by using the command line interface

To remove any custom configuration of the learning settings for the specified profile and security check, and return the learning settings to their defaults, at the command prompt type the following commands:

- unset appfw learningsettings <profileName> [-startURLMinThreshold] [-startURLPercentThreshold] [-cookieConsistencyMinThreshold] [-cookieConsistencyPercentThreshold] [-CSRFtagMinThreshold]

[-CSRFtagPercentThreshold] [-fieldConsistencyMinThreshold]
[-fieldConsistencyPercentThreshold] [-crossSiteScriptingMinThreshold]
[-crossSiteScriptingPercentThreshold] [-SQLInjectionMinThreshold]
[-SQLInjectionPercentThreshold] [-fieldFormatMinThreshold]
[-fieldFormatPercentThreshold] [-XMLWSIMinThreshold] [-XMLWSIPercentThreshold]
[-XMLAttachmentMinThreshold] [-XMLAttachmentPercentThreshold]

- save ns config

To display the learning settings for a profile by using the command line interface

At the command prompt, type the following command:

show appfw learningsettings <profileName>

To display unreviewed learned rules or relaxations for a profile by using the command line interface

At the command prompt, type the following command:

show appfw learningdata <profileName> <securityCheck>

To remove specific unreviewed learned rules or relaxations from the learning database by using the command line interface

At the command prompt, type the following command:

rm appfw learningdata <profileName> (-startURL <expression> | -cookieConsistency <string> | (-fieldConsistency <string> <formActionURL>) | (-crossSiteScripting <string> <formActionURL>) | (-SQLInjection <string> <formActionURL>) | (-fieldFormat <string> <formActionURL>) | (-CSRFTag <expression> <CSRFFormOriginURL>) | -XMLDoSCheck <expression> | -XMLWSICheck <expression> | -XMLAttachmentCheck <expression>) [-TotalXMLRequests]

Example

The following example removes all unreviewed learned relaxations for the pr-basic profile, HTML SQL Injection security check, that apply to the LastName form field.

rm appfw learningdata pr-basic -SQLInjection LastName

To remove all unreviewed learned data by using the command line interface

At the command prompt, type the following command:

reset appfw learningdata

To export learning data by using the command line interface

At the command prompt, type the following command:

export appfw learningdata <profileName> <securitycheck> [-target <string>]

Example

The following example exports learned relaxations for the `pr-basic` profile and the HTML SQL Injection security check to a comma-separated values (CSV) format file in the `/var/learnt_data/` directory under the filename specified in the `-target` parameter.

export appfw learningdata pr-basic SQLInjection -target sqli_ld

To configure the Learning feature by using the configuration utility

1. In the navigation pane, expand Application Firewall, and then select Profiles.
2. In the Profiles pane, select the profile, and then click Open.
3. Click the Learning tab. At the top of the Learning tab is list of the security checks that are available in the current profile and that support the learning feature.
4. To configure the learning thresholds, select a security check, and then type the appropriate values in the following text boxes:
   - **Minimum number threshold.** Depending on which security check's learning settings you are configuring, the minimum number threshold might refer to the minimum number of total user sessions that must be observed, the minimum number of requests that must be observed, or the minimum number of times a specific form field must be observed, before a learned relaxation is generated. Default: 1
   - **Percentage of times threshold.** Depending on which security check's learning settings you are configuring, the percentage of times threshold might refer to the percentage of total observed user sessions that violated the security check, the percentage of requests, or the percentage of times a form field matched a particular field type, before a learned relaxation is generated. Default: 0
5. To remove all learned data and reset the learning feature, so that it must start its observations again from the beginning, click Remove All Learned Data.

   Note: This button removes only learned recommendations that have not been reviewed and either approved or skipped. It does not remove learned relaxations that have been accepted and deployed.
6. Click Close to return to the Configure Application Firewall Profile dialog box.
7. Click Close to close the Configure Application Firewall Profile dialog box, and return to the Application Firewall Profile screen.

To review learned rules or relaxations by using the configuration utility

1. In the navigation pane, expand Application Firewall, and then select Profiles.
2. Select the security check for which you want to review learned rules or relaxations, and then click Manage Rules.
3. In the Manage Learned Rules dialog box, choose how you want to review the learned rules.
   - To review the actual learned patterns as displayed in the window, do nothing and proceed to the next step.
   - To review the learned data hierarchically as a branching tree, enabling you to choose general patterns that match many of the learned patterns, click Visualizer.
4. If you have chosen to review actual learned patterns, perform the following steps.
   a. Select the first learned relaxation and choose how to handle it.
      - To modify and then accept the relaxation, click Edit & Deploy, edit the relaxation regular expression, and then click OK.
      - To accept the relaxation without modifications, click Deploy.
      - To remove the relaxation from the list without deploying it, click Skip.
   b. Repeat the previous step to review each additional learned relaxation.
5. If you have chosen to use the Learning Visualizer, perform the following steps.
   a. In the branching hierarchical display, select a node that contains a learned pattern, and choose how to handle it.

      The screen area beneath the tree structure, under Regex of Selected Node, displays a generalized expression that matches all of the patterns in that node. If you want to display an expression that matches just one of the branches or just one of the leaves, select that branch or leaf.

      - To modify and then accept the learned relaxation, click Edit & Deploy, edit the relaxation regular expression, and then click OK.
      - To accept the relaxation without modifications, click Deploy.
      - To remove the modification from the list without deploying it, click Skip.
   b. Repeat the previous step to review other portions of the display.
   c. Click Close to return to the Manage Learned Rules dialog box.
6. Click Close to return to the Configure Application Firewall Profile dialog box.
7. Click Close to close the Configure Application Firewall Profile dialog box, and return to the Application Firewall Profile screen.

Supplemental Information about Profiles

Following is supplemental information about particular aspects of application firewall profiles. This information explains how to include special characters in a security check rule or relaxation, and how to use variables when configuring profiles.

Configuration Variable Support

Instead of using static values, to configure the application firewall's security checks and settings, you can now use standard NetScaler named variables. By creating variables, you can more easily export and then import configurations to new NetScaler appliances, or update existing NetScaler appliances from a single set of configuration files. This simplifies updates when you use a test bed setup to develop a complex application firewall configuration that is tuned for your local network and servers and then transfer that configuration to your production NetScaler appliances.

You create application firewall configuration variables in the same manner as you do any other NetScaler named variables, following standard NetScaler conventions. To create a named expression variable by using the configuration utility, you use the "Add Expression dialog box." To create a named expression variable by using the NetScaler command line, you use the `add expression` command followed by the appropriate parameter.

The following URLs and expressions can be configured with variables instead of static values:

- **Start URL** (-starturl)
- **Deny URL** (-denyurl)
- **Form Action URL** for *Form Field Consistency Check* (-fieldconsistency)
- **Action URL** for *XML SQL Injection Check* (-xmlSQLInjection)
- **Action URL** for *XML Cross-Site Scripting Check* (-xmlXSS)
- **Form Action URL** for *HTML SQL Injection Check* (-sqlInjection)
- **Form Action URL** for *Field Format Check* (-fieldFormat)
- **Form Origin URL** and **Form Action URL** for *Cross-Site Request Forgery (CSRF) Check* (-csrfTag)
- **Form Action URL** for *HTML Cross-Site Scripting Check* (-crossSiteScripting)
- **Safe Object** (-safeObject)
- **Action URL** for *XML Denial-of-Service (XDoS) check* (-XMLDoS)
- **URL** for *Web Services Interoperability check* (-XMLWSIURL)

- **URL** for *XML Validation check* (-XMLValidationURL)
- **URL** for *XML Attachment check* (-XMLAttachmentURL)

For more information, see "Policies and Expressions."

To use a variable in the configuration, you enclose the variable name between two at (@) symbols and then use it exactly as you would the static value that it replaces. For example, if you are configuring the Deny URL check by using the configuration utility and want to add the named expression variable myDenyURL to the configuration, you would type `@myDenyURL@` into the Add Deny URL dialog box, Deny URL text area. To do the same task by using the NetScaler command line, you would type `add appfw profile <name> -denyURLAction @myDenyURL@`.

PCRE Character Encoding Format

The NetScaler operating system supports direct entry of characters in the printable ASCII character set only—characters with hexadecimal codes between HEX 20 (ASCII 32) and HEX 7E (ASCII 127). To include a character with a code outside that range in your application firewall configuration, you must enter its UTF-8 hexadecimal code as a PCRE regular expression.

A number of character types require encoding using a PCRE regular expression if you include them in your application firewall configuration as a URL, form field name, or Safe Object expression. They include:

- **Upper-ASCII characters.** Characters with encodings from HEX 7F (ASCII 128) to HEX FF (ASCII 255). Depending on the character map used, these encodings can refer to control codes, ASCII characters with accents or other modifications, non-Latin alphabet characters, and symbols not included in the basic ASCII set. These characters can appear in URLs, form field names, and safe object expressions.
- **Double-Byte characters.** Characters with encodings that use two 8-byte words. Double-byte characters are used primarily for representing Chinese, Japanese, and Korean text in electronic format. These characters can appear in URLs, form field names, and safe object expressions.
- **ASCII control characters.** Non-printable characters used to send commands to a printer. All ASCII characters with hexadecimal codes less than HEX 20 (ASCII 32) fall into this category. These characters should never appear in a URL or form field name, however, and would rarely if ever appear in a safe object expression.

The NetScaler appliance does not support the entire UTF-8 character set, but only the characters found in the following eight charsets:

- **English US (ISO-8859-1).** Although the label reads, “English US,” the application firewall supports all characters in the ISO-8859-1 character set, also called the Latin-1 character set. This character set fully represents most modern western European languages and represents all but a few uncommon characters in the rest.
- **Chinese Traditional (Big5).** The application firewall supports all characters in the BIG5 character set, which includes all of the Traditional Chinese characters (ideographs) commonly used in modern Chinese as spoken and written in Hong Kong, Macau, Taiwan, and by many people of Chinese ethnic heritage who live outside of mainland China.

- **Chinese Simplified (GB2312).** The application firewall supports all characters in the GB2312 character set, which includes all of the Simplified Chinese characters (ideographs) commonly used in modern Chinese as spoken and written in mainland China.

- **Japanese (SJIS).** The application firewall supports all characters in the Shift-JIS (SJIS) character set, which includes most characters (ideographs) commonly used in modern Japanese.

- **Japanese (EUC-JP).** The application firewall supports all characters in the EUC-JP character set, which includes all characters (ideographs) commonly used in modern Japanese.

- **Korean (EUC-KR).** The application firewall supports all characters in the EUC-KR character set, which includes all characters (ideographs) commonly used in modern Korean.

- **Turkish (ISO-8859-9).** The application firewall supports all characters in the ISO-8859-9 character set, which includes all letters used in modern Turkish.

- **Unicode (UTF-8).** The application firewall supports certain additional characters in the UTF-8 character set, including those used in modern Russian.

When configuring the application firewall, you enter all non-ASCII characters as PCRE-format regular expressions using the hexadecimal code assigned to that character in the UTF-8 specification. Symbols and characters within the normal ASCII character set, which are assigned single, two-digit codes in that character set, are assigned the same codes in the UTF-8 character set. For example, the exclamation point (!), which is assigned hex code 21 in the ASCII character set, is also hex 21 in the UTF-8 character set. Symbols and characters from another supported character set have a paired set of hexadecimal codes assigned to them in the UTF-8 character set. For example, the letter a with an acute accent (á) is assigned UTF-8 code C3 A1.

The syntax you use to represent these UTF-8 codes in the application firewall configuration is “\xNN” for ASCII characters; “\xNN\xNN” for non-ASCII characters used in English, Russian, and Turkish; and “\xNN\xNN\xNN” for characters used in Chinese, Japanese, and Korean. For example, if you want to represent a ! in an application firewall regular expression as a UTF-8 character, you would type \x21. If you want to include an á, you would type \xC3\xA1.

Note: Normally you do not need to represent ASCII characters in UTF-8 format, but when those characters might confuse a web browser or an underlying operating system, you can use the character’s UTF-8 representation to avoid this confusion. For example, if a URL contains a space, you might want to encode the space as \x20 to avoid confusing certain browsers and web server software.

Below are examples of URLs, form field names, and safe object expressions that contain non-ASCII characters that must be entered as PCRE-format regular expressions to be included in the application firewall configuration. Each example shows the actual URL, field name, or expression string first, followed by a PCRE-format regular expression for it.

- A URL containing extended ASCII characters.

  Actual URL: `http://www.josénuñez.com`

  Encoded URL: `^http://www[.]jos\xC3\xA9nu\xC3\xB1ez[.]com$`

- Another URL containing extended ASCII characters.

  Actual URL: `http://www.example.de/trömso.html`

  Encoded URL: `^http://www[.]example[.]de/tr\xC3\xB6mso[.]html$`

- A form field name containing extended ASCII characters.

  Actual Name: `nome_do_usuário`

  Encoded Name: `^nome_do_usu\xC3\xA1rio$`

- A safe object expression containing extended ASCII characters.

  Unencoded Expression `[A-Z]{3,6}¥[1-9][0-9]{6,6}`

  Encoded Expression: `[A-Z]{3,6}\xC2\xA5[1-9][0-9]{6,6}`

You can find a number of tables that include the entire Unicode character set and matching UTF-8 encodings on the Internet. A useful web site that contains this information is located at the following URL:

http://www.utf8-chartable.de/unicode-utf8-table.pl

For the characters in the table on this web site to display correctly, you must have an appropriate Unicode font installed on your computer. If you do not, the visual display of the character may be in error. Even if you do not have an appropriate font installed to display a character, however, the description and the UTF-8 and UTF-16 codes on this set of web pages will be correct.

Inverted PCRE Expressions

In addition to matching content that contains a pattern, you can match content that does not contain a pattern by using an inverted PCRE expression. To invert an expression, you simply include an exclamation point (!) followed by white space as the first character in the expression.

Note: If an expression consists only of an exclamation point with nothing following, the exclamation point is treated as a literal character, not syntax indicating an inverted expression.

The following application firewall commands support inverted PCRE expressions:

- Start URL (URL)
- Deny URL (URL)
- Form Field Consistency (form action URL)
- Cookie Consistency (form action URL)
- Cross Site Request Forgery (CSRF) (form action URL)
- HTML Cross-site Scripting (form action URL)

- Field Format (form action URL)
- Field Type (type)
- Confidential Field (URL)

Note: If the security check contains an isRegex flag or check box, it must be set to YES or checked to enable regular expressions in the field. Otherwise the contents of that field are treated as literal and no regular expressions (inverted or not) are parsed.

Disallowed Names for Application Firewall Profiles

The following names are assigned to built-in actions and profiles on the NetScaler appliance, and cannot be used as names for a user-created application firewall profile.

- AGRESSIVE
- ALLOW
- BASIC
- CLIENTAUTH
- COMPRESS
- CSSMINIFY
- DEFLATE
- DENY
- DNS-NOP
- DROP
- GZIP
- HTMLMINIFY
- IMGOPTIMIZE
- JSMINIFY
- MODERATE
- NOCLIENTAUTH
- NOCOMPRESS
- NONE
- NOOP
- NOREWRITE

- RESET
- SETASLEARNNSLOG_ACT
- SETNSLOGPARAMS_ACT
- SETSYSLOGPARAMS_ACT
- SETTMSESSPARAMS_ACT
- SETVPNPARAMS_ACT
- SET_PREAUTHPARAMS_ACT
- default_DNS64_action
- dns_default_act_Cachebypass
- dns_default_act_Drop
- nshttp_default_profile
- nshttp_default_strict_validation
- nstcp_default_Mobile_profile
- nstcp_default_XA_XD_profile
- nstcp_default_profile
- nstcp_default_tcp_interactive_stream
- nstcp_default_tcp_lan
- nstcp_default_tcp_lan_thin_stream
- nstcp_default_tcp_lfp
- nstcp_default_tcp_lfp_thin_stream
- nstcp_default_tcp_lnp
- nstcp_default_tcp_lnp_thin_stream
- nstcp_internal_apps

Policies

The application firewall uses two types of policies: firewall policies and auditing policies. Firewall policies control which traffic is sent to the application firewall. Auditing policies control the log server to which application firewall logs are sent.

Firewall policies can be complex because the policy rule can consist of multiple expressions in the NetScaler expressions language, which is a full-fledged object oriented programming language capable of defining with extreme precision exactly which connections to filter. Because firewall policies operate within the context of the application firewall, they must meet certain criteria that are connected to how the application firewall functions and what traffic is appropriately filtered by it. As long as you keep these criteria in mind, however, firewall policies are similar to policies for other NetScaler features. The instructions here do not attempt to cover all aspects of writing firewall policies, but only provide an introduction to policies and cover those criteria that are unique to the application firewall.

Auditing policies are simple because the policy rule is always `ns_true`. You need only specify the log server that you want to send logs to, the logging levels that you want to use, and a few other criteria that are explained in detail.

Firewall Policies

A firewall policy is a rule associated with a profile. The rule is an expression or group of expressions that defines the types of request/response pairs that the application firewall is to filter by applying the profile. Firewall policy expressions are written in the NetScaler expressions language, an object-oriented programming language with special features to support specific NetScaler functions. The profile is the set of actions that the application firewall is to use to filter request/response pairs that match the rule.

Firewall policies enable you to assign different filtering rules to different types of web content. Not all web content is alike. A simple web site that uses no complex scripting and accesses and handles no private data might require only the level of protection provided by a profile created with basic defaults. Web content that contains JavaScript-enhanced web forms or accesses an SQL database probably requires more tailored protection. You can create a different profile to filter that content, and create a separate firewall policy that can determine which requests are attempting to access that content. You then associate the policy expression with a profile you created and globally bind the policy to put it into effect.

The application firewall processes only HTTP connections, and therefore uses a subset of the overall NetScaler expressions language. The information here is limited to topics and examples that are likely to be useful when configuring the application firewall. Following are links to additional information and procedures for firewall policies:

- For procedures that explain how to create and configure a policy, see "Creating and Configuring Application Firewall Policies."
- For a procedure that explains in detail how to create a policy rule (expression), see "To create or configure an Application Firewall rule (expression)."
- For a procedure that explains how to use the Add Expression dialog box to create a policy rule, see "To add a firewall rule (expression) by using the Add Expression dialog box."
- For a procedure that explains how to view the current bindings for a policy, see "Viewing a Firewall Policy's Bindings."
- For procedures that explain how to bind an application firewall policy, see "Binding Application Firewall Policies."
- For detailed information about the NetScaler expressions language, see "Policies and Expressions."

Creating and Configuring Application Firewall Policies

A firewall policy consists of two elements: a *rule*, and an associated *profile*. The rule selects the HTTP traffic that matches the criteria that you set, and sends that traffic to the application firewall for filtering. The profile contains the filtering criteria that the application firewall uses.

The policy rule consists of one or more expressions in the NetScaler expressions language. The NetScaler expressions syntax is a powerful, object-oriented programming language that enables you to precisely designate the traffic that you want to process with a specific profile. For users who are not completely familiar with the NetScaler expressions language syntax, or who prefer to configure their NetScaler appliance by using a web-based interface, the configuration utility provides two tools: the Prefix menu and the Add Expression dialog box. Both help you to write expressions that select exactly the traffic that you want to process. Experienced users who are thoroughly familiar with the syntax may prefer to use the NetScaler command line to configure their NetScaler appliances.

Note: In addition to the default expressions syntax, for backward compatibility the NetScaler operating system supports the NetScaler classic expressions syntax on NetScaler Classic and nCore appliances and virtual appliances. Classic expressions are not supported on NetScaler Cluster appliances and virtual appliances. Current NetScaler users who want to migrate existing configurations to the NetScaler Cluster must migrate any policies that contain classic expressions to the default expressions syntax.

For detailed information about the NetScaler expressions languages, see "Policies and Expressions."

You can create a firewall policy by using the configuration utility or the NetScaler command line.

To create and configure a policy by using the command line interface

At the command prompt, type the following commands:

- add appfw policy <name> <rule> <profileName>
- save ns config

Example

The following example adds a policy named `pl-blog`, with a rule that intercepts all traffic to or from the host `blog.example.com`, and associates that policy with the profile `pr-blog`. This is an appropriate policy to protect a blog hosted on a specific hostname.

```
add appfw policy pl-blog "HTTP.REQ.HOSTNAME.DOMAIN.EQ("blog.example.com")" pr-blog
```

Parameters for Creating and Configuring Firewall Policies

name

A name for your policy. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 128 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols.

rule

A policy rule, or expression, in NetScaler expressions language. For a short description and some useful examples of Application Firewall rules. For a complete description of the NetScaler expressions language, see "Introduction to Policies and Expressions."

profile

The name of the profile that you previously created.

To create and configure a policy by using the configuration utility

1. Navigate to Application Firewall > Policies.
2. In the details pane, do one of the following:
   - To create a new firewall policy, click Add. The Create Application Firewall Policy is displayed.
   - To edit an existing firewall policy, select the policy, and then click Open. The Configure Application Firewall Policy is displayed.
3. If you are creating a new firewall policy, in the Create Application Firewall Policy dialog box, Policy Name text box, type a name for your new policy.

   The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 128 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) symbols.

   If you are configuring an existing firewall policy, this field is read-only. You cannot modify it.
4. Select the profile that you want to associate with this policy from the Profile drop-down list. You can create a new profile to associate with your policy by clicking New, and you can modify an existing profile by clicking Modify.
5. In the Expression text area, create a rule for your policy.
   - You can type a rule directly into the text area.
   - You can click Prefix to select the first term for your rule, and follow the prompts. See "To Create an Application Firewall Rule (Expression)" for a complete description of this process.
   - You can click Add to open the Add Expression dialog box, and use it to construct the rule. See "The Add Expression Dialog Box" for a complete description of this process.
6. Click Create or OK, and then click Close.

To create or configure an Application Firewall rule (expression)

The policy rule, also called the *expression*, defines the web traffic that the application firewall filters by using the profile associated with the policy. Like other NetScaler policy rules (or *expressions*), application firewall rules use NetScaler expressions syntax. This syntax is powerful, flexible, and extensible. It is too complex to describe completely in this set of instructions. You can use the following procedure to create a simple firewall policy rule, or you can read it as an overview of the policy creation process.

1. If you have not already done so, navigate to the appropriate location in the Application Firewall wizard or the NetScaler configuration utility to create your policy rule:

- If you are configuring a policy in the Application Firewall wizard, in the navigation pane, click Application Firewall, then in the details pane click Application Firewall Wizard, and then navigate to the Specify Rule screen.

- If you are configuring a policy manually, in the navigation pane, expand Application Firewall, then Policies, and then Firewall. In the details pane, to create a new policy, click Add. To modify an existing policy, select the policy, and then click Open.

2. On the Specify Rule screen, the Create Application Firewall Profile dialog box, or the Configure Application Firewall Profile dialog box, click Prefix, and then choose the prefix for your expression from the drop-down list. Your choices are:

   - **HTTP.** The HTTP protocol. Choose this if you want to examine some aspect of the request that pertains to the HTTP protocol.

   - **SYS.** The protected Web site(s). Choose this if you want to examine some aspect of the request that pertains to the recipient of the request.

   - **CLIENT.** The computer that sent the request. Choose this if you want to examine some aspect of the sender of the request.

   - **SERVER.** The computer to which the request was sent. Choose this if you want to examine some aspect of the recipient of the request.

   After you choose a prefix, the application firewall displays a two-part prompt window that displays the possible next choices at the top, and a brief explanation of what the selected choice means at the bottom.

3. Choose your next term.

   If you chose HTTP as your prefix, your only choice is REQ, which specifies the Request/Response pair. (The application firewall operates on the request and response as a unit instead of on each separately.) If you chose another prefix, your choices are more varied. For help on a specific choice, click that choice once to display information about it in the lower prompt window.

   When you have decided which term you want, double-click it to insert it into the Expression window.

4. Type a period after the term you just chose. You are then prompted to choose your next term, as described in the previous step. When a term requires that you type a value, fill in the appropriate value. For example, if you choose `HTTP.REQ.HEADER("")`, type the header name between the quotation marks.

5. Continue choosing terms from the prompts and filling in any values that are needed, until your expression is finished.

   Following are some examples of expressions for specific purposes.

   - **Specific web host.** To match traffic from a particular web host:

     ```
     HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
     ```

     For `shopping.example.com`, substitute the name of the web host that you want to match.

- **Specific web folder or directory.** To match traffic from a particular folder or directory on a Web host:

  HTTP.REQ.URL.STARTSWITH("https//www.example.com/folder")

  For `www.example.com`, substitute the name of the web host. For `folder`, substitute the folder or path to the content that you want to match. For example, if your shopping cart is in a folder called `/solutions/orders`, you substitute that string for folder.

- **Specific type of content: GIF images.** To match GIF format images:

  HTTP.REQ.URL.ENDSWITH(".gif")

  To match other format images, substitute another string in place of `.gif`.

- **Specific type of content: scripts.** To match all CGI scripts located in the `CGI-BIN` directory:

  HTTP.REQ.URL.STARTSWITH("https//www.example.com/CGI-BIN")

  To match all JavaScripts with `.js` extensions:

  HTTP.REQ.URL.ENDSWITH(".js")

  For more information about creating policy expressions, see "Policies and Expressions."

Note: If you use the command line to configure a policy, remember to escape any double quotation marks within NetScaler expressions. For example, the following expression is correct if entered in the configuration utility:

HTTP.REQ.HEADER("Host").EQ("shopping.example.com")

If entered at the command line, however, you must type this instead:

HTTP.REQ.HEADER(\"Host\").EQ(\"shopping.example.com\")

To add a firewall rule (expression) by using the Add Expression dialog box

The Add Expression dialog box (also referred to as the *Expression Editor*) helps users who are not familiar with the NetScaler expressions language to construct a policy that matches the traffic that they want to filter.

1. If you have not already done so, navigate to the appropriate location in the Application Firewall wizard or the NetScaler configuration utility:

- If you are configuring a policy in the Application Firewall wizard, in the navigation pane, click Application Firewall, then in the details pane click Application Firewall Wizard, and then navigate to the Specify Rule screen.

- If you are configuring a policy manually, in the navigation pane, expand Application Firewall, then Policies, and then Firewall. In the details pane, to create a new policy, click Add. To modify an existing policy, select the policy, and then click Open.

2. On the Specify Rule screen, in the Create Application Firewall Profile dialog box, or in the Configure Application Firewall Profile dialog box, click Add.

3. In the Add Expression dialog box, in the Construct Expression area, in the first list box, choose one of the following prefixes:

   - **HTTP.** The HTTP protocol. Choose this if you want to examine some aspect of the request that pertains to the HTTP protocol. The default choice.

   - **SYS.** The protected Web site(s). Choose this if you want to examine some aspect of the request that pertains to the recipient of the request.

   - **CLIENT.** The computer that sent the request. Choose this if you want to examine some aspect of the sender of the request.

   - **SERVER.** The computer to which the request was sent. Choose this if you want to examine some aspect of the recipient of the request.

4. In the second list box, choose your next term. The available terms differ depending on the choice you made in the previous step, because the dialog box automatically adjusts the list to contain only those terms that are valid for the context. For example, if you selected HTTP in the previous list box, the only choice is REQ, for requests. Because the application firewall treats requests and associated responses as a single unit and filters both, you do not need to specific responses separately. After you choose your second term, a third list box appears to the right of the second. The Help window displays a description of the second term, and the Preview Expression window displays your expression.

5. In the third list box, choose the next term. A new list box appears to the right, and the Help window changes to display a description of the new term. The Preview Expression window updates to display the expression as you have specified it to that point.

6. Continue choosing terms, and when prompted filling in arguments, until your expression is complete. If you make a mistake or want to change your expression after you have already selected a term, you can simply choose another term. The expression is modified, and any arguments or additional terms that you added after the term that you modified are cleared.

7. When you have finished constructing your expression, click OK to close the Add Expression dialog box. Your expression is inserted into the Expression text area.

Binding Application Firewall Policies

After you have configured your application firewall policies, you bind them to Global or a bind point to put them into effect. After binding, any request or response that matches an application firewall policy is transformed by the profile associated with that policy.

When you bind a policy, you assign a priority to it. The priority determines the order in which the policies you define are evaluated. You can set the priority to any positive integer. In the NetScaler OS, policy priorities work in reverse order - the higher the number, the lower the priority.

Because the application firewall feature implements only the first policy that a request matches, not any additional policies that it might also match, policy priority is important for achieving the results that you intend. If you give your first policy a low priority (such as 1000), you configure the application firewall to perform it only if other policies with a higher priority do not match a request. If you give your first policy a high priority (such as 1), you configure the application firewall to perform it first, and skip any other policies that might also match. You can leave yourself plenty of room to add other policies in any order, without having to reassign priorities, by setting priorities with intervals of 50 or 100 between each policy when you bind your policies.

For more information about binding policies on the NetScaler appliance, see "Policies and Expressions."

To bind an application firewall policy by using the command line interface

At the command prompt, type the following commands:

- bind appfw global <policyName> <priority>
- save ns config

Example

The following example binds the policy named `pl-blog` and assigns it a priority of `10`.

```
bind appfw global pl-blog 10
save ns config
```

Parameters for Binding Application Firewall Policies

policyName

The name of the application firewall policy you want to bind.

priority

The priority assigned to this application firewall policy. The priority determines the order in which policies are evaluated, allowing the NetScaler to evaluate the most specific policy first, and more general policies in descending order, finishing with the most general policy.

To bind an application firewall policy by using the configuration utility

1. In the navigation pane, expand Application Firewall, then Policies, and then select Firewall Policies.

2. In the details pane, click Policy Manager.

3. In the Application Firewall Policy Manager dialog box, choose the bind point to which you want to bind the policy. The choices are:

   - **Override Global.** Policies that are bound to this bind point process all traffic from all interfaces on the NetScaler appliance, and are applied before any other policies.

   - **LB Virtual Server.** Policies that are bound to a load balancing virtual server are applied only to traffic that is processed by that load balancing virtual server, and are applied before any Default Global policies. After selecting LB Virtual Server, you must also select the specific load balancing virtual server to which you want to bind this policy.

   - **CS Virtual Server.** Policies that are bound to a content switching virtual server are applied only to traffic that is processed by that content switching virtual server, and are applied before any Default Global policies. After selecting CS Virtual Server, you must also select the specific content switching virtual server to which you want to bind this policy.

   - **Default Global.** Policies that are bound to this bind point process all traffic from all interfaces on the NetScaler appliance.

   - **Policy Label.** Policies that are bound to a policy label process traffic that the policy label routes to them. The policy label controls the order in which policies are applied to this traffic.
4. Select Insert Policy to insert a new row and display a drop-down list with all available, unbound application firewall policies.

5. Select the policy you want to bind, or select New Policy to create a new policy. The policy that you selected or created is inserted into the list of globally bound application firewall policies.

6. Make any additional adjustments to the binding.

   - To modify the policy priority, click the field to enable it, and then type a new priority. You can also select Regenerate Priorities to renumber the priorities evenly.

   - To modify the policy expression, double click that field to open the Configure Application Firewall Policy dialog box, where you can edit the policy expression.

   - To set the Goto Expression, double click field in the Goto Expression column heading to display the drop-down list, where you can choose an expression.

   - To set the Invoke option, double click field in the Invoke column heading to display the drop-down list, where you can choose an expression
7. Repeat steps 3 through 6 to add any additional application firewall policies you want to globally bind.

8. Click OK. A message appears in the status bar, stating that the policy has been successfully bound.

Viewing a Firewall Policy's Bindings

You can quickly check to determine what bindings are in place for any firewall policy by viewing the bindings in the configuration utility.

To view bindings for an application firewall policy

1. In the navigation pane, expand Application Firewall, then Policies, and then select Firewall Policies.
2. In the details pane, select the policy that you want to check, and then click Show Bindings. The Binding Details for Policy: Policy message box is displayed, with a list of bindings for the selected policy.
3. Click Close.

Auditing Policies

Auditing policies determine the messages that are generated and logged during an Application Firewall session. These messages are logged in SYSLOG format to the local NSLOG server or to an external logging server. Different types of messages are logged on the basis of the level of logging selected.

To create an auditing policy, you must first create either an NSLOG server or a SYSLOG server. After specifying the server, you create the policy and specify the type of log and the server to which logs are sent.

To create an auditing server by using the command line interface

You can create two different types of auditing server: an NSLOG server or a SYSLOG server. The command names are different, but the parameters for the commands are the same.

To create an auditing server, at the NetScaler command prompt, type the following commands:

- add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> ... [-dateFormat (**MMDDYYYY** | **DDMMYYYY**)] [-logFacility <logFacility>] [-tcp (**NONE** | **ALL**)] [-acl (**ENABLED** | **DISABLED**)] [-timeZone (**GMT_TIME** | **LOCAL_TIME**)] [-userDefinedAuditlog (**YES** | **NO**)] [-appflowExport (**ENABLED** | **DISABLED**)]
- save ns config

Example

The following example creates a syslog server named syslog1 at IP 10.124.67.91, with loglevels of emergency, critical, and warning, log facility set to LOCAL1, that logs all TCP connections:

```
add audit syslogAction syslog1 10.124.67.91 -logLevel emergency critical warning -logFacility LOCAL1 -tcp ALL
save ns config
```

To modify or remove an auditing server by using the command line interface

- To modify an auditing server, type the set audit <type> command, the name of the auditing server, and the parameters to be changed, with their new values.
- To remove an auditing server, type the rm audit <type> command and the name of the auditing server.

Example

The following example modifies the syslog server named syslog1 to add errors and alerts to the log level:

```
set audit syslogAction syslog1 10.124.67.91 -logLevel emergency critical warning alert error
-logFacility LOCAL1 -tcp ALL
save ns config
```

Parameters for configuring an auditing server

type (Auditing Type)

The type of logging server you are configuring. Possible values: nslogAction (NSLOG), syslogAction (SYSLOG).

name (Name)

A name for the syslog server. The name can consist of from one to 31 upper-case and lower-case letters, numbers, and the period (.), underscore (_) and hyphen (-) symbols.

serverIP (IP Address)

The IP address of the server, in IPV4 or IPV6 format.

serverPort (Port)

The port number on which the server listens for connections.

logLevel (Log Levels)

The types of information to be logged to the server. The choices are:

- ALERT
- CRITICAL
- DEBUG
- EMERGENCY

- ERROR
- INFORMATIONAL
- NOTICE
- WARNING

dateFormat (Date format)

The format used for dates in the logs. The choices are MMDDYYYY (U.S. style) or DDMMYYYY (International style).

logFacility (Log Facility)

The log facility on the NetScaler appliance. Possible values: LOCAL0, LOCAL1, LOCAL2.

tcp (TCP Logging)

Enable logging of TCP connections. Possible values: NONE, ALL.

acl (ACL Logging)

Enable logging of ACL connections. Possible values: ENABLED, DISABLED.

timeZone (Time Zone)

The Unix time zone to use in the logs.

userDefinedAuditLog (User Configurable Log Messages)

Enable user configurable log messages. Possible values: YES, NO.

appflowExport (AppFlow Logging)

Enable export of logs to the NetScaler AppFlow feature. Possible values: ENABLED, DISABLED.

Example

The following example creates a syslog server named syslog1 at IP 10.124.67.91, with loglevels of emergency, critical, and warning, log facility set to LOCAL1, that logs all TCP connections:

```
add audit syslogAction syslog1 10.124.67.91 -logLevel emergency critical warning
-logFacility LOCAL1 -tcp ALL
save ns config
```

To create or configure an auditing server by using the configuration utility

1. Navigate to Application Firewall > Policies > Auditing.
2. In the details pane, click the Server tab.
3. Do one of the following:
   - To add a new auditing server, click Add.
   - To modify an existing auditing server, select the server, and then click Open.
4. In the Create Auditing Server or Configure Auditing Server dialog box, set the following parameters:
   - Name
   - Auditing Type
   - IP Address
   - Port
   - Log Levels
   - Log Facility
   - TCP Logging
   - ACL Logging
   - User-Configurable Log Messages
   - AppFlow Logging
   - Date Format
   - Time Zone
5. Click Create or OK.

To create an auditing policy by using the command line interface

You can create an NSLOG policy or a SYSLOG policy. The type of policy must match the type of server. The command names for the two types of policy are different, but the parameters for the commands are the same.

At the command prompt, type the following commands:

- add audit syslogPolicy <name> [-rule <expression>] [-action <string>]
- save ns config

Example

The following example creates a policy named syslogP1 that logs application firewall traffic to a syslog server named syslog1.

```
add audit syslogPolicy syslogP1 -rule "ns_true" -action syslog1
save ns config
```

To configure an auditing policy by using the command line interface

At the command prompt, type the following commands:

- set audit syslogPolicy <name> [-rule <expression>] [-action <string>]
- save ns config

Example

The following example modifies the policy named syslogP1 to log application firewall traffic to a syslog server named syslog2.

```
set audit syslogPolicy syslogP1 -rule "ns_true" -action syslog2
save ns config
```

Parameters for an auditing policy

type (Auditing Type)

The type of syslog server that you are using. The choices are nslogPolicy (NSLOG) and syslogPolicy (SYSLOG).

name (Name)

A name for the syslog server. The name can consist of from one to 31 upper-case and lower-case letters, numbers, and the period (.), underscore (_) and hyphen (-) symbols.

rule (no configuration utility equivalent)

The rule that defines the policy. Always `ns_true` for application firewall policies. Must be included when configuring an auditing policy at the NetScaler command line. Is included automatically when configuring by using the configuration utility.

action (Server)

The name of the auditing server.

To configure an auditing policy by using the configuration utility

1. Navigate to Application Firewall > Policies > Auditing.
2. In the details pane, do one of the following:
   - To add a new policy, click Add.
   - To modify an existing policy, select the policy, and then click Open.
3. In the Create Auditing Policy or Configure Auditing Policy dialog box, set the following parameters:
   - Name
   - Auditing Type
   - Server
4. Click Create or OK.

Imports

Several application firewall features make use of external files that you upload to the application firewall when configuring it. Using the configuration utility, you manage those files in the Imports pane, which has four tabs corresponding to the four types of files you can import: HTML error objects, XML error objects, XML schemas, and Web Services Description Language (WSDL) files. Using the NetScaler command line, you can import these types of files, but you cannot export them.

HTML Error Object

When a user's connection to an HTML or Web 2.0 page is blocked, or a user asks for a non-existent HTML or Web 2.0 page, the application firewall sends an HTML-based error response to the user's browser. When configuring which error response the application firewall should use, you have two choices:

- You can configure a *redirect URL*, which can be hosted on any Web server to which users also have access. For example, if you have a custom error page on your Web server, `404.html`, you can configure the application firewall to redirect users to that page when a connection is blocked.
- You can configure an *HTML error object*, which is an HTML-based Web page that is hosted on the application firewall itself. If you choose this option, you must upload the HTML error object to the application firewall. You do that in the Imports pane, on the HTML Error Object tab.

The error object must be a standard HTML file that contains no non-HTML syntax except for application firewall error object customization variables. It cannot contain any CGI scripts, server-parsed code, or PHP code. The customization variables enable you to embed troubleshooting information in the error object that the user receives when a request is blocked. While most requests that the application firewall blocks are illegitimate, even a properly configured application firewall can occasionally block legitimate requests, especially when you first deploy it or after you make significant changes to your protected Web sites. By embedding information in the error page, you provide the user with the information that he or she needs to give to the technical support person so that any issues can be fixed.

The application firewall error page customization variables are:

- `${NS_TRANSACTION_ID}`. The transaction ID that the application firewall assigned to this transaction.
- `${NS_APPFW_SESSION_ID}`. The application firewall session ID.
- `${NS_APPFW_VIOLATION_CATEGORY}`. The specific application firewall security check or rule that was violated.
- `${NS_APPFW_VIOLATION_LOG}`. The detailed error message associated with the violation.

- `${COOKIE("<CookieName>")}`. The contents of the specified cookie. For <CookieName>, substitute the name of the specific cookie that you want to display on the error page. If you have multiple cookies whose contents you want to display for troubleshooting, you can use multiple instances of this customization variable, each with the appropriate cookie name.

  Note: If you have blocking enabled for the Cookie Consistency Check, any blocked cookies are not displayed on the error page because the application firewall blocks them.

To use these variables, you embed them in the HTML or XML of the error page object as if they were an ordinary text string. When the error object is displayed to the user, for each customization variable the application firewall substitutes the information to which the variable refers. An example HTML error page that uses custom variables is shown below.

```
<!doctype html public "-//w3c//dtd html 4.0//en">
<html>
<head>
<title>Page Not Accessible</title>
</head>
<body>
<h1>Page Not Accessible</h1>
<p>The page that you accessed is not available. You can:</p>
<ul>
<li>return to the <b><a href="[homePage]">home page</a></b>, re-establish your session, and try again, or,
<li>report this incident to the help desk via <b><a href="mailto:[helpDeskEmailAddress]">email</a></b> or b
</ul>
<p>If you contact the help desk, please provide the following information:</p>
<table cellpadding=8 width=80%>
<tr><th align="right" width=30%>Transaction ID:</th><td align="left" valign="top" width=70%>${NS_TRANSACT
<tr><th align="right" width=30%>Session ID:</th><td align="left" valign="top" width=70%>${NS_APPFW_SESSIO
<tr><th align="right" width=30%>Violation Category:</th><td align="left" valign="top" width=70%>${NS_APPFW
<tr><th align="right" width=30%>Violation Log:</th><td align="left" valign="top" width=70%>${NS_APPFW_VIO
<tr><th align="right" width=30%>Cookie Name:</th><td align="left" valign="top" width=70%>${COOKIE("[cooki
</table>
<body>
<html>
```

To use this error page, copy it into a text or HTML editor. Substitute the appropriate local information for the following variables, which are enclosed in square brackets to distinguish them from the NetScaler variables. (Leave those unchanged.):

- **[homePage]**. The URL for your web site's home page.
- **[helpDeskEmailAddress]**. The email address that you want users to use to report blocking incidents.
- **[helpDeskPhoneNumber]**. The phone number that you want users to call to report blocking incidents.
- **[cookieName]**. The name of the cookie whose contents you want to display on the error page.

XML Error Object

When a user's connection to an XML page is blocked, or a user asks for a nonexistent XML application, the application firewall sends an XML-based error response to the user's browser. You configure the error response by uploading an XML-based error page to the application firewall in the Imports Pane, on the XML Error Object tab. All XML error responses are hosted on the application firewall. You cannot configure a redirect URL for XML applications.

Note: You can use the same customization variables in an XML error object as in an HTML error object.

XML Schema

When the application firewall performs a validation check on a user's request for an XML or Web 2.0 application, it can validate the request against the XML schema or design type document (DTD) for that application and reject any request that does not follow the schema or DTD. Both an XML schema and a DTD are standard XML configuration files that describe the structure of a specific type of XML document.

WSDL

When the application firewall performs a validation check on a user's request for an XML SOAP-based web service, it can validate the request against the web services type definition (*WSDL*) file for that web service. A WSDL file is a standard XML SOAP configuration file that defines the elements of a specific XML SOAP web service.

Importing and Exporting Files

You can import HTML or XML error objects, XML schemas, DTDs, and WSDLs to the application firewall by using the configuration utility or the NetScaler command line. To export any of these files or objects, or to edit a file or object directly on the application firewall, you must use the configuration utility.

To import a file or object by using the command line interface

At the command prompt, type the following commands:

- import appfw htmlerrorpage <src> <name>
- save ns config

Example

The following example imports an HTML error object from a file named `error.html` and assigns it the name `HTMLError`.

```
import htmlerrorpage error.html HTMLError
save ns config
```

Parameters for Importing a File or Object

type (Type)

The type of file or object that you are uploading. Possible Values: `HTMLErrorPage`, `xmlerrorpage`, `xmlschema`, `wsdl`.

src (Source File)

The full URL or path and filename of the object or file that you want to upload.

- If you are uploading the object from a web site or intranet location, you should type a URL in standard browser format.
- If you are importing the object from your local computer, you should type the path and file name of the object in the appropriate format for your local computer, or use the browse dialog to locate the file.

name (Name)

The name to be assigned to the file or object on the application firewall. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 31

letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) symbols.

To import a file or object by using the configuration utility

Before you attempt to import an XML schema, DTD, or WSDL file, or an HTML or XML error object from a network location, verify that the NetScaler appliance can connect to the Internet or LAN computer where the file is located. Otherwise, you cannot import the file or object.

1. In the Application Firewall Imports pane, select the tab for the type of file you want to import, and then click Add.

   The upload process is identical on all four tabs from the user point of view.

2. In the Import New dialog box, Name text box, type a name for the object you are importing.

3. Choose the type of upload.

   - If the object is on a web site or other location on a LAN, WAN, or the Internet, select Import from URL.

   - If the object is on your local computer or a file server mounted on your local computer, select Import from Local File.

4. In the URL or Local File text box, type the full URL or path and filename to the resource.

5. Click Import.

   - If the application firewall finds the specified resource, the Import Console message box notifies you that the import succeeded. Click Close.

   - If the application firewall is unable to locate the resource, and you are uploading from an Internet or Intranet site, and you have verified that the URL and file you requested exists, click Close to close the Import Console message box. Next, check the NetScaler log file (`ns.log`) to verify that the URL or path and file that you used is accessible from your application firewall. If it is not, fix the access issue or move the file or object to a location that is accessible, and then repeat steps 4 and 5 to import the object.

6. To delete an object, select the object, and then click Remove. When the Proceed dialog box appears, click OK.

To export a file or object

Before you attempt to export an XML schema, DTD, or WSDL file, or an HTML or XML error object from a network location, verify that the application firewall appliance can connect to the Internet or LAN computer where the file is located. Otherwise, you cannot export the file or object.

1. In the Application Firewall Imports pane, select the tab for the type of file you want to export.

   The export process is identical on all four tabs from the user point of view.

2. Select the file that you want to export, and then click Export.

3. In the Export dialog box, click Browse, navigate to a local file system and directory in which to save the file or object that you are exporting, and click Select.

4. Click Export.

To edit a file or object

In the configuration utility, you can modify the properties of configuration files that you previously uploaded to the application firewall. You can also edit the text of HTML and XML error objects directly in the configuration utility.

1. Select the file that you want to modify, and then click Open.

   - If the object is an HTML or XML error object, the text of the object is displayed in a window. You can modify the text by using the standard browser-based editing tools and methods for your browser.

     Note: The edit window is designed to allow you to make minor changes to your HTML or XML error object. To make extensive changes, you may prefer to export the error object to your local computer and use standard HTML or XML web page editing tools.

   - If the object is an XML schema, DTD, or WSDL file, the name and URL of the object are displayed in a dialog box. The name is read-only. You can modify the URL.

2. Click OK (for HTML or XML error objects) or Import (for XML schemas, DTDs, or WSDLs) to save your changes, and then click Close.

Global Configuration

The application firewall global configuration affects all profiles and policies. The Global Configuration items are:

- **Engine Settings.** A collection of global settings—session cookie name, session time-out, maximum session lifetime, logging header name, undefined profile, default profile, and import size limit—that pertain to all connections that the application firewall processes, rather than to a specific subset of connections.

- **Confidential Fields.** A set of form fields in web forms that contain sensitive information that should not be logged to the application firewall logs. Form fields such as password fields on a logon page or credit card information on a shopping cart checkout form are normally designated as confidential fields.

- **Field Types.** The list of web form field types used by the Field Formats security check. Each of these field types is defined by a PCRE-compliant regular expression that defines the type of data and the minimum/maximum length of data that should be allowed in that type of form field.

- **XML Content Types.** The list of content types recognized as XML and subjected to XML-specific security checks. Each of these content types is defined by a PCRE-compliant regular expression that defines the exact MIME type assigned to that content.

- **JSON Content Types.** The list of content types recognized as JSON and subjected to JSON-specific security checks. Each of these content types is defined by a PCRE-compliant regular expression that defines the exact MIME type assigned to that content.

Engine Settings

The engine settings affect all requests and responses that the application firewall processes. They include the following items:

- **Cookie name**—The name of the cookie that stores the NetScaler session ID.
- **Session timeout**—The maximum inactive period allowed. If a user session shows no activity for this length of time, the session is terminated and the user is required to reestablish it by visiting a designated start page.
- **Cookie post-encrypt prefix**—The string that precedes the encrypted portion of any encrypted cookies.
- **Maximum session lifetime**—The maximum amount of time, in seconds, that a session is allowed to remain live. After this period is reached, the session is terminated and the user is required to reestablish it by visiting a designated start page.
- **Logging header name**—The name of the HTTP header that holds the Client IP, for logging.
- **Undefined profile**—The profile applied when the corresponding policy action evaluates as undefined.
- **Default profile**—The profile applied to connections that do not match a policy.
- **Import size limit**—The maximum size in bytes of files imported to the NetScaler appliance.
- **Learn message rate limit**—The maximum number of requests and responses per second that the learning engine is to process. Any additional requests or responses over this limit are not sent to the learning engine.
- **CEF logging**—Use the CEF format instead of the NetScaler format when logging application firewall entries to the NetScaler log.
- **Entity decoding**—Decode HTML entities when running application firewall checks.
- **Log malformed request**—Enable logging of malformed HTTP requests.
- **Use configurable secret key**—Use a configurable secret key for application firewall operations.
- **Manage learned data**—Remove all learned data from the application firewall. Restarts the learning process by collecting fresh data.

Normally, the default values for these settings are correct. If the default settings cause a conflict with other servers or cause premature disconnection of your users, however, you may need to modify them.

To configure engine settings by using the command line interface

At the command prompt, type the following commands:

- set appfw settings [-sessionCookieName <name>] [-sessionTimeout <positiveInteger>] [-cookiePostEncryptPrefix <string>] [-sessionLifetime <positiveInteger>] [-clientIPLoggingHeader <headerName>] [-undefaction <profileName>] [-defaultProfile <profileName>] [-importSizeLimit <positiveInteger>] [-cookiePostEncryptPrefix <string>] [-logMalformedReq (ON | OFF)] [-CEFLogging (ON | OFF)] [-entityDecoding (ON | OFF)] [-useConfigurableSecretKey (ON | OFF)] [-learnRateLimit <positiveInteger>]
- save ns config

Example

```
set appfw settings -sessionCookieName citrix-appfw-id -sessionTimeout 3600
-sessionLifetime 14400 -clientIPLoggingHeader NS-AppFW-Client-IP -undefaction APPFW_RESET
-defaultProfile APPFW_RESET -importSizeLimit 4096
save ns config
```

Parameters for configuring engine settings

sessionCookieName (Cookie Name)

Name of the session cookie, which is a cookie that the application firewall uses to track user sessions. You do not normally need to modify the name of this cookie, but if it conflicts in any way with a cookie set by your protected web servers, you can change it. The cookie name must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols. Default: `citrix_ns_id`.

sessionTimeout (Session Timeout)

Length of time, in seconds, that the application firewall waits before timing out user sessions. After the application firewall times out the session, the user must reestablish a session by visiting the home page or a designated start URL. Possible values: 1 to 600 seconds. Default: 900 seconds (15 minutes).

cookiePostEncryptPrefix (Cookie Post Encrypt Prefix)

String that is prepended to all encrypted cookie values. Default: ENC

sessionLifetime (Maximum Session Lifetime)

Maximum amount of time, in seconds, that the application firewall allows a user session to remain active, regardless of user activity. When the limit is reached, the application firewall terminates the session. To regain access, the user must establish a new session by visiting a designated start page. Possible values: Disabled, or any value from 1 through 14,400 seconds. Default: 900 seconds (15 minutes).

clientIPLoggingHeader (Logging Header Name)

Name of an HTTP header containing the IP address that the client used to connect to your protected web site or service. Possible values: Any value that the HTTP server supports. Default: Null value (do not add a logging header).

undefAction (Undefined Profile)

Profile to use when an application firewall policy evaluates as undefined. An undefined evaluation indicates an internal error condition. If such an error occurs when evaluating a classic policy, the application firewall aborts processing of the associated connections and passes them back to the NetScaler appliance without attempting to filter them. This behavior can constitute a security hazard in some circumstances, so the default setting specifies the APPFW_BLOCK built-in profile. You can specify a different built-in or user-created profile as the undefined profile.

defaultProfile (Default Profile)

Profile to use when a connection does not match any of the policies that you have defined on the application firewall. Normally the default profile is set to APPFW_BYPASS, which configures the application firewall to send connections that fail to match any policy back to the NetScaler appliance without attempting to filter them further.

importSizeLimit (Import Size Limit)

Cumulative total maximum number of bytes allowed for importing files to the application firewall. If the total size of uploaded files in a web form is larger than the configured limit, the application firewall blocks the request. Possible value: Any number. Default: 0 (disabled).

learnRateLimit (Learn Message Rate Limit)

Total number of requests and responses per second that the application firewall learning feature is to examine and use to learn new rules and relaxations. The learning feature ignores any requests or responses in excess of this number. Possible value: Any positive integer. Default: 0 (disabled).

CEFLogging (CEF Logging)

Enable or disable CEF-format logging. For more information about CEF logging, see "Logs, Statistics, and Reports." Possible values: Yes, No. Default: No.

entityDecoding (Entity Decoding)

Decode HTML entities before performing security checks. Possible values: Yes, No. Default: No

logMalformedReq (Log Malformed Request)

Log requests that are so malformed that the application firewall does not attempt to parse them. Possible values: Yes, No. Default: No

useConfigurableSecretKey (Use Configurable Secret Key)

Use a configurable secret key for application firewall operations. Possible values: Yes, No. Default: No

(Manage Learned Data)

Click Remove Learned Data to remove all learned data that you have not yet reviewed and deployed from the learning feature, and starts over from the beginning. Does not remove learned data that has been deployed (implemented) as rules or relaxations for security checks. This button is only available when using the configuration utility, and is identical to the Remove Learned Data button on the Configure Application Firewall Profile dialog box, Learning tab.

To configure engine settings by using the configuration utility

1. In the navigation pane, click Application Firewall.
2. In the details pane, click Change Engine Settings.
3. In the Application Firewall Engine Settings dialog box, set the following parameters:
   - Cookie Name
   - Session Timeout
   - Cookie Post Encrypt Prefix
   - Maximum Session Lifetime
   - Logging Header Name
   - Undefined Profile
   - Default Profile
   - Import Size Limit
   - Learn Messages Rate Limit
   - CEF Logging
   - Entity Decoding
   - Log Malformed Request
   - Use Configurable Secret Key
   - Manage Learned Data
   - Signatures Auto Update
   - Signatures Update URL
4. Click OK.

Confidential Fields

You can designate web-form fields as confidential to protect the information users type into them. Normally, any information a user types into a web form on one of your protected web servers is logged in the NetScaler logs. The information typed into a web-form field designated as confidential, however, is not logged. That information is saved only where the web site is configured to save such data, normally in a secure database.

Common types of information that you may want to protect with a confidential field designation include:

- Passwords
- Credit card numbers, validation codes, and expiration dates
- Social security numbers
- Tax ID numbers
- Home addresses
- Private telephone numbers

In addition to being good practice, proper use of confidential field designations may be necessary for PCI-DSS compliance on ecommerce servers, HIPAA compliance on servers that manage medical information in the United States, and compliance with other data protection standards.

Important: In the following two cases, the Confidential Field designation does not function as expected:

- If a Web form has either a confidential field or an action URL longer than 256 characters, the field or action URL is truncated in the NetScaler logs.
- With certain SSL transactions, the logs are truncated if either the confidential field or the action URL is longer than 127 characters.

In either of these cases, the application firewall masks a fifteen-character string with the letter "x," instead of the normal eight character string. To ensure that any confidential information is removed, the user must use form field name and action URL expressions that match the first 256, or (in cases where SSL is used) the first 127 characters.

To configure your application firewall to treat a web-form field on a protected web site as confidential, you add that field to the Confidential Fields list. You can enter the field name as a string, or you can enter a PCRE-compatible regular expression specifying one or more fields. You can enable the confidential-field designation when you add the field, or you can modify the designation later.

To add a confidential field by using the command line interface

At the command prompt, type the following commands:

- add appfw confidField <fieldName> <url> [-isRegex (REGEX | NOTREGEX)] [-comment "<string>"] [-state (ENABLED | DISABLED)]
- save ns config

Example

The following example adds all web form fields whose names begin with Password to the confidential fields list.

```
add appfw confidField Password "https?://www[.]example[.]com/[^<>]*[^a-z]password[0-9a-z._-]*[.](asp|cg
save ns config
```

To modify a confidential field by using the command line interface

At the command prompt, type the following commands:

- set appfw confidField <fieldName> <url> [-isRegex (REGEX | NOTREGEX)] [-comment "<string>"] [-state (ENABLED | DISABLED)]
- save ns config

Example

The following example modifies the confidential field designation to add a comment.

```
set appfw confidField Password "https?://www[.]example[.]com/[^<>]*[^a-z]password[0-9a-z._-]*[.](asp|cgi
save ns config
```

To remove a confidential field by using the command line interface

At the command prompt, type the following commands:

- rm appfw confidField <fieldName> <url>
- save ns config

Parameters for configuring a confidential field

state (Enable)

Enable the field's designation as a confidential field.

name (Field Name)

The name of the web form field that you are designating as confidential.

isRegex (Is form field name a regular expression)

Is the string that you used to define the form field name a regular expression or not?

url (Action URL)

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

comment (Comments)

A comment. Optional.

To configure a confidential field by using the configuration utility

1. In the navigation pane, click Application Firewall.
2. In the details pane, under Settings, click Manage Confidential Fields.
3. In the Manage Confidential Fields dialog box, do one of the following:
   - To add a new form field to the list, click Add.
   - To change an existing confidential field designation, select the field, and then click Open.

   The Create Confidential Form Field dialog box or the Configure Confidential Form Field dialog box appears.

   Note: If you select an existing confidential field designation and then click Add, the Create Confidential Form Field dialog box displays the information for that confidential field. You can modify that information to create your new confidential field.
4. In the dialog box, fill out the elements. They are:
   - **Enabled check box.** Select or clear to enable/disable this confidential field designation.
   - **Is form field name a regular expression check box.** Select or clear to enable PCRE-format regular expressions in the form field name.
   - **Field Name.** Enter a literal string or PCRE-format regular expression that either represents a specific field name or that matches multiple fields with names that follow a pattern.
   - **Action URL.** Enter a literal URL or a regular expression that defines one or more URLs of the web page(s) on which the web form(s) that contains the confidential field are located.
   - **Comments.** Enter a comment. Optional.
5. Click Create or OK.
6. To remove a confidential field designation from the confidential fields list, select the confidential field listing you want to remove, then click Remove to remove it, and then click OK to confirm your choice.
7. When you have finished adding, modifying, and removing confidential field designations, click Close.

Examples

Following are some regular expressions that define form field names that you might find useful:

- `^passwd_` (Applies confidential-field status to all field names that begin with the "passwd_" string.)

- `^(([0-9a-zA-Z._-]*||\\x[0-9A-Fa-f][0-9A-Fa-f])+-)?passwd_` (Applies confidential-field status to all field names that begin with the string passwd_, or that contain the string -passwd_ after another string that might contain non-ASCII special characters.)

Following are some regular expressions that define specific URL types that you might find useful. Substitute your own web host(s) and domain(s) for those in the examples.

- If the web form appears on multiple web pages on the web host `www.example.com`, but all of those web pages are named `logon.pl?`, you could use the following regular expression:

  https?://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_.-]*/)*logon[.]pl\?

- If the web form appears on multiple web pages on the web host `www.example-español.com`, which contains the n-tilde (ñ) special character, you could use the following regular expression, which represents the n-tilde special character as an encoded UTF-8 string containing C3 B1, the hexadecimal code assigned to that character in the UTF-8 charset:

  https?://www[.]example-espa\xC3\xB1ol[.]com/([0-9A-Za-z][0-9A-Za-z_.-]*/)* logon[.]pl\?

- If the web form containing `query.pl` appears on multiple web pages on different hosts within the `example.com` domain, you could use the following regular expression:

  https?://([0-9A-Za-z][0-9A-Za-z_-.]*[.])*example[.]com/([0-9A-Za-z][0-9A-Za-z_-.]*/)*logon[.]pl\?

- If the web form containing `query.pl` appears on multiple web pages on different hosts in different domains, you could use the following regular expression:

  https?://([0-9A-Za-z][0-9A-Za-z_-.]*[.])*[0-9A-Za-z][0-9A-Za-z_-.]+[.][a-z]{2,6}/([0-9A-Za-z][0-9A-Za-z_-.

- If the web form appears on multiple web pages on the web host `www.example.com`, but all of those web pages are named `logon.pl?`, you could use the following regular expression:

  https?://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-.]*/)*logon[.]pl\?

Field Types

A field type is a PCRE-format regular expression that defines a particular data format and minimum/maximum data lengths for a form field in a web form. Field types are used in the Field Formats check.

The application firewall comes with several default field types, which are:

- `integer`. A string of any length consisting of numbers only, without a decimal point, and with an optional preceding minus sign (-).
- `alpha`. A string of any length consisting of letters only.
- `alphanum`. A string of any length consisting of letters and/or numbers.
- `nohtml`. A string of any length consisting of characters, including punctuation and spaces, that does not contain HTML symbols or queries.
- `any`. Anything at all.

  Important: Assigning the `any` field type as the default field type, or to a field, allows active scripts, SQL commands, and other possibly dangerous content to be sent to your protected web sites and applications in that form field. You should use the any type sparingly, if you use it at all.

You can also add your own field types to the Field Types list. For example, you might want to add a field type for a social security number, postal code, or phone number in your country. You might also want to add a field type for a customer identification number or store credit card number.

To add a field type to the Field Types list, you enter the field name as a literal string or PCRE-format regular expression.

To add a field type by using the command line interface

At the command prompt, type the following commands:

- add appfw fieldType <name> <regex> <priority> [-comment "<string>"]
- save ns config

Example

The following example adds a field type named `SSN` that matches US Social Security numbers to the Field Types list, and sets its priority to 1.

```
add appfw fieldType SSN "^[1-9][0-9]{2,2}-[0-9}{2,2}-[0-9]{4,4}$" 1
save ns config
```

To modify a field type by using the command line interface

At the command prompt, type the following commands:

- set appfw fieldType <name> <regex> <priority> [-comment "<string>"]
- save ns config

Example

The following example modifies the field type to add a comment.

```
set appfw fieldType SSN "^[1-9][0-9]{2,2}-[0-9}{2,2}-[0-9]{4,4}$" 1 -comment "US Social Security Number"
save ns config
```

To remove a field type by using the command line interface

At the command prompt, type the following commands:

- rm appfw fieldType <name>
- save ns config

Parameters for configuring a field type

name (Field Name)

The name of the field type. If you are adding a new field type, this can be a string of from one to 31 letters, numbers, and the underscore and hyphen symbols.

rule (Regular Expression)

The PCRE-format regular expression that defines the character format and length allowed in this field type.

url (URL)

A literal string or PCRE-format regular expression that describes the URL or URLs that host the web form(s) where the form field(s) are located.

priority (Priority)

A positive integer that designates the order in which this field type is checked for a match. A field type with a lower priority (such as 1) is checked before a field type with a higher priority (such as 2)

comment (Comments)

A comment. Optional.

To configure a field type by using the configuration utility

1. In the navigation pane, click Application Firewall.
2. In the details pane, under Settings, click Manage Field Types.
3. In the Manage Field Types dialog box, do one of the following:
   - To add a new field type to the list, click Add.
   - To change an existing field type, select the field type, and then click Open.

   The Create Field Type dialog box or the Configure Field Type dialog box appears.

   Note: If you select an existing field type designation and then click Add, the Create Field Type dialog box displays the information for that field type. You can modify that information to create your new field type.
4. In the dialog box, fill out the elements. They are:
   - Name
   - Regular Expression
   - Priority
   - Comment
5. Click Create or OK.
6. To remove a field type from the Field Types list, select the field type listing you want to remove, then click Remove to remove it, and then click OK to confirm your choice.
7. When you have finished adding, modifying, and removing field types, click Close.

Examples

Following are some regular expressions for field types that you might find useful:

- `^[1-9][0-9]{2,2}-[0-9}{2,2}-[0-9]{4,4}$` U.S. Social Security numbers
- `^[A-C][0-9]{7,7}$` California driver's license numbers.

- `^+[0-9]{1,3} [0-9() -]{1,40}$` International phone numbers with country codes.
- `^[0-9]{5,5}-[0-9]{4,4}$` U.S. ZIP code numbers.
- `^[0-9A-Za-z][0-9A-Za-z.+_-]{0,25}@([0-9A-Za-z][0-9A-Za-z_-]*[.]){1,4}[A-Za-z]{2,6}$` Email addresses.

XML Content Types

By default, the application firewall treats files that follow certain naming conventions as XML. You can configure the application firewall to examine web content for additional strings or patterns that indicate that those files are XML files. This can ensure that the application firewall recognizes all XML content on your site, even if certain XML content does not follow normal XML naming conventions, ensuring that XML content is subjected to XML security checks.

To configure the XML content types, you add the appropriate patterns to the XML Content Types list. You can enter a content type as a string, or you can enter a PCRE-compatible regular expression specifying one or more strings. You can also modify the existing XML content types patterns.

To add an XML content type pattern by using the command line interface

At the command prompt, type the following commands:

- add appfw XMLContentType <XMLContenttypevalue> [-isRegex (REGEX | NOTREGEX)]
- save ns config

Example

The following example adds the pattern `.*/xml` to the XML Content Types list and designates it as a regular expression.

```
add appfw XMLContentType ".*/xml" -isRegex REGEX
```

To remove an XML content type pattern by using the command line interface

At the command prompt, type the following commands:

- rm appfw XMLContentType <XMLContenttypevalue>
- save ns config

Parameters for configuring an XML content type pattern

XMLContenttypevalue (XML Content Type)

The string or regular expression that identifies the XML content type.

isRegex (Is XML content type a regular expression)

Is the string that you used to define the XML content type a regular expression or not?

To configure the XML content type list by using the configuration utility

1. In the navigation pane, click Application Firewall.
2. In the details pane, under Settings, click Manage XML Content Types.
3. In the Manage XML Content Types dialog box, click Add. The Create XML Content Type dialog box appears.

   Note: If you select an existing XML content type pattern and then click Add, the Create XML Content Type dialog box displays the information for that XML content type pattern. You can modify that information to create your new XML content type pattern.
4. In the dialog box, fill out the elements. They are:
   - **Is XML content type a regular expression check box.** Select or clear to enable PCRE-format regular expressions in the form field name.
   - **XML Content Type** Enter a literal string or PCRE-format regular expression that matches the XML content type pattern that you want to add.
5. Click Create.
6. To remove an XML content type pattern from the list, select it, then click Remove to remove it, and then click OK to confirm your choice.
7. When you have finished adding and removing XML content type patterns, click Close.

JSON Content Types

By default, the application firewall treats files with the content type "appliction/json" as JSON files. You can configure the application firewall to examine web content for additional strings or patterns that indicate that those files are JSON files. This can ensure that the application firewall recognizes all JSON content on your site, even if certain JSON content does not follow normal JSON naming conventions, ensuring that JSON content is subjected to JSON security checks.

To configure the JSON content types, you add the appropriate patterns to the JSON Content Types list. You can enter a content type as a string, or you can enter a PCRE-compatible regular expression specifying one or more strings. You can also modify the existing JSON content types patterns.

To add a JSON content type pattern by using the command line interface

At the command prompt, type the following commands:

- add appfw JSONContentType <JSONContenttypevalue> [-isRegex (REGEX | NOTREGEX)]
- save ns config

Example

The following example adds the pattern `.*/json` to the JSON Content Types list and designates it as a regular expression.

```
add appfw JSONContentType ".*/json" -isRegex REGEX
```

To configure the JSON content type list by using the configuration utility

1. In the navigation pane, click Application Firewall.
2. In the details pane, under Settings, click Manage JSON Content Types.
3. In the Manage JSON Content Types dialog box, click Add. The Create JSON Content Type dialog box appears.

   Note: If you select an existing JSON content type pattern and then click Add, the Create JSON Content Type dialog box displays the information for that JSON content type pattern. You can modify that information to create your new JSON content type pattern.

4. In the dialog box, fill out the elements. They are:

   - **Is JSON content type a regular expression check box.** Select or clear to enable PCRE-format regular expressions in the form field name.
   - **JSON Content Type** Enter a literal string or PCRE-format regular expression that matches the JSON content type pattern that you want to add.

5. Click Create.
6. To remove a JSON content type pattern from the list, select it, then click Remove to remove it, and then click OK to confirm your choice.
7. When you have finished adding and removing XML content type patterns, click Close.

Logs, Statistics, and Reports

The information maintained in the logs and statistics, and displayed in the reports, provides important guidance for configuring and maintaining the application firewall.

The Application Firewall Logs

The logs provide information about the requests and responses that the application firewall has observed while protecting your web sites and applications. Most important, it logs each connection that matches a signature or a security check. You can observe the logs to determine which connections are matching a signature or security check. You can then use this information, along with your own knowledge about your protected web sites and applications, to determine whether the connections that each signature or check is matching are valid (*false positives*). If they are, you can either remove the signature or check from your configuration, or take appropriate measures to mitigate the false positives before you enable blocking for that signature or security check.

NetScaler Format Logs

When configured to use NetScaler format logs, the application firewall produces logs that follow the same format as other NetScaler features. Each log contains the following fields:

- **Timestamp.** The date and time when the connection occurred.
- **Severity.** The severity level of the log.
- **Module.** The NetScaler module that generated the log entry.
- **Event Type.** The type of event, such as signature violation or security check violation.
- **Event ID.** The ID assigned to the event.
- **Client IP.** The IP address of the user whose connection was logged.
- **Transaction ID**. The ID assigned to the transaction that caused the log.
- **Session ID.** The ID assigned to the user session that caused the log.
- **Message.** The log message. Contains information identifying the signature or security check that triggered the log entry.

You can search on any of these fields, or any combination of information from different fields, to select logs to display, limited only by the capabilities of the tools you use to view the logs. You can observe the signatures by using the application firewall wizard to access the NetScaler syslog viewer, or manually by logging onto the NetScaler appliance or NetScaler virtual appliance.

Viewing the Application Firewall Logs

You can view the logs by using the syslog viewer, or by logging onto the NetScaler appliance, opening a Unix shell, and using the Unix text editor of your choice.

- **Viewing by using the syslog viewer.** You invoke the syslog viewer from one of two locations: the Select Signature Actions page or the Select Advanced Actions page in the Application Firewall Wizard. To invoke the syslog viewer for a signature, in the Select Signature Actions pane click the logs link to the right of that signature. To invoke the syslog viewer for a security check, in the Select Advanced Actions page, security checks list, select that security check, and then beneath the list click the Logs button. Either procedure causes the configuration utility to download the current `ns.log` file and then display the entries that are relevant to that signature or security check.

  The syslog viewer contains the following elements:

  - *Module list box*. The NetScaler module whose logs you want to view. Always set to APPFW for application firewall logs.
  - *Event Type list box*. The type of event. For signatures, this is always APPFW_SIGNATURE_MATCH. For security checks, this is the specific security check that you selected.
  - *Severity*. It lets you specify only logs of a specific severity level. Leave blank to see all logs.
  - *Find Now button*. Search the `nslog.file`, using the current criteria, and display the logs that match.
  - *Clear button*. Resets your settings to the defaults.
  - *Logs display window*. Displays the logs that meet the current criteria. Log information is displayed in several columns that correspond to the log fields for the log format that the application firewall is currently configured to maintain, with an additional column, Deploy, to the extreme left. You can sort the display by clicking a column heading. You can create and implement a relaxation for a signature or security check that is blocking legitimate use of a protected web site or web service by selecting a log that shows the unwanted blocking, and then clicking Deploy.
  - *Log directory*. The directory where the logs are stored. If you have archived logs stored in a different directory and want to view those, you can click Browse and browse to that directory to display those logs in the Log files list.
  - *Log files list*. A list of the log files in the Log directory. To download and uncompress an archived log file, select the file, and then click Download. To refresh the display, click Refresh.
  - *Search in list box*. Searches in a particular section of logs when selecting logs to display in the Logs display window. To search something other than the log message, select a different choice.
  - *Search string*. Search for the specified string or regular expression to choose the logs to display in the Logs display window. This field is filled out by the application firewall wizard for you with the appropriate value to display the logs relevant to the signature or security check that you selected. You can modify the string to choose logs based on different criteria.

- *Case Sensitive check box*. Select if the Search string is case sensitive.
- *Regular Expression check box*. Select if the Search string is a regular expression.
- *Clear button*. Resets the syslog viewer to its default settings.
- *Go button*. Uses the new search criteria to search the `ns.log` file and displays the results in the Logs display window.

For more information about the Application Firewall Wizard, see "The Application Firewall Wizard."

- **Viewing from the command line.** Log onto the application firewall appliance, and then type the following command at the NetScaler command prompt:

  ```
  shell
  ```

  After the Unix shell is displayed, type the following command to navigate to the directory where the logs are stored:

  ```
  cd /var/log
  ```

  You can use the vi editor, or any Unix text editor or text search tool of your choice to view and filter the logs for specific entries.

  Note: If the text editor or text search tool is not installed by default on the NetScaler appliance, you must first install it before you can use it to view and filter the logs.

The Application Firewall Statistics

When you enable the statistics action for application firewall signatures or security checks, the application firewall maintains information about connections that match that signature or security check. You can view the accumulated statistics information on the Monitoring tab of the main logon page of your application firewall appliance by selecting one of the following choices in the Select Group list box:

- **Application Firewall.** A summary of all statistics information gathered by your application firewall appliance for all profiles.
- **Application Firewall (per profile).** The same information, but displayed per-profile rather than summarized.

You can use this information to monitor how your application firewall is operating and determine whether there is any abnormal activity or abnormal amounts of hits on a signature or security check. If you see such a pattern of abnormal activity, you can check the logs for that signature or security check, to diagnose the issue, and then take corrective action.

The Application Firewall Reports

The application firewall reports provide information about your application firewall configuration and how it is handling traffic for your protected web sites.

The PCI DSS Report

The Payment Card Industry (PCI) Data Security Standard (DSS), version 1.2, consists of twelve security criteria that most credit card companies require businesses who accept online payments via credit and debit cards to meet. These criteria are designed to prevent identity theft, hacking, and other types of fraud. If an internet service provider or online merchant does not meet the PCI DSS criteria, that ISP or merchant risks losing authorization to accept credit card payments through its web site.

ISPs and online merchants prove that they are in compliance with PCI DSS by having an audit conducted by a PCI DSS Qualified Security Assessor (QSA) Company. The PCI DSS report is designed to assist them both before and during the audit. Before the audit, it shows which application firewall settings are relevant to PCI DSS, how they should be configured, and (most important) whether your current application firewall configuration meets the standard. During the audit, the report can be used to demonstrate compliance with relevant PCI DSS criteria.

The PCI DSS report consists of a list of those criteria that are relevant to your application firewall configuration. Under each criterion, it lists your current configuration options, indicates whether your current configuration complies with the PCI DSS criterion, and explains how to configure the application firewall so that your protected web site(s) will be in compliance with that criterion.

The PCI DSS report is located under System > Reports. To generate the report as an Adobe PDF file, click Generate PCI DSS Report. Depending on your browser settings, the report is displayed in the pop-up window or you are prompted to save it to your hard disk.

Note: To view this and other reports, you must have the Adobe Reader program installed on your computer.

The PCI DSS report consists of the following sections:

- **Description.** A description of the PCI DSS Compliance Summary report.
- **Firewall License and Feature Status.** Tells you whether the application firewall is licensed and enabled on your NetScaler appliance.
- **Executive Summary.** A table that lists the PCI DSS criteria and tells you which of those criteria are relevant to the application firewall.
- **Detailed PCI DSS Criteria Information.** For each PCI DSS criterion that is relevant to your application firewall configuration, the PCI DSS report provides a section that contains information about whether your configuration is currently in compliance and, if it is not, how to bring it into compliance.
- **Configuration.** Data for individual profiles, which you access either by clicking Application Firewall Configuration at the top of the report, or directly from the Reports pane. The Application Firewall Configuration report is the same as the PCI DSS report, with the PCI DSS-specific summary omitted, and is described below.

The Application Firewall Configuration Report

The Application Firewall Configuration report is located under System > Reports. To display it, click Generate Application Firewall Configuration Report. Depending on your browser settings, the report is displayed in the pop-up window or you are prompted to save it to your hard disk.

The Application Firewall Configuration report starts with a Summary page, which consists of the following sections:

- **Application Firewall Policies.** A table that lists your current application firewall policies, showing the policy name, the content of the policy, the action (or profile) it is associated with, and global binding information.

- **Application Firewall Profiles.** A table that lists your current application firewall profiles and indicates which policy each profile is associated with. If a profile is not associated with a policy, the table displays INACTIVE in that location.

To download all report pages for all policies, at the top of the Profiles Summary page click Download All Profiles. You display the report page for each individual profile by selecting that profile in the table at the bottom of the screen. The Profile page for an individual profile shows whether each check action is enabled or disabled for each check, and the other configuration settings for the check.

To download a PDF file containing the PCI DSS report page for the current profile, click Download Current Profile at the top of the page. To return to the Profiles Summary page, click Application Firewall Profiles. To go back to the main page, click Home. You can refresh the PCI DSS report at any time by clicking Refresh in the upper right corner of the browser. You should refresh the report if you make changes to your configuration.

Appendices

The following supplemental material provides additional detail about complex or peripheral application firewall tasks.

PCRE Character Encoding Format

The NetScaler operating system supports direct entry of characters in the printable ASCII character set only—characters with hexadecimal codes between HEX 20 (ASCII 32) and HEX 7E (ASCII 127). To include a character with a code outside that range in your application firewall configuration, you must enter its UTF-8 hexadecimal code as a PCRE regular expression.

A number of character types require encoding using a PCRE regular expression if you include them in your application firewall configuration as a URL, form field name, or Safe Object expression. They include:

- **Upper-ASCII characters.** Characters with encodings from HEX 7F (ASCII 128) to HEX FF (ASCII 255). Depending on the character map used, these encodings can refer to control codes, ASCII characters with accents or other modifications, non-Latin alphabet characters, and symbols not included in the basic ASCII set. These characters can appear in URLs, form field names, and safe object expressions.

- **Double-Byte characters.** Characters with encodings that use two 8-byte words. Double-byte characters are used primarily for representing Chinese, Japanese, and Korean text in electronic format. These characters can appear in URLs, form field names, and safe object expressions.

- **ASCII control characters.** Non-printable characters used to send commands to a printer. All ASCII characters with hexadecimal codes less than HEX 20 (ASCII 32) fall into this category. These characters should never appear in a URL or form field name, however, and would rarely if ever appear in a safe object expression.

The NetScaler appliance does not support the entire UTF-8 character set, but only the characters found in the following eight charsets:

- **English US (ISO-8859-1).** Although the label reads, “English US,” the application firewall supports all characters in the ISO-8859-1 character set, also called the Latin-1 character set. This character set fully represents most modern western European languages and represents all but a few uncommon characters in the rest.

- **Chinese Traditional (Big5).** The application firewall supports all characters in the BIG5 character set, which includes all of the Traditional Chinese characters (ideographs) commonly used in modern Chinese as spoken and written in Hong Kong, Macau, Taiwan, and by many people of Chinese ethnic heritage who live outside of mainland China.

- **Chinese Simplified (GB2312).** The application firewall supports all characters in the GB2312 character set, which includes all of the Simplified Chinese characters (ideographs) commonly used in modern Chinese as spoken and written in mainland China.

- **Japanese (SJIS).** The application firewall supports all characters in the Shift-JIS (SJIS) character set, which includes most characters (ideographs) commonly used in modern Japanese.

- **Japanese (EUC-JP).** The application firewall supports all characters in the EUC-JP character set, which includes all characters (ideographs) commonly used in modern Japanese.

- **Korean (EUC-KR).** The application firewall supports all characters in the EUC-KR character set, which includes all characters (ideographs) commonly used in modern Korean.

- **Turkish (ISO-8859-9).** The application firewall supports all characters in the ISO-8859-9 character set, which includes all letters used in modern Turkish.

- **Unicode (UTF-8).** The application firewall supports certain additional characters in the UTF-8 character set, including those used in modern Russian.

When configuring the application firewall, you enter all non-ASCII characters as PCRE-format regular expressions using the hexadecimal code assigned to that character in the UTF-8 specification. Symbols and characters within the normal ASCII character set, which are assigned single, two-digit codes in that character set, are assigned the same codes in the UTF-8 character set. For example, the exclamation point (!), which is assigned hex code 21 in the ASCII character set, is also hex 21 in the UTF-8 character set. Symbols and characters from another supported character set have a paired set of hexadecimal codes assigned to them in the UTF-8 character set. For example, the letter a with an acute accent (á) is assigned UTF-8 code C3 A1.

The syntax you use to represent these UTF-8 codes in the application firewall configuration is “\xNN” for ASCII characters; “\xNN\xNN” for non-ASCII characters used in English, Russian, and Turkish; and “\xNN\xNN\xNN” for characters used in Chinese, Japanese, and Korean. For example, if you want to represent a ! in an application firewall regular expression as a UTF-8 character, you would type \x21. If you want to include an á, you would type \xC3\xA1.

Note: Normally you do not need to represent ASCII characters in UTF-8 format, but when those characters might confuse a web browser or an underlying operating system, you can use the character’s UTF-8 representation to avoid this confusion. For example, if a URL contains a space, you might want to encode the space as \x20 to avoid confusing certain browsers and web server software.

Below are examples of URLs, form field names, and safe object expressions that contain non-ASCII characters that must be entered as PCRE-format regular expressions to be included in the application firewall configuration. Each example shows the actual URL, field name, or expression string first, followed by a PCRE-format regular expression for it.

- A URL containing extended ASCII characters.

  Actual URL: `http://www.josénuñez.com`

  Encoded URL: `^http://www[.]jos\xC3\xA9nu\xC3\xB1ez[.]com$`

- Another URL containing extended ASCII characters.

  Actual URL: `http://www.example.de/trömso.html`

  Encoded URL: `^http://www[.]example[.]de/tr\xC3\xB6mso[.]html$`

- A form field name containing extended ASCII characters.

Actual Name: `nome_do_usuário`

Encoded Name: `^nome_do_usu\xC3\xA1rio$`

- A safe object expression containing extended ASCII characters.

  Unencoded Expression `[A-Z]{3,6}¥[1-9][0-9]{6,6}`

  Encoded Expression: `[A-Z]{3,6}\xC2\xA5[1-9][0-9]{6,6}`

You can find a number of tables that include the entire Unicode character set and matching UTF-8 encodings on the Internet. A useful web site that contains this information is located at the following URL:

http://www.utf8-chartable.de/unicode-utf8-table.pl

For the characters in the table on this web site to display correctly, you must have an appropriate Unicode font installed on your computer. If you do not, the visual display of the character may be in error. Even if you do not have an appropriate font installed to display a character, however, the description and the UTF-8 and UTF-16 codes on this set of web pages will be correct.

Whitehat WASC Signature Types for WAF Use

The Citrix NetScaler Application Firewall accepts and generates blocking rules for all vulnerability types that the Whitehat scanners generate. However, certain vulnerabilities are most applicable to a web application firewall. Following are lists of those vulnerabilities, categorized by whether they are addressed by WASC 1.0, WASC 2.0, or best practices signature types.

WASC 1.0 Signature Types

- HTTP Request Smuggling
- HTTP Response Splitting
- HTTP Response Smuggling
- Null Byte Injection
- Remote File Inclusion
- URL Redirector Abuse

WASC 2.0 Signature Types

- Abuse of Functionality
- Brute Force
- Content Spoofing
- Denial of Service
- Directory Indexing
- Information Leakage
- Insufficient Anti-automation
- Insufficient Authentication
- Insufficient Authorization
- Insufficient Session Expiration
- LDAP Injection
- Session Fixation

Best Practices

- Autocomplete Attribute
- Insufficient Cookie Access Control
- Insufficient Password Strength
- Invalid HTTP Method Usage
- Non-HttpOnly Session Cookie
- Persistent Session Cookie
- Personally Identifiable Information
- Secured Cachable HTTP Messages
- Unsecured Session Cookie

Content Filtering

Content filtering can do some of the same tasks as the Citrix® Application Firewall™, and is a less CPU-intensive tool. It is limited, however, to examining the header portion of the HTTP request or response and to performing a few simple actions on connections that match. If you have a complex Web site that makes extensive use of scripts and accesses back-end databases, the Application Firewall may be the better tool for protecting that Web site. For more information about the Citrix® Application Firewall™, see the *Citrix Application Firewall Guide* at http://support.citrix.com/article/CTX132360.

Content filtering is based on regular expressions that you can apply to either HTTP requests or HTTP responses. To block requests from a particular site, for example, you could use an expression that compares each request's URL to the URL specified in the expression. The expression is part of a policy, which also specifies an action to be performed on requests or responses that match the expression. For example, an action might drop a request or reset the connection.

Following are some examples of things you can do with content filtering policies:

- Prevent users from accessing certain parts of your Web sites unless they are connecting from authorized locations.
- Prevent inappropriate HTTP headers from being sent to your Web server, possibly breaching security.
- Redirect specified requests to a different server or service.

To configure content filtering, once you have made sure that the feature is enabled, you configure filtering actions for your servers to perform on selected connections (unless the predefined actions are adequate for your purposes). Then you can configure policies to apply the actions to selected connections. Your policies can use predefined expressions, or you can create your own. To activate the policies you configured, you bind them either globally or to specific virtual servers.

Enabling Content Filtering

By default, content filtering is enabled on NetScaler appliances running the NetScaler operating system 8.0 or above. If you are upgrading an existing appliance from an operating system version earlier than 8.0, you must update the licenses before you can use content filtering, and you may need to enable the content filtering feature itself manually.

To enable content filtering by using the command line interface

At the command prompt, type the following commands to enable content filtering and verify the configuration:

- enable ns feature `ContentFiltering`
- show ns feature

Example

```
> enable ns feature ContentFiltering
 Done
> show ns feature

      Feature                 Acronym          Status
      -------                 -------          ------
1)    Web Logging               WL               ON
2)    Surge Protection          SP               OFF
.
.
.
.
11)   Http DoS Protection       HDOSP            OFF
12)   Content Filtering         CF               ON
.
.
23)   HTML Injection            HTMLInjection    ON
24)   NetScaler Push            push             OFF
Done
```

To enable content by filtering by using the configuration utility

1. In the navigation pane, expand System, and then select Settings.
2. In the details pane, click Change basic features.
3. In the Configure Basic Features dialog box, select the Content Filtering check box, and then click OK.
4. In the Enable/Disable feature(s) dialog box, click Yes. A message appears in the status bar, stating that the selected feature is enabled.

Configuring a Content Filtering Action

After you enable the content filtering feature, you create one or more actions to tell your NetScaler appliance how to handle the connections it receives.

Content filtering supports the following actions for HTTP requests:

Add

Adds the specified HTTP header before sending the request to the Web server.

Reset

Terminates the connection, sending the appropriate termination notice to the user's browser.

Forward

Redirects the request to the designated service.

Drop

Silently deletes the request, without sending a response to the user's browser.

Corrupt

Modifies the designated HTTP header in a manner that prevents it from performing the function it was intended to perform, then sends the request to the server.

Content filtering supports the following actions for HTTP responses:

Add

Adds the specified HTTP header before sending the response to the user's browser.

ErrorCode

Returns the designated HTTP error code to the user's browser.

Corrupt

Modifies the designated HTTP header in a manner that prevents it from performing the function it was intended to perform, then sends the response to the user's browser.

To configure a content filtering action by using the command line interface

At the command prompt, type the following commands to configure a Content Filtering action and verify the configuration:

- add filter action <name> <qualifier> [<serviceName>] [<value>] [<respCode>] [<page>]
- show filter action <name>

Example

```
> add filter action act_drop Drop
 Done
> show filter action act_drop
1)      Name: act_drop    Filter Type: drop
 Done
```

Parameters for configuring a content filtering action

name

A name for the filtering action. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should choose a name that helps identify the type of action. (Cannot be changed after the action has been created.)

qualifier

The action that you want your content filtering Action to perform. (Cannot be changed after the action has been created.)

servicename

If the Qualifier is Forward, the name of the service to which you want to forward requests. If the Qualifier is Forward, you must configure either a servicename or a page, but not both. Otherwise, you should not set this value.

value

If the Qualifier is Add, the header that you want added. This argument is optional.

respcode

If the Qualifier is ErrorCode, the numeric code you want returned to the user (such as 404, the standard HTTP code for a non-existent Web page). This argument is optional.

page

If the Qualifier is Forward, you must configure either a servicename or a page, but not both. Otherwise, you should not set this value.

To configure a content filtering action by using the configuration utility

1. Navigate to Protection Features > Filter.
2. In the details pane, do one of the following:
   - To create a new action, click Add.
   - To modify an existing action, select the action, and then click Open.
3. In the Add Filter Action or Configure Filter Action dialog box, specify values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for configuring a content filtering action" as follows (asterisk indicates a required parameter):
   - Action Name*—name
   - Qualifier*—qualifier (Determines which of the following parameters you can configure)
   - Service Name—servicename
   - HeaderName:Value—value
   - Response Code—respcode
   - Response Page—page
4. Fill in any other required information. For example, if you are configuring an action to send an HTTP error code, you must choose the appropriate error code from a drop-down list. If necessary, you can then modify the text of the error message, which is displayed beneath the drop-down list.
5. Click Create or OK, and then click Close. The Actions list displays the action you configured, and a message in the status bar indicates that your action has been created.

Configuring a Content Filtering Policy

To implement content filtering, you must configure at least one policy to tell your NetScaler appliance how to distinguish the connections you want to filter. You must first have configured at least one filtering action, because when you configure a policy, you associate it with an action.

Content filtering policies examine a combination of one or more of the following elements to select requests or responses for filtering:

URL

The URL in the HTTP request.

URL query

Only the query portion of the URL, which is the portion after the query (?) symbol.

URL token

Only the tokens in the URL, if any, which are the parts that begin with an ampersand (&) and consist of the token name, followed by an equals sign (=), followed by the token value.

HTTP method

The HTTP method used in the request, which is usually GET or POST, but can be any of the eight defined HTTP methods.

HTTP version

The HTTP version in the request, which is usually HTTP 1.1.

Standard HTTP header

Any of the standard HTTP headers defined in the HTTP 1.1 specification.

Standard HTTP header value

The value portion of the HTTP header, which is the portion after the colon and space (:).

Custom HTTP header

A non-standard HTTP header issued by your Web site or that appears in a user request.

Custom header value

The value portion of the custom HTTP header, which (as with the standard HTTP header) is the portion after the colon and space (:).

Client Source IP

The IP from which the client request was sent.

Content filtering policies use the simpler of two NetScaler expressions languages, called classic expressions. For a complete description of classic expressions, how they work, and how to configure them manually, see "Policies and Expressions."

Note: Users who are not experienced in configuring policies at the NetScaler command line will usually find using the configuration utility considerably easier.

To configure a content filtering policy by using the command line interface

At the command prompt, type the following commands to configure a content filtering policy and verify the configuration:

- add filter policy <name> -rule <expression> (-reqAction <action> | -resAction <string>
- show filter policy <name>

Example

```
> add filter policy cf-pol -rule "REQ.HTTP.URL CONTAINS http://abc.com" -reqaction DROP
 Done
> show filter policy cf-pol
1)     Name: cf-pol    Rule: REQ.HTTP.URL CONTAINS http://abc.com
       Request action: DROP
       Response action:
       Hits: 0
 Done
```

Parameters for configuring a content filtering policy

name

A name for the filtering action. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should chose a name that helps identify the type of action. (Cannot be changed after the action has been created.)

rule

A NetScaler classic expression that describes the connections you want to select using this policy.

reqaction or resaction

Type -reqaction if your policy applies to requests, or -resaction if your policy applies to responses. You must choose one or the other, but not both.

action

The name of the content filtering action you want to perform on connections that match this policy.

To configure a content filtering policy by using the configuration utility

1. In the details pane, to create a new policy, click Add.

2. If you are creating a new policy, in the Create Filter Policy dialog box, in the Filter Name text box, type a name for your new policy.

3. Select either Request Action or Response Action to activate the drop-down list to the right of that item.

4. Click the down arrow to the right of the drop-down list and select the action to be performed on the request or response. The default choices are RESET and DROP. Any other actions you have created will also appear in this list.

   Note: You can also click New to create a new Content Filtering action, or Modify to modify an existing Content Filtering action. You can only modify actions you created; the default actions are read-only.

5. If you want to use a predefined expression (or named expression) to define your policy, choose one from the Named Expressions list.

   a. Click the down arrow to the right of the first Named Expressions drop-down list, and choose the category of named expressions that contains the named expression you want to use.

   b. Click the down arrow to the right of the second Named Expressions drop-down list, and choose the named expression you want. As you choose a named expression, the regular expression definition of that named expression appears in the Preview Expression pane beneath the Named Expression list boxes.

   c. Click Add Expression to add that named expression to the Expression list.

   Note: You should perform either this step or step 7, but not both.

6. If you want to create a new expression to define your policy, use the Expression Editor.

   a. Click the Add button. The Add Expression dialog box appears.

   b. In the Add Expression dialog box, choose the type of connection you want to filter. The Flow Type is set to REQ by default, which tells the NetScaler appliance to look at incoming connections, or requests. If you want to filter outgoing connections (responses), you click the right arrow beside the drop-down list and choose RES.

   c. If the Protocol is not already set to HTTP, click the down arrow to the right of the Protocol drop-down list and choose HTTP.

      Note: In the NetScaler classic expressions language, “HTTP” includes HTTPS requests, as well.

   d. Click the down arrow to the right of the Qualifier drop-down list, and then choose a qualifier for your expression. Your choices are:

      METHOD

The HTTP method used in the request.

URL

The contents of the URL header.

URLTOKENS

The URL tokens in the HTTP header.

VERSION

The HTTP version of the connection.

HEADER

The header portion of the HTTP request.

URLLEN

The length of the contents of the URL header.

URLQUERY

The query portion of the contents of the URL header.

URLQUERYLEN

The length of the query portion of the URL header.

The contents of the remaining list boxes change to the choices appropriate to the Qualifier you pick. For example, if you choose HEADER, a text field labeled Header Name* appears below the Flow Type list box.

e. Click the down arrow to the right of the Operator drop-down list, and choose an operator for your expression. Your choices will vary depending on the Protocol you chose in the preceding step. The following list includes all of the operators:

==

Matches the following text string exactly.

!=

Does not exactly match the following text string.

>

Is greater than the following integer.

CONTAINS

Contains the following text string.

CONTENTS

The contents of the designated header, URL, or URL query.

EXISTS

The specified header or query exists.

NOTCONTAINS

Does not contain the following text string.

NOTEXISTS

The specified header or query does not exist.

f. If the Value text box is visible, type the appropriate string or number. If you are testing a string in any way, type the string into the Value text box. If you are testing an integer in any way, type the integer into the Value text box.

g. If you chose HEADER as the Protocol, type the header you want in the Header Name* text box.

h. Click OK to add your expression to the Expressions list.

i. Repeat steps B through H to create any additional expressions you want for your profile.

j. Click Close to close the Expressions Editor.

7. If you created a new expression, in the Expression frame select an option from the Match Any Expression drop-down list. Your choices are:

- Match Any Expression. If a request matches any expression in the Expressions list, the request matches this policy.

- Match All Expressions If a request matches all expressions in the Expressions list, the request matches this policy. If it does not matchall of them, it does not match this policy.

- Tabular Expression Switches the Expressions list to a tabular format with three columns. In the first column you can place a BEGIN [(] operator. The second column contains the expressions you have selected or created. In the third column, you can place any of the other operators in the following list, to create complex policy groups in which each group can be configured for match any expression or match all expressions.
- The AND [&&] operator tells the appliance to require that are quest match both the current expression and the following expression.

- The OR [||] operator tells the appliance to require that arequest match either the current expression or the following expression, or both. Only if the request does not match either expression does it not match the policy.

- The END [)] operator tells the appliance that this is the last expression in this expression group or policy.

Note: The Tabular format allows you to create a complex policy that contains both “Match Any Expression” and “Match All Expressions” on a per-expression

basis. You are not limited to just one or the other.

- Advanced Free-Form Switches off the Expressions Editor entirely and modifies the Expressions list into a text area. In the text area, you can type the PCRE-format regular expression of your choice to define this policy. This is both the most powerful and the most difficult method of creating a policy, and is recommended only for those thoroughly familiar with the NetScaler appliance and PCRE-formatregular expressions.

  Caution: If you switch to Advanced Free Form expression editing mode, you cannot switch back to any of the other modes. Do not choose this expression editing mode unless you are sure that is what you want.

8. Repeat steps 6 through 8 to add any additional expressions you want to the Expressions list. You can mix named expressions and expressions created in the Expressions Editor. To the NetScaler appliance, they are all the same.

9. Click Create to create your new policy. Your new policy appears in the Policies pane list.

10. Click Close. To create additional Content Filtering policies, repeat the previous procedure. To remove a Content Filtering policy, select the policy in the Policies tab and click Remove.

Binding a Content Filtering Policy

You must bind each content filtering policy to put it into effect. You can bind policies globally or to a particular virtual server. Globally bound policies are evaluated each time traffic directed to any virtual server matches the policy. Policies bound to a specific vserver are evaluated only when that vserver receives traffic that matches the policy.

To bind a policy to a virtual server by using the command line interface

At the command prompt, type the following commands to bind a policy to a virtual server and verify the configuration:

- bind lb vserver <name>@ -policyName <string> -priority <positive_integer>
- show lb vserver <name>

Example

```
> bind lb vserver vs-loadbal -policyName policyTwo -priority 100
 Done
> show lb vserver vs-loadbal
1)      vs-loadbal (10.102.29.20:80) - HTTP      Type: ADDRESS
        State: OUT OF SERVICE
        Last state change was at Wed Aug 19 09:05:47 2009 (+211 ms)
        Time since last state change: 2 days, 00:58:03.260
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

 Done
```

To globally bind a policy by using the command line interface

At the command prompt, type the following commands to globally bind a policy and verify the configuration:

- bind filter global (<policyName> [-priority <positive_integer>]) [-state (ENABLED | DISABLED)]
- show filter global

Example

```
bind filter global cf-pol -priority 1
Done show filter global
1)      Policy Name: cf-pol     Priority: 1
Done
```

To bind a policy to a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing and click Virtual Servers.
2. In the details pane, select the virtual server to which you want to bind the content filtering policy from the list, and click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, select the Policies tab, and then select the check box in the Active column of the filter policy that you want to bind to the virtual server.
4. Click OK. The policies you have bound display a check mark and the word Yes in the Policies Bound column of the Policies tab.

To globally bind a policy by using the configuration utility

1. In the navigation pane, expand Protection Features, and then select Filter.
2. In the details pane, in the Policies tab, select the policy that you want to bind, and then click Global Bindings.
3. In the Bind/Unbind Filter Policies dialog box, in the Policy Name drop-down list, select a policy, and then click Add. The policy is added to the Configured list.

   Note: To select multiple policies from the list, press and hold the Ctrl key, then click each policy you want.
4. Click OK, and then click Close. The policies you have bound display a check mark and the word Yes in the Globally Bound column of the Policies tab.

Configuring Content Filtering for a Commonly Used Deployment Scenario

This example provides instructions for using the configuration utility to implement a content filtering policy in which, if a requested URL contains root.exe or cmd.exe, the content filtering policy filter-CF-nimda is evaluated and the connection is reset.

To configure this content filtering policy, you must do the following:

- Enable content filtering
- Configure content filtering policy
- Bind content filtering policy globally or to a virtual server
- Verify the configuration

Note: Since this example uses a default content filtering action, you do not need to create a separate content filtering action.

To enable content filtering

1. In the navigation pane, expand System, and click Settings.
2. In the details pane, under Modes & Features, click Change Basic Features.
3. In the Configure Basic Features dialog box, select the Content Filtering check box, and then click OK.
4. In the Enable/Disable feature(s) dialog box, click Yes. A message appears in the status bar, stating that the selected feature is enabled.

To configure the content filtering policy filter-CF-nimda

1. In the navigation pane, expand Protection Features, and click Filter.
2. In the details pane, click Add. The Create Filter Policy dialog box appears.
3. In the Create Filter Policy dialog box, in the Filter Name text box, type the name `filter-CF-nimda`.
4. Select the Request Action option, and in the drop-down list, select RESET.
5. In the Expression frame, select Match Any Expression from the drop-down list, and then click Add.
6. In the Add Expression dialog box, Expression Type drop-down list, select General.
7. In the Flow Type drop-down list, select REQ.
8. In the Protocol drop-down list, select HTTP.
9. In the Qualifier drop-down list, select URL.
10. In the Operator drop-down list, select CONTAINS.
11. In the Value text box, type `cmd.exe`, and then click OK. The expression is added in the Expression text box.
12. To create another expression, repeat Steps 7 through 11, but in the Value text box, type `root.exe`. Then click OK, and finally click Close.
13. Click Create on the Create Filter Policy dialog box. The filter policy filter-CF-nimda appears in the Filter list.
14. Click Close.

To globally bind the content filtering policy

1. In the navigation pane, expand Protection Features, and click Filter. The Filter page appears in the right pane.
2. In the details pane, Policies tab, select the policy that you want to bind and click Global Bindings. The Bind/Unbind Filter Policies dialog box appears.
3. In the Bind/Unbind Filter Policies dialog box, in the Policy Name drop-down list, select the policy filter-CF-nimda, and click Add. The policy is added to the Configured list.
4. Click OK, and then click Close. The policy you have bound displays a check mark and Yes in the Globally Bound column of the Policies tab.

To bind the content filtering policy to a virtual server

1. In the navigation pane, expand the Load Balancing node and click Virtual Servers.
2. In the details pane virtual servers list, select vserver-CF-1 to which you want to bind the content filtering policy and click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, select the Policies tab.
4. In the Active column, select the check box for the policy filter-CF-nimda, and then click OK. Your content filtering policy is now active, and should be filtering requests. If it is functioning correctly, the Hits counter is incremented every time there is a request for a URL containing either root.exe or cmd.exe. This allows you to confirm that your content filtering policy is working. The content filtering policy is bound to the virtual server.

To verify the content filtering configuration by using the command line interface

At the command prompt, type the following command to verify the content filtering configuration:

show filter policy filter-CF-nimda

Example

```
sh filter policy filter-CF-nimda
      Name: filter-CF-nimda   Rule: REQ.HTTP.URL CONTAINS cmd.exe || REQ.HTTP.URL CONTAINS root.exe
      Request action: RESET
      Response action:
      Hits: 0
Done
```

Note: The Hits counter displays an integer that denotes the number of times the `filter-CF-nimda` policy is evaluated. In the preceding steps, the Hits counter is set to zero because no requests for a URL containing either cmd.exe or root.exe have been made yet. If you want to see the counter increment in real time, you can simply request a URL that contains either of these strings.

To verify the content filtering configuration by using the configuration utility

1. In the navigation pane, expand Protection Features, and click Filter.
2. In the details pane, select the filter policy filter-CF-nimda. The bottom of the pane should display the following:

   Request Action:

   RESET

   Rule:

   REQ.HTTP.URL CONTAINS cmd.exe || REQ.HTTP.URL CONTAINS root.exe

   Hits:

   0

HTTP Denial-of-Service Protection

Internet hackers can bring down a site by sending a surge of GET requests or other HTTP-level requests. HTTP Denial-of-Service (HTTP Dos) Protection provides an effective way to prevent such attacks from being relayed to your protected Web servers. The HTTP DoS feature also ensures that a NetScaler appliance located between the internet cloud and your Web servers is not brought down by an HTTP DoS attack.

Most attackers on the Internet use applications that discard responses to reduce computation costs, and minimize their size to avoid detection. The attackers focus on speed, devising ways to send attack packets, establish connections or send HTTP requests as rapidly as possible.

Real HTTP clients such as Internet Explorer, Firefox, or NetScape browsers can understand HTML Refresh meta tags, Java scripts, and cookies. In standard HTTP the clients have most of these features enabled. However, the dummy clients used in DoS attacks cannot parse the response from the server. If malicious clients attempt to parse and send requests intelligently, it becomes difficult for them to launch the attack aggressively.

When the NetScaler appliance detects an attack, it responds to a percentage of incoming requests with a Java or HTML script containing a simple refresh and cookie. (You configure that percentage by setting the Client Detect Rate parameter.) Real Web browsers and other Web-based client programs can parse this response and then resend a POST request with the cookie. DoS clients drop the NetScaler appliance's response instead of parsing it, and their requests are therefore dropped as well.

Even when a legitimate client responds correctly to the NetScaler appliance's refresh response, the cookie in the client's POST request may become invalid in the following conditions:

- If the original request was made before the NetScaler appliance detected the DoS attack, but the resent request was made after the appliance had come under attack.
- When the client's think time exceeds four minutes, after which the cookie becomes invalid.

Both of these scenarios are rare, but not impossible. In addition, the HTTP DoS protection feature has the following limitations:

- Under an attack, all POST requests are dropped, and an error page with a cookie is sent.
- Under an attack, all embedded objects without a cookie are dropped, and an error page with a cookie is sent.

The HTTP DoS protection feature may affect other NetScaler features. Using DoS protection for a particular content switching policy, however, creates additional overhead because the policy engine must find the policy to be matched. There is some overhead for SSL requests due to SSL decryption of the encrypted data. Because most attacks are not on a secure network, though, the attack is less aggressive.

If you have implemented priority queuing, while it is under attack a NetScaler appliance places requests without proper cookies in a low-priority queue. Although this creates overhead, it protects your Web servers from false clients. HTTP DoS protection typically has minimal effect on throughput, since the test JavaScript is sent for a small percentage of requests only. The latency of requests is increased, because the client must re-issue the request after it receives the JavaScript. These requests are also queued

To implement HTTP DoS protection, you enable the feature and define a policy for applying this feature. Then you configure your services with the settings required for HTTP DoS. You also bind a TCP monitor to each service and bind your policy to each service to put it into effect.

Layer 3-4 SYN Denial-of-Service Protection

Any NetScaler appliance with system software version 8.1 or later automatically provides protection against SYN DoS attacks.

To mount such an attack, a hacker initiates a large number of TCP connections but does not respond to the SYN-ACK messages sent by the victimized server. The source IP addresses in the SYN messages received by the server are typically spoofed. Because new SYN messages arrive before the half-open connections initiated by previous SYN messages time out, the number of such connections increases until the server no longer has enough memory available to accept new connections. In extreme cases, the system memory stack can overflow.

A NetScaler appliance defends against SYN flood attacks by using SYN cookies instead of maintaining half-open connections on the system memory stack. The appliance sends a cookie to each client that requests a TCP connection, but it does not maintain the states of half-open connections. Instead, the appliance allocates system memory for a connection only upon receiving the final ACK packet, or, for HTTP traffic, upon receiving an HTTP request. This prevents SYN attacks and allows normal TCP communications with legitimate clients to continue uninterrupted.

SYN DoS protection on the NetScaler appliance ensures the following:

- The memory of the NetScaler is not wasted on false SYN packets. Instead, memory is used to serve legitimate clients.
- Normal TCP communications with legitimate clients continue uninterrupted, even when the Web site is under SYN flood attack.

In addition, because the NetScaler appliance allocates memory for HTTP connection state only after it receives an HTTP request, it protects Web sites from idle connection attacks.

SYN DoS protection on your NetScaler appliance requires no external configuration. It is enabled by default.

Enabling HTTP DoS Protection

To configure HTTP DoS protection, you must first enable the feature.

To enable HTTP DoS protection by using the command line interface

At the command prompt, type the following commands to enable HTTP DoS protection and verify the configuration:

- enable ns feature HttpDoSProtection
- show ns feature

Example

```
> enable ns feature HttpDoSProtection
 Done
> show ns feature

      Feature                 Acronym          Status
      -------                 -------          ------
 1)   Web Logging               WL               ON
 2)   Surge Protection          SP               OFF
 .
 .
 .
 10)  Global Server Load Balancing  GSLB            ON
 11)  Http DoS Protection        HDOSP            ON
 12)  Content Filtering          CF               ON
 .
 .
 23)  HTML Injection             HTMLInjection    ON
 24)  NetScaler Push             push             OFF
 Done
>
```

To enable HTTP DoS protection by using the configuration utility

1. Navigate to System > Settings.
2. In the details pane, click Configure Advanced Features.
3. In the Configure Advanced Features dialog box, select the HTTP DoS Protection check box.
4. Click OK.

Defining an HTTP DoS Policy

After you enable HTTP DoS protection, you next create a policy.

Note: Before changing the default setting for Client Detect Rate, see "Tuning the Client Detection/JavaScript Challenge Response Rate."

To configure a HTTP DoS policy by using the command line interface

At the command prompt, type one of the following commands to configure an HTTP DoS policy and verify the configuration:

- add dos policy <name> -qDepth <positive_integer> [-cltDetectRate <positive_integer>]
- set dos policy <name> -qDepth <positive_integer> [-cltDetectRate <positive_integer>]

Example

```
> add dos policy pol-HTTP-DoS  -qDepth 30
 Done
> set dos policy pol-HTTP-DoS  -qDepth 40
 Done
> show dos policy
1)      Policy: pol-HTTP-DoS    QDepth: 40
 Done
>
```

Parameters for defining an HTTP DoS policy

name

A name for your HTTP DoS policy. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should chose a name that helps identify the type of action.

qdepth

An integer that represents the maximum number of connections that can be placed in the queue at one time.

cltDetectRate

An integer that represents the percentage of traffic to which the HTTP DoS policy should be applied.

To configure an HTTP DoS policy by using the configuration utility

1. Navigate to Protection Features > HTTP DoS.
2. In the details pane, do one of the following:
   - To create a new policy, click Add.
   - To modify an existing policy, select the policy, and then click Open.
3. In the Create HTTP DoS Policy or Configure HTTP DoS Policy dialog box, specify values for the parameters. The contents of the dialog box correspond to the parameters described in "Parameters for defining an HTTP DoS policy" as follows (asterisk indicates a required parameter):
   - Name*—name (You cannot change the name of an existing policy.)
   - QDepth*—qdepth
   - Client Detect Rate—cltDetectRate (Before changing the default setting for cltDetectRate, see "Tuning the Client Detection/JavaScript Challenge Response Rate.")
4. Click OK to create your new policy. The policy that you created appears in the details pane, and the status bar displays a message indicating that the DoS policy is successfully configured.

Configuring an HTTP DoS Service

After you configure an HTTP DoS policy, you must configure a service for your policy. The service accepts HTTP traffic that is protected by the HTTP DoS policy.

To configure an HTTP DoS service by using the command line interface

At the command prompt, type one of the following commands to configure an HTTP DoS service and verify the configuration:

- add service <name>@ (<IP>@ | <serverName>@) HTTP <port> [-maxClient <positive_integer>] [-maxReq <positive_integer>] -state ENABLED
- set service <name>@ (<IP>@ | <serverName>@) HTTP <port> [-maxClient <positive_integer>] [-maxReq <positive_integer>] -state ENABLED

Example

```
> add service ser-HTTP-Dos1 10.102.29.40 HTTP 87
 Done
> set service ser-HTTP-Dos1 -maxReq 20
 Done
> show service
1)      srv-http-10 (10.102.29.30:80) - HTTP
        State: DOWN
        Last state change was at Wed Jul  8 07:49:52 2009
        Time since last state change: 34 days, 00:48:18.700
        Server Name: 10.102.29.30
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 180 sec   Server: 360 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED
         .
         .
         .
5)      ser-HTTP-Dos1 (10.102.29.40:87) - HTTP
```

```
        State: DOWN
        Last state change was at Tue Aug 11 08:23:40 2009
        Time since last state change: 0 days, 00:14:30.300
        Server Name: 10.102.29.40
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 20     Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): YES
        Idle timeout: Client: 180 sec   Server: 360 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED
 Done
>
```

Parameters for configuring an HTTP DoS service

name

A name for your service. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should chose a name that helps identify the traffic this service will handle.

IP

The IP of the server that the service represents.

serverName

The FQDN of the server that the service represents.

port

The port on which your service will listen. This is normally port 80 (for HTTP) or port 443 (for HTTPS).

maxClient

The maximum number of clients.

maxReq

The maximum number of requests that can be sent on a persistent connection to the service.

state

The state of the service after it is added.

To configure an HTTP DoS service by using the configuration utility

1. Navigate to Load Balancing > Services.
2. In the details pane, do one of the following:
   - To create a new service, click Add.
   - To modify an existing service, select the service, and then click Open.
3. In the Create Server or Configure Server dialog box, specify values for the following parameters, which correspond to the descriptions in "Parameters for configuring an HTTP DoS service" as follows (asterisk indicates a required parameter):
   - Service Name*—name (You cannot change the name of an existing service.)
   - Server*—IP or serverName (Specify one or the other, not both.)
   - Port*—port
4. If the Enable Service check box is not selected, select it.
5. Select the Advanced tab, and select the Override Global check box to enable those choices.
6. Specify values for the following parameters.
   - Max Clients*—maxClient
   - Max Requests*—maxReq
7. Click Create or OK, and then click Close. The service appears in the list of services.

Binding an HTTP DoS Monitor and Policy

To put HTTP DoS protection into effect after you have configured an HTTP DoS service, you must bind the monitor, and then bind the service to the HTTP DoS policy.

To bind the monitor to the service by using the command line interface

At the command prompt, type the following commands to bind the monitor to the service and verify the configuration:

- bind lb monitor <monitorName> <serviceName>
- show lb monitor

Example

```
> bind lb monitor tcp ser-HTTP-DoS
 Done
> show lb monitor
1)  Name.......:  ping-default  Type......:    PING   State....ENABLED
2)  Name.......:   tcp-default  Type......:     TCP   State....ENABLED
3)  Name.......:        ping  Type......:    PING   State....ENABLED
4)  Name.......:         tcp  Type......:     TCP   State....ENABLED
5)  Name.......:        http  Type......:    HTTP   State....ENABLED
 .
 .
 .
17)  Name.......:     ldns-dns  Type......: LDNS-DNS   State....ENABLED
 Done
```

To bind the policy to the service by using the command line interface

At the command prompt, type the following commands to bind the policy to the service and verify the configuration:

bind service <serviceName> -policyName <policyname>

Example

```
> bind service ser-HTTP-DoS -policyName pol-HTTP-DoS
```

```
 Done
> show service
1)    srv-http-10 (10.102.29.30:80) - HTTP
      State: DOWN
      Last state change was at Wed Jul  8 07:49:52 2009
      Time since last state change: 34 days, 01:24:58.510
      Server Name: 10.102.29.30
      Server ID : 0   Monitor Threshold : 0
      Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
      Use Source IP: NO
      Client Keepalive(CKA): NO
      Access Down Service: NO
      TCP Buffering(TCPB): NO
      HTTP Compression(CMP): NO
      Idle timeout: Client: 180 sec   Server: 360 sec
      Client IP: DISABLED
      Cacheable: NO
      SC: OFF
      SP: ON
      Down state flush: ENABLED
      .
      .
      .
4)    ser-HTTP-Dos (10.102.29.18:88) - HTTP
      State: DOWN
      Last state change was at Tue Aug 11 08:19:45 2009
      Time since last state change: 0 days, 00:55:05.40
      Server Name: 10.102.29.18
      Server ID : 0   Monitor Threshold : 0
      Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
      Use Source IP: NO
      Client Keepalive(CKA): NO
      Access Down Service: NO
      TCP Buffering(TCPB): NO
      HTTP Compression(CMP): YES
      Idle timeout: Client: 180 sec   Server: 360 sec
      Client IP: DISABLED
      Cacheable: NO
      SC: OFF
      SP: ON
      Down state flush: ENABLED
5)    ser-HTTP-Dos1 (10.102.29.40:87) - HTTP
      State: DOWN
      Last state change was at Tue Aug 11 08:23:40 2009
      Time since last state change: 0 days, 00:51:10.110
      Server Name: 10.102.29.40
      Server ID : 0   Monitor Threshold : 0
      Max Conn: 0     Max Req: 20     Max Bandwidth: 0 kbits
      Use Source IP: NO
      Client Keepalive(CKA): NO
      Access Down Service: NO
      TCP Buffering(TCPB): NO
      HTTP Compression(CMP): YES
      Idle timeout: Client: 180 sec   Server: 360 sec
      Client IP: DISABLED
      Cacheable: NO
```

```
        SC: OFF
        SP: OFF
        Down state flush: ENABLED
 Done
>
```

To bind the monitor and policy to the service by using the configuration utility

1. Navigate to Load Balancing > Services.
2. In the details pane, select the service that you want to bind, and then click Open.
3. In the Configure Service dialog box, select the Monitor tab, click the name of the monitor you want in the Monitors list, and then click Add. The selected monitor is added to the Configured frame.
4. Select the Policies tab, then select the HTTP DoS tab.
5. Select a policy from the Available Policies list, and then click Add. The policy appears in the Configured Policies list.
6. Click OK, and then click Close. A message appears in the status bar, stating that the service has been configured.

Tuning the Client Detection/JavaScript Challenge Response Rate

After you have enabled and configured HTTP DoS protection, if more than the maximum specified number of clients are waiting in the NetScaler surge queue for the HTTP DoS service, the HTTP DoS protection function is triggered. The default rate of challenged JavaScript responses sent to the client is one percent of the server response rate. The default response rate is inadequate in many real attack scenarios, however, and may need to be tuned.

For example, assume that the Web server is capable of a maximum of 500 responses/sec, but is receiving 10,000 Gets/sec. If 1% of the server responses are sent as JavaScript challenges, responses are reduced to almost none: 5 client (500 *0.01) JavaScript responses, for 10000 waiting client requests. Only about 0.05% of the real clients receive JavaScript challenge responses. However, if the client detection/JavaScript challenge response rate is very high (for example, 10%, generating 1000 challenge JavaScript responses per second), it may saturate the upstream links or harm the upstream network devices. Exercise care when modifying the default **Client Detect Rate** value.

If the configured triggering surge queue depth is, for example, 200, and the surge queue size is toggling between 199 and 200, the NetScaler toggles between the “attack” and “no-attack” modes, which is not desirable. The HTTP DoS feature includes a window mechanism is provided. When the surge queue size reaches the designated queue depth value, triggering “attack” mode, the surge queue size must fall for the NetScaler to enter “no-attack” mode. In the scenario just described, if the value of WINDOW_SIZE is set to 20, the surge queue size must fall below 180 before the NetScaler enters “no-attack” mode. During configuration, you must specify a value more than the WINDOW_SIZE for the **QDepth** parameter when adding a DoS policy or setting a DoS policy.

The triggering surge queue depth should be configured on the basis of previous observations of traffic characteristics. For more information about setting up a correct configuration, see "Guidelines for HTTP DoS Protection Deployment."

Guidelines for HTTP DoS Protection Deployment

Citrix recommends you to deploy the HTTP DoS protection feature in a tested and planned manner and closely monitor its performance after the initial deployment. Use the following information to fine-tune the deployment of HTTP DoS Protection.

- The maximum number of concurrent connections supported by your servers.
- The average and normal values of the concurrent connections supported by your servers.
- The maximum output rate (responses/sec) that your server can generate.
- The average traffic that your server handles.
- The typical bandwidth of your network.
- The maximum bandwidth available upstream.
- The limits affecting bandwidth (such as external links, a particular router, or other critical devices on the path that may suffer from a traffic surge).
- Whether allowing a greater number of clients to connect is more important than protecting upstream network devices.

To determine the characteristics of a HTTP DoS attack, you should consider the following issues.

- What is the rate of incoming fake requests that you have experienced in the past?
- What types of requests have you received (complete posts, incomplete gets)?
- Did previous attacks saturate your downstream links? If not, what was the bandwidth?
- What types of source IP addresses and source ports did the HTTP requests have (e.g., IP addresses from one subnet, constant IP, ports increasing by one).
- What types of attacks do you expect in future? What type have you seen in the past?
- Any or all information that can help you tune DoS attack protection.

Priority Queuing

The priority queuing feature lets you filter incoming HTTP traffic on the basis of categories that you create and define, and prioritize those HTTP requests accordingly. Priority queuing directs high-priority requests to the server ahead of low-priority requests, so that users who need resources for important business uses receive expedited access to your protected Web servers.

Note: The priority queuing feature is not supported in NetScaler 9.2 nCore.

To implement priority queuing, you create priority queuing policies that specify a priority, weight, threshold, and implicit action. When an incoming request matches a priority queuing policy, the request is processed as the associated action indicates. For example, you can create a priority queuing policy that places all matching requests above a certain threshold in a surge queue, while giving priority treatment to other requests.

You can bind up to three priority queuing policies to a single load balancing virtual server. The priority levels are:

Level 1

A Level 1 policy processes priority requests.

Level 2

A Level 2 policy processes requests that should receive responses as soon as Level 1 requests have been cleared from the queue.

Level 3

A Level 3 policy processes non-priority requests that receive responses only after requests in the first two queues have been cleared.

You can use weighted queuing to adjust the relative priority of each of these queues. Weights can range from 0 to 101. A weight of 101 tells the NetScaler appliance to clear all requests in that queue before forwarding any requests in the lower-priority queues to the Web server. A weight of 0 tells the appliance to send requests in that queue to the Web server only when there are no requests waiting in any of the other queues.

You must assign a unique name to each priority queuing policy. Policy names can be up to 127 characters. Multiple policies bound to the same load balancing virtual server cannot have the same priority level. No two virtual servers that have one or more common underlying physical services can have priority queuing configured or enabled on both virtual servers simultaneously.

To configure priority queuing the NetScaler, you perform the following steps:

- Enable the load balancing feature
- Define a server and service
- Define a load balancing virtual server

- Bind the service to the load balancing virtual server
- Enable the priority queuing feature
- Create the priority queuing policies
- Bind the priority queuing policies to the load balancing virtual server
- Enable priority queuing on load balancing virtual server

For information about enabling load balancing, creating servers, creating virtual servers and services, and binding these servers and services, see the *Citrix NetScaler Traffic Management Guide* at http://support.citrix.com/article/CTX132359. For complete information about policies and expressions, see the *Citrix NetScaler Policy Configuration and Reference Guide* at http://support.citrix.com/article/CTX132362.

Enabling Priority Queuing

To use the priority queuing feature the NetScaler appliance, you must first enable it.

To enable priority queuing by using the command line interface

At the command prompt, type the following commands to enable priority queuing and verify the configuration:

- enable ns feature PriorityQueuing
- show ns feature

Example

```
> enable ns feature PriorityQueuing
 Done
> show ns feature

      Feature                 Acronym           Status
      -------                 -------           ------
1)    Web Logging               WL               ON
2)    Surge Protection          SP               OFF
3)    Load Balancing            LB               ON
.
.
.
8)    Priority Queuing          PQ               ON
.
23)   HTML Injection            HTMLInjection    ON
24)   NetScaler Push            push             OFF
Done
```

To enable priority queuing by using the configuration utility

1. Navigate to System > Settings.
2. In the details pane, click Configure advanced features.
3. In the Configure Advanced Features dialog box, select the Priority Queuing check box.
4. Click OK.

Configuring a Priority Queuing Policy

To configure a priority queuing policy, you can use either the configuration utility or the command line.

Note: For more information about using the command line, see "Command Reference."

To configure a priority queuing policy by using the command line interface

At the command prompt, type the following command to configure a priority queuing policy and verify the configuration:

add pq policy <policyName> -rule <expression> -priority <positive_integer> [-weight <positive_integer>] [-qDepth <positive_integer> | -polqDepth <positive_integer>]

Example

```
> add pq policy pol_cgibin -rule "URL == '/cgi-bin/'" -priority 1
 Done
> show pq policy pol_cgibin
1)      Policy: pol_cgibin      Rule: URL == '/cgi-bin/'        Priority: 1     Weight: 10
        Hits: 0
 Done
```

Parameters for configuring a priority queuing policy

policyName

A name for your priority queuing policy. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should chose a name that helps identify the type of action.

rule

An expression that tells the policy which connections it should handle. For complete information about policy expressions, "Policies and Expressions."

priority

An integer from 1 to 3 that represents the priority queue that connections matching this policy should be placed in.

weight

An integer from 1 to 101 that represents the weight assigned to this priority queuing policy. For detailed information about the meaning and uses of different policy weights, see "Setting Up Weighted Queuing."

qDepth

An integer that represents the maximum number of connections that can be placed in the queue at one time.

polqDepth

An integer that represents the total number of waiting clients or requests belonging to the policy.

To configure a priority queuing policy by using the configuration utility

1. Navigate to Protection Features > Priority Queuing.
2. In the details pane, do one of the following:
   - To create a new policy, click Add.
   - To modify an existing policy, select the policy, and then click Open.
3. If you are creating a new policy, in the Create PQ Policy dialog box, in the Name text box, type a name for your new policy.

   The name can consist of from one to 127 letters, numbers and the hyphen and underscore symbol.

   If you are modifying an existing policy, skip this step. You cannot change the name of an existing policy.

4. In the Rule text box, either enter the policy expression directly, or click New to create a policy expression. If you click New, perform the following steps:

   a. In the Create Expression dialog box, click Add.

   b. In the Add Expression dialog box, leave Expression Type set to `General`, and in the Flow Type drop-down list, select a Flow Type. Your choices are REQ (for requests) and RES (for responses).

   c. In the Protocol drop-down list, select a protocol. If you selected REQ in the previous step, your choices are HTTP (Web-based connections), SSL (secure Web connections), TCP and IP. If you selected RES in the previous step, your choices are HTTP, TCP and IP.

   d. In the Qualifier drop-down list, select a qualifier.

      Your choices depend upon your selections in the previous step. Common choices are HTTP VERSION (the version of the HTTP connection), HTTP HEADER (the specified HTTP header), TCP SOURCEPORT/ DESTPORT (the source or destination port of a TCP connection), and IP SOURCEIP/DESTIP (the source or destination IP of the connection).

      If you choose HTTP HEADER, the Header text box appears beneath the original row of text boxes. You fill in the name of the HTTP header you want.

      For a complete description of the available choices, see "Policies and Expressions."

   e. In the Operator drop-down list, select an operator.

      For a complete description of the available choices, see "Policies and Expressions."

   f. In the Value text box, type the value you want to test for.

      This may be a text string or a number, depending upon the context. For a complete description of values appropriate to the specific context, see "Policies and

Expressions."

g. Click OK. The expression is added in the Expression text box.

h. Click Create. The expression appears in the Rule text box.

5. In the Priority and Weight text boxes, type numeric values, for example, 1 and 30. For more information about Priority and Weight, see "Setting Up Weighted Queuing."

6. Enter a numeric value for either Queue Depth or Policy Queue Depth, for example 234, and click Create.

   - Queue Depth Defines the total number of waiting clients or requests on the virtual server to which the policy is bound.

   - Policy Queue Depth Defines the total number of waiting clients or requests belonging to the policy.

   The policy is created and appears in the Priority Queuing page.

   Note: To create additional priority queuing policies, repeat the procedure in the preceding section, and click Close after you finish.

Binding a Priority Queuing Policy

After you create a priority queuing policy, you must bind it to the appropriate virtual server to put it into effect.

To bind a priority queuing policy by using the command line interface

At the command prompt, type the following commands to bind a policy and verify the configuration:

- bind lb vserver <name> -policyName <policyname>
- show lb vserver <name>

Example

```
> bind lb vserver lbvip -policyname pol_cgibin
 Done
> show lb vserver lbvip
        lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
        State: DOWN
        Last state change was at Wed Jul 15 05:54:24 2009 (+782 ms)
        Time since last state change: 26 days, 05:44:37.370
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1)      Policy : ns_cmp_msapp Priority:0

1)      Priority Queuing Policy : pol_cgibin
 Done
>
```

To bind a priority queuing policy by using the configuration utility

1. In the navigation pane, locate and select the virtual server to which you want to bind the priority queuing policy.

   - To select a load balancing virtual server, expand Load Balancing > Virtual Servers, then select the load balancing virtual server that you want..

   - To select a content switching virtual server, expand Content Switching > Virtual Servers, then select the content switching virtual server that you want..
2. In the Configure Virtual Server dialog box, select the Policies tab.

3. Click the double right-arrow (») symbol to display the complete list of policy types, and then select Priority Queuing from the drop-down list.

4. Click Insert Policy.

5. In the Policy Name row, select the policy that you want to bind from the drop-down list.

6. ClickOK to save your changes.

Setting Up Weighted Queuing

When priority queuing is implemented, lower-priority requests are typically kept on hold while higher-priority requests are served. The lower-priority requests may therefore be delayed if there is a constant flow of higher-priority requests.

To prevent delays for low-priority requests across multiple priority levels, you can configure weighted queuing for serving requests. The default weights for the priorities are:

- Gold - Priority 1 - Weight 3
- Silver - Priority 2 - Weight 2
- Bronze - Priority 3 - Weight 1

You assign the minimum weight, zero (0), to requests that the NetScaler appliance should send to the server only if no requests are stored in any of the other queues. You assign the maximum weight, 101, to requests that the appliance should send to the server immediately, ahead of any requests stored in any of the other queues. Weights between these two set the relative priority of a particular queue in relation to the other queues. Queues with a higher weight are processed first; queues with a lower weight after the others have been processed. To assign the weights, see "Configuring a Priority Queuing Policy."

Note: The weight assigned to a higher-priority queue must be larger than the weight assigned to a lower-priority queue. For example, the weight assigned to The Gold (Priority 1) queue must be greater than the weight assigned to the Silver (Priority 2) queue.

SureConnect

You can use the SureConnect feature of the Citrix NetScaler appliance to service all incoming connections with either the requested content or a custom Web page that displays information about a delay in the request being serviced.

When servers are overloaded with the requests, the servers might either respond slowly or not at all. The SureConnect feature enables the NetScaler appliance to detect and compensate such conditions by ensuring that every client request gets serviced in some way, such as either a custom Web page or actual content is sent to the client.

SureConnect is activated when the response time or maximum server connections to a client request exceeds a limit that you have set. The SureConnect browser window displays one of the following:

- A progress bar with the amount of time remaining until the requested content will be available.
- Alternate Web content of your choice (alternate page).
- Both a progress bar and alternate page.
- Complete custom content of your choice.

You can configure whether the SureConnect progress bar alone is displayed or both the progress bar and the alternate page are displayed.

When the server becomes responsive again, the original request for content is served. If the user chooses, the alternate content window can remain in focus.

Subsequent requests from the same user within the same session are served immediately. This can be configured using the settings described later in this section.

SureConnect can be activated when a response is delayed, and when the number of user connections to a given URL exceeds a specified threshold.

SureConnect works with all standard browsers, including Microsoft Internet Explorer, Netscape Navigator, and Mozilla Firefox.

SureConnect is advantageous in the following situations:

- **Full server queue**

  The server can respond fast, but there are too many users. This results in the server's queue being full and unable to process additional client requests.

  SureConnect Solution: In this situation, the SureConnect window is displayed, showing the time left until the content will be available. The alternate page is displayed under the progress bar, if an alternate page has been configured.

- **Large response delay**

The server response is slow. Typically, if a Web server does not respond to a client request quickly, the user will leave the site.

SureConnect Solution: When the predicted delay reaches a configured time threshold, the SureConnect window displays the progress bar and the optional alternate page in the client browser.

- **Client time-out**

  When the client requests content from a very slow Web site, a time-out message displays in the client browser, and the content is not delivered. The user may leave the site.

  SureConnect Solution: The appliance stores the request until the server is no longer busy and delivers the requested content to the client.

- **Server experiencing a traffic surge**

  The server typically responds quickly, but the current load of open connections is greater than the server capacity to serve them. Therefore, the server response is delayed.

  SureConnect Solution: A SureConnect window is displayed in the client browser, showing the time left. The alternate page from the server is also displayed if it has been configured.

Installing SureConnect

SureConnect files must be installed on the alternate content server, which can be the same as the primary server.

On a Windows server, extract the sc_xx.exe file (where xx is the build number), or on a UNIX server, extract the sc_xx.tar file (where xx is the build number).

Note: You must install SureConnect in the default Web root directory.

If the alternate content server is the same as the primary server, place the SureConnect and alternate content files in any directory under the Web root directory. Specify this path when you add a policy to configure SureConnect. By default, SureConnect files are installed in the /Citrix NetScaler appliance directory under the default Web root directory.

If the alternate content server is different than the primary server, the SureConnect and alternate content files must be in a unique directory under the Web root directory. By default, this unique directory is the /Citrix NetScaler system directory. Specify this path when you add a policy to configure SureConnect.

The following files are extracted:

- Alternate content files (progressbar.htm, alternatepage.htm, and barandpage.htm)
- System-Logo.gif
- Customer-Logo.gif
- Sample.gif
- README.txt.

Installing on UNIX

This section describes how to install SureConnect alternate content on a UNIX server. The following are the prerequisites:

- The UNIX server is running the Apache server.
- The shell with the # prompt is in use.
- Apache is installed in the default location.
- The sc_xx.tar file is downloaded from the organization's Web site into the /var/ftp/incoming directory.

To install SureConnect

1. At the command prompt, navigate to the htdocs directory:

   cd /usr/local/apache/htdocs

2. Type the following command:

   tar xvpf/var/ftp/incoming/sc_xx.tar

The output from the .tar file is displayed. A /Citrix NetScaler system directory is created under the specified path and the SureConnect files are installed.

Installing on Windows

This section describes how to install SureConnect alternate content on a Windows server. The following are the prerequisites:

- The server is running the Microsoft Internet Information Server.
- The DOS prompt is being used.
- The SureConnect zip (self-extracting) file is downloaded from the organization Web site using FTP into the C:\inetpub\wwwroot directory.

To install SureConnect on Windows

Do one of the following:

- At the command prompt, navigate to the wwwroot directory:

  cd c:\inetpub\wwwroot

- Type the name of the executable file:

  sc_xx.exe

- Double-click the sc_xx.exe icon from the Microsoft Windows Explorer Web browser, extract from the compressed file into the default path (for example, the c:\inetpub\wwwroot directory).

Output from the zip file is displayed. A /Citrix NetScaler system directory is created under the specified path, and the SureConnect files are installed.

Configuring SureConnect

The following topics describe how to configure SureConnect for scenarios involving alternate server failure.

- "Configuring the Response for Alternate Server Failure"
- "Configuring the SureConnect Policies"
- "Customizing the Alternate Content File"
- "Configuring SureConnect for Citrix NetScaler Features"

Configuring the Response for Alternate Server Failure

If the alternate server fails, and the primary server cannot immediately deliver the requested content to the client, SureConnect does not display alternate content from the failed alternate server in the client Web browser.

The Citrix NetScaler appliance automatically sends a response to the client browser. You can customize the server response to display information suited to your needs.

The default response is:

```
Your Request is being processed… Estimated Time: ____ Secs
```

Customizing the Default Response

The NetScaler appliance automatically sends the response to the client if the alternate server fails, or if the appliance is configured to send the default response.

To customize the default response of the appliance, create a vsr.htm file (a sample is provided in this section) as follows:

- The file can contain any valid HTML statements other than embedded objects.
- The file size cannot exceed 800 bytes.
- The file must reside on the NetScaler appliance. If you have a high availability (HA) setup, the file must reside on the primary and secondary nodes. Any changes made to the file on the primary node must also be applied to the file on the secondary node.
- Put vsr.htm file in the /etc directory.

To customize the default response

Change any of the contents between the </HEAD> and </HTML> tags in the vsr.htm file. Following is the sample content from vsr.htm file. The sections that you can edit are in bold text.

HTTP/1.1 200 OK
Server: NS_WS3.0
Content-Type: text/html
Cache-control: no-cache
Pragma: no-cache
Set-Cookie: NSC_BPIP=@@SID@@; path=/
<HTML> <HEAD> <META HTTP-EQUIV="Refresh" CONTENT="0">
</HEAD> **Your request is being processed...**
**
Estimated Delay: @@DELAY@@ Sec ** </HTML>

Note: Include @@DELAY@@ to display the predicted delayed response time in seconds.

SureConnect with In-Memory response (NS action)

When defining the SureConnect policy by using the add sc policy command, you can configure the NetScaler Appliance to serve alternative content to the client.

To enable SureConnect and configure the in-memory response, perform the following tasks:

- Enable the SureConnect feature on the appliance by using the `enable feature SC` command
- Define the services by using the `add service <servicename> <IP address> <servicetype> <port>` command. This identifies the original server for which the SureConnect is configured and the types of services.
- Add a SureConnect policy by using the `add sc policy` command. You can configure a URL-based policy or a rule-based policy. The incoming requests are validated against the URL or rule you specify in the policy.

Note: You can configure the SureConnect feature on a load balancing virtual server. In that case, perform the following additional actions:

- Enable Load Balancing by using the `enable feature LB` command.
- Enable SureConnect feature on the virtual server by using the `set lb vserver <vservername> -sc ON` command.
- Bind services to the virtual server by using the `bind lb vserver <name> <serviceName>` command.
- Bind policies to the virtual server by using the `bind lb vserver <name> -policyname <name>` command.

The following example illustrates how to configure SureConnect for the load balancing feature so that SureConnect will display alternative content from the NetScaler appliance.

In this example, two physical servers, with IP addresses, 10.101.3.187 and 10.101.3.188 are load balanced by the NetScaler appliance. The appliance has one configured virtual server, vs-NSact, whose IP address is 10.101.3.201. The file that contains the alternative content is vsr.htm. It is copied from the file system into system memory. Services are loaded until the SureConnect policy triggers, and the appliance supplies the alternate content.

```
enable feature SC LB
add service psvc1 10.101.3.187 http 80
add service psvc2 10.101.3.188 http 80
add lb vserver vs-NSact HTTP 10.101.3.201 80
bind lb vserver vs-NSact psvc1
bind lb vserver vs-NSact psvc2
```

```
add sc policy policyNS -url /cgi-bin/*.cgi -delay 400000
-action NS
set sc parameter -vsr /nsconfig/ssl/vsr.htm
bind lb vserver vs-NSact -policyName policyNS
set lb vserver vs-NSact -sc ON
save config
```

Table 1. Parameter values used in this example

Service	
Name	psvc1, psvc2
Server	10.101.3.187, 10.101.3.188
Protocol	HTTP
Port	80
Load Balancing Virtual Server	
Name	vs-NSact
IP Address	10.101.3.201
Protocol	HTTP
Port	80
SureConnect Policy	
Name	policyNS
URL	/cgi-bin/*.cgi
Delay(microseconds)	400000
SC Parameter	
VSR File Name	vsr.htm

To configure this example by using the configuration utility

1. In the In the navigation pane, navigate to System > Settings. In the Modes and Features pane, perform the following actions:

   a. Click Configure Basic Features, select Load Balancing, and Click Go.

   b. Click Configure Advanced Features, select SureConnect, and Click Go.
2. In the navigation pane, navigate to Protection Features > SureConnect. In the details pane, click Parameters. In the Configure SureConnect Parameters window, browse and select the VSR filename.

3. Navigate to Load Balancing > Services. In the details pane, click Add. In the **Create Services** window, enter the paramter values as shown in Table 5-1, and click **OK**.

4. Navigate to Load Balancing > Virtual servers. In the details pane, click Add. In the Create Virtual Server (Load Balancing) dialog box, enter the values shown in Table 5.1 for the Load Balancing Virtual Server parameters and click OK.

5. In the navigation pane, navigate to Load Balancing > Virtual servers. Select the virtual server vs-NSact and click Open in the details pane. The Configure Virtual system (Load Balancing) dialog box, displays the list of configured services. Select services psvc1 and psvc2 and click OK.

6. In the navigation pane, expand Protection Features > SureConnect. In the details pane, click Add. Create the policy with the values as given in the parameters table.

7. In the navigation pane, navigate to Load Balancing > Virtual servers. Select the virtual server vs-NSact and click Open in the details pane. In the Configure Virtual system (Load Balancing) dialog box, click the Policies tab. Click >> to expand the features. Select **SureConnect**. When the list of SureConnect polices appear, select policyNS and click OK.

8. In the navigation pane, navigate to Load Balancing > Virtual servers. Select the virtual server vs-NSact and click Open in the details pane. In the Configure Virtual system (Load Balancing) dialog box, on the Advanced tab, select SC and click OK.

Configuring the SureConnect Policies

You can configure the following SureConnect policies. The NetScaler appliance matches incoming requests in the order the policies are configured:

- Exact URL-based policies
- Wildcard rule-based policies

Configuring Exact URL Based Policies

When you configure an exact URL based policy, the NetScaler appliance matches the incoming request against the URL that has been configured in the policy. URL based policies take precedence over rule based policies.

To configure an exact URL based policy by using the command line interface

At the command prompt, type:

add sc policy <name> [-url <*URL*> | -rule <*expression*>] [-delay <*usecs*>] [-maxConn <positive_integer>] [-action (ACS <altContentSvcName> <altContentPath>) | NS | NOACTION)]

Parameters for configuring an exact URL-based policy

name (Name)

The name of the SureConnect policy. Maximum length: 31 characters. Must begin with an ASCII alphabetic or underscore (_) character and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

url (URL)

The URL against which to match incoming client request. If the request does not match any SureConnect policy, SureConnect does not trigger. Maximum Length: 127 characters. Must begin with an ASCII alphabetic or underscore (_) character and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

rule (Expression)

The expression that the system matches against the incoming request. Expression logic requires names of predefined expressions separated by the logical operators || and &&, and possibly grouped by using parentheses. If the expression contains blanks (for example, between an expression name and a logical operator), the entire argument must be enclosed in double quotation marks ("This requirement does not apply to the configuration utility"). Following are examples of valid expression logic:

```
ns_ext_cgi||ns_ext_asp
```

```
ns_non_get && (ns_header_cookie||ns_header_pragma)
```

Maximum Length: 1499 characters.

delay (Delay)

The delay threshold, in microseconds, for the configured URL or the rule. If the delay statistics gathered for the request that matches the URL specified in the policy exceed the specified delay SureConnect is triggered for that request. Minimum value: 1 Maximum value: 599999999.

maxConn (Maximum Client Connections)

The maximum number of concurrent connections that can be open for the configured policy. Minimum value: 1 Maximum value: 4294967294

action (Action)

The action to be taken when the thresholds are reached. Possible values: ACS , NS, NOACTION.

ACS - Specifies that alternative content is to be served from altContSvcName, with the path altContPath.

NS - Specifies that alternate content is to be served from the NetScaler appliance.

NO ACTION - Specifies that no alternative content is to be served. However, delay statistics are still collected for the configured URLs, and, if the - maxconn parameter is set, the number of connections is limited to the value specified by that parameter. (However, alternative content is not served even if the -maxconn threshold is met).

altContentSvcName (Alternate Service Name)

The alternative content service name used in the ACS action. Maximum Length: 127 characters.

altContentPath (Alternate Content Path)

The alternative content path for the ACS action. Maximum Length: 127 characters.

To configure an exact URL based policy by using the configuration utility

1. In the navigation pane, expand Protection Features, and then click SureConnect.
2. In the details pane, click Add.
3. In the Create SureConnect Policy dialog box, set the following parameters:
   - Name*
   - URL (Make sure that the URL check box is selected)
   - Value*
   - Delay (microseconds)*
   - Maximum Client Connections
   - Action (Select from the Choose Action list.)
   - Alternate Service Name (if you select ACS as the Action)
   - Alternate Content Path (if you select ACS as the Action)

   *A required parameter
4. Click Create, and click Close. The URL based policy appears in the right pane, and a message displays in the status bar that the policy is successfully configured.

Configuring Wildcard Rule-Based Policies

SureConnect matches the incoming requests to a defined rule, if you configure a rule-based policy.

To configure a SureConnect policy based on a wildcard rule by using the command line interface

1. Create the expression(s).

   Use the add expression command to create each expression.

2. Create the rule(s).

   Use the add sc policy command with the -rule expression_logic argument to specify the rule(s). In the -rule expression_logic argument, refer to the expression(s) you created in step 1.

   Repeat this command to create and name each rule.

The following example creates a rule “rule = = /*.cgi”:

```
add vserver vs-lb http 1.1.1.1 80
add expression expr1 url == /cgi-bin/*.cgi
add expression expr2 url == /index.html
add sc policy surecpolicy1 -rule (expr1||expr2) -delay 1000000 -action NS
bind lb vserver vs-lb -policyName surecpolicy1
```

To complete the SureConnect configuration, you will need to enter additional commands, beyond those shown in the example.

To configure a wildcard rule-based policy by using the configuration utility

1. Navigate to Protection Features > SureConnect.
2. In the details pane, click Add.
3. In the Create SureConnect Policy dialog box, in the Name text box, type the name of the policy.
4. Under What to Monitor, click Expression, and then click Configure.
5. In the Create Expression dialog box, click Add.
6. In the Add Expression dialog box, enter an expression. For example, you can select an Expression Type of General, a Flow Type of REQ, a Protocol of HTTP, a Qualifier of URLQUERY, an Operator of CONTAINS, and in the Value text box, type AA. For more information about expressions, see "Policies and Expressions."
7. Click OK, and click Close.
8. In the Create Expression dialog box, click Create.

Examples of wildcard rules:

`"/sports/*"` matches all URLs under `/sports`

`"/sports*"` matches all URLs whose prefix matches `"/sports"`, starting at the beginning of the URL.

`"/*.jsp"` matches all URLs whose file extension is `"jsp"`

When configuring rule-based policies, first add the more specific rule-based policies, before adding more generic rules (for example, `add /cgi-bin/sports*.cgi before adding /cgi-bin/*.cgi`).

Displaying the Configured SureConnect Policy

To view the SureConnect policy that you have configured, at the NetScaler command prompt, enter the show sc policy command.

Customizing the Alternate Content File

When SureConnect activates, it can display alternate content from one of the following files that you have configured:

- **progressbar.htm.** Displays the progress information.
- **alternatepage.htm.** Displays an alternate page.
- **barandpage.htm.** Displays both the progress information and an alternate page.

The alternate content files are JavaScript files. During SureConnect installation, these files are copied onto the server that contains the alternate content. These files can contain alternate content (including an alternate page) or references to other files that contain the alternate content.

This section describes the changes you can make to the alternate content file provided by the appliance.

```
//**** DEFINE YOUR VALUES HERE ****
var alt_url = "/Citrix NetScaler system /sample.gif";
var alt_url = "http://www.DomainName.com";
var Citrix NetScaler system _logo = "netscaler_logo.gif";
var our_logo = "netscaler_logo.gif";
var height = 450;
var width = 550;
var top = 200;
var left = 200;
var popunder = "no"; //specify yes for pop-under & no for pop-up
var shift_focus = "yes" //if you want to send pop-up to background on getting primary content else specify no
//**** YOUR DEFINITIONS ENDS HERE ****
```

You can make these changes:

- **var alt_url.** Specify the URL for the alternate content if a file provides the alternate content. For example:

  var alt_url = “/Citrix NetScaler system/sports.htm”

  Note: The alternate content file must be present in the /Citrix NetScaler system directory under the documents root of the Web server.
- **var our_logo.** Specify the image file of your organization logo.
- **var height.** Specify the height of the SureConnect window.
- **var width.** Specify the width of the SureConnect window.
- **var top and var left.** Specify the position of the SureConnect window.

- **var popunder.** Specifies the position of the alternate content window. Specify the value as NO to place the alternate content window above the original window. Specify the value as YES to place the alternate content window beneath the original window.

- **var shift_focus.** Specify the focus of the alternate content window. YES places the pop-up window in the background when getting the primary content. NO always keeps the pop-up window in focus, even when getting the primary content.

Note: For more information, see the README.txt file provided by the appliance with other alternate content files.

Configuring SureConnect for Citrix NetScaler Features

This section describes how SureConnect works in combination with the load balancing, content switching, cache redirection, and high availability features of the NetScaler appliance.

Configuring SureConnect for Load Balancing

You can use SureConnect in environments where the primary servers use the load balancing feature, with or without alternate servers. If the load balancing virtual server configured for SureConnect fails, the backup virtual server (if there is one) handles the traffic. Backup virtual servers do not support SureConnect policies.

Note: For information about load balancing, see "Load Balancing."

Configuring SureConnect for Cache Redirection

You can use SureConnect in environments where cache redirection is configured. The primary server is a load balancing virtual server bound to the cache redirection virtual server. Regardless of any rules configured for the cache redirection feature:

- You can configure any URL for SureConnect.
- Once SureConnect is activated for a client, requests from the client are always sent to the origin server.

Configuring SureConnect for High Availability

SureConnect is compatible with NetScaler appliances operating in high availability mode.

Note: If the optional vsr.htm file is used, it must be present in both nodes (primary and secondary) and must use the same name and directory.

Activating SureConnect

You can set the Citrix NetScaler appliance to activate SureConnect if either of two criteria match. Both criteria are arguments to the add sc policy command, as described here:

- -delay <microseconds>

  The first time the client requests the URL, the appliance records how long the server takes to respond. The appliance will not activate SureConnect until the second time the URL is requested. The first and second requests may be from the same or different clients.

  If you set -delay argument, SureConnect will be activated the second time the delay reaches the threshold you set.

- -maxConn <positive_integer>

  When the appliance receives a request, it checks the number of connections to the server for the configured URL. SureConnect is activated if the number of connections is greater than or equal to the value that you set for the -maxConn argument.

  If you will be providing alternate content to be displayed in the client’s Web browser, you should configure the -action argument of the add sc policy command. This specifies for the NetScaler appliance whether the alternate content is coming from a dedicated alternate server (-action ACS) or the appliance (-action NS).

  When SureConnect is activated by the –maxConn argument, the SureConnect window and progress bar are displayed in the client's browser (with an alternate page, if configured).

SureConnect Environments

The following topics describe SureConnect environments.

- "Primary and Alternate Servers"
- "Configuration Checklist"
- "Example Configurations"

Primary and Alternate Servers

The SureConnect environment uses a dedicated server to provide alternate content when the requested content is not available. The alternate content may include an alternate page, plus optional components such as frame set, organization logo, and so on. The alternate and primary servers can be the same server.

You can configure SureConnect to display a progress bar when the requested content is not available (or the progress bar and an alternate page).

The following figure illustrates the SureConnect environment.

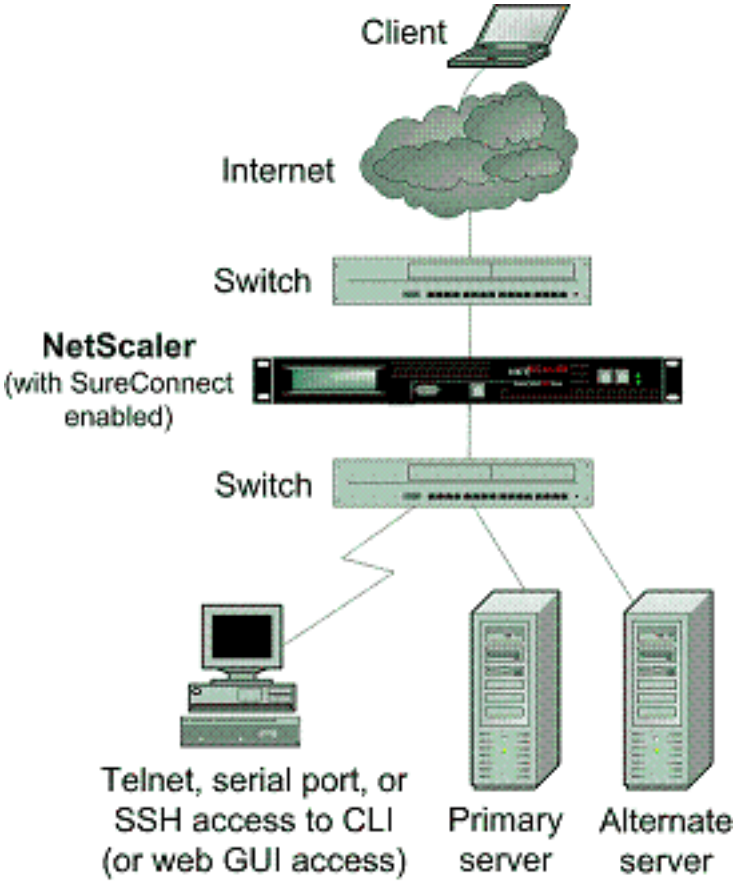


Figure 1. SureConnect - Primary and Alternate Servers

Configuration Checklist

Complete the following checklist before you start configuration:

Table 1. Configuration Checklist

☐	The same builds are running for the appliance and for the SureConnect files as suggested by appliance staff. Appliance Build Number: _____ SureConnect (sc_xx.exe) Build Number: _____
☐	The latest SureConnect files (style files) are extracted to: · All primary servers (required for NS action). · The alternate content server (required for ACS action).
☐	All customizations to the latest style and vsr.htm files are applied.
☐	The alternate content server is accessible from the Internet (required for ACS action).
☐	If the -redirectURL URL argument of the add vserver CLI command needs to be specified: · The URL is up and running. · This URL is not on the configured servers. · This URL does not match any content in the vserver (that is, do not redirect a missing URL to itself). Redirecting a missing URL to itself can send some browsers into an infinite loop.
☐	All URLs to be configured for SureConnect are top-level URLs only. (Only the URLs that occupy the whole window or frame can be configured, not the embedded objects).

Following are the steps to configure SureConnect in a setup with a primary server and a dedicated alternate server:

· Enable the SureConnect feature

· Add the SureConnect policy

· Bind the SureConnect policy

You can optionally configure the following:

· Redirect the client to another URL if the primary server fails, or send a customized response to the client if the alternate server fails.

· If the servers do not provide alternate content, send a default or customized response.

To redirect the client to another URL

1. Enable the SureConnect feature.

2. Define the primary server and its service.

   You must identify the original server for which SureConnect support is being configured. At the NetScaler command prompt, type the following command:

   add service <serviceName> <IP> HTTP <port>

   where <serviceName> assigns a name for the service; <IP> is the server's IP address; and <port> is the port number that the service will use.

   Repeat use of the add service CLI command for each service that is to be added.

   You can also configure SureConnect on a load balancing virtual server. At the NetScaler command prompt, type the following command:

   add vserver <name> HTTP <IP> <port>

3. Define and bind the SureConnect policy as follows. If you are configuring a rule-based policy, perform this step as described in "Configuring Wildcard Rule-Based Policies." To configure a URL-based policy, at the NetScaler command prompt, type the following command:

   add sc policy <name> [-url <URL>] [-delay <microsec>] [-maxConn <positiveInteger>]

   For a detailed description of the add sc policy command, see "Command Reference."

   To bind the SureConnect policy, at the NetScaler command prompt, type the following command:

   bind service <serviceName> -policyname <string>

   where <serviceName> is the name of the service defined in step 2, and <string> is the name of the SureConnect policy.

   Repeat the bind service command for each policy created.

   You must include the alternate content page in the altContSvcName argument, and in the altContPath argument of the add sc policy command.

   In the following example, the name of the alternate content file is /Citrix NetScaler system /barandpage.htm, and this file resides in svc2.

4. To save the configuration, at the NetScaler command prompt, type the following command:

   save config

Example Configurations

The following examples illustrate various SureConnect configurations.

The examples assume that monitoring of physical services is enabled. If the alternate system is down, SureConnect will deliver the alternate content from the system itself.

Example 1 - SureConnect Progress Bar and Alternate Page

You can configure SureConnect to display both the progress bar and an alternate page to the user.

To bind a SureConnect policy to a load balancing virtual server, at the command prompt, type the following commands:

bind lb vserver <virtualServerName> -policyName <string>

where <virutalServerName> is the name of the load balancing virtual server defined in step 2 of the configuration process, and <string> is the name of the SureConnect policy defined in step 3.

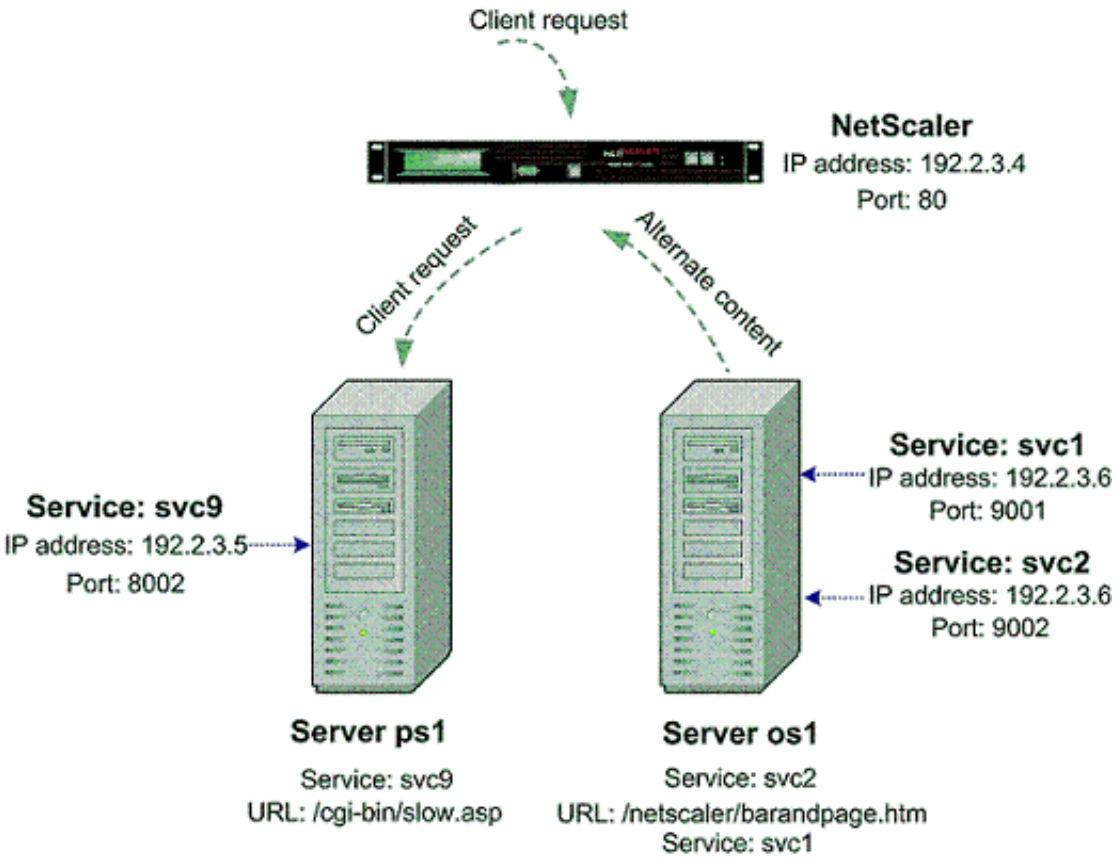


Figure 1. SureConnect Configuration - Example 1

At the NetScaler command prompt, type the following commands:

```
enable feature SC
show ns info
add service svc2 192.2.3.6 HTTP 9002
show server
show service svc2
add service svc9 192.2.3.5 HTTP 8002
add sc policy policy8 -url /cgi-bin/slow.asp
-delay 3000000 -action ACS svc2 /NetScaler 9000 system barandpage.htm
bind service svc9 -policyname policy8
set service svc9 -sc ON
save config
```

After you configure SureConnect, you can enter commands that show information to verify what you have configured.

Example 2 - SureConnect Progress Bar Only

In this example, SureConnect will display only the progress bar. The server orgsrvr with IP address 10.101.8.187 has service orgsvc. This server is connected to the appliance. The service is bound to the appliance. The progressbar.htm file specifies that only the progress bar will be displayed.

At the NetScaler command prompt, type the following commands:

```
enable feature SC
add service orgsvc 10.101.3.187 HTTP 80
add sc policy policy9 -url /cgi-bin/slow.asp
-delay 4000000 -action ACS orgsvc /NetScaler 9000 system / progressbar.htm
bind service orgsvc -policyname policy9
set service orgsvc -sc ON
save config
```

Example 3 - SureConnect with Load Balancing

This example illustrates how to configure the load balancing feature so that SureConnect will display alternate contents from the primary server. For information about load balancing, see "Load Balancing."

In this example, two physical servers with IP 10.101.3.187 and 10.101.3.188 are being load balanced by the appliance. The name and location of the alternate page file is specified in the file alternatepage.htm, which resides on both servers.

The appliance has one configured virtual server address: 10.101.3.201. At the NetScaler command prompt, type the following commands:

```
enable feature SC LB
add service psvc1 10.101.3.187 HTTP 80
add service psvc2 10.101.3.188 HTTP 80
add vserver vs-SureC HTTP 10.101.3.201 80
bind lb vserver vs-SureC psvc1
bind lb vserver vs-SureC psvc2
add sc policy policy9 -url /cgi-bin/slow.asp -delay 4000000
-action ACS vs-SureC /NetScaler system /alternatepage.htm
bind lb vserver vs-SureC -policyName policy9
set lb vserver vs-SureC -sc ON
save config
```

Example 4 - SureConnect with Load Balancing (ACS Action)

This example illustrates how to configure the NetScaler appliance load balancing feature so that SureConnect will display alternate content from the alternate server. For information about load balancing, see "Load Balancing."

In this case, there are two physical servers, IP 10.101.3.187 and 10.101.3.188. Both are being load balanced by the appliance.

The name and location of the alternate page file are specified in file barandpage.htm, which resides on a third server not being load balanced.

The third server's IP address is 10.101.3.189. Because barandpage.htm is specified, the progress bar and alternate page will both be displayed.

The appliance has one configured virtual server "vsvr" whose IP address (Virtual Server) is 10.101.3.200.

At the NetScaler command prompt, type the following commands:

```
enable feature SC LB
add service psvc1 10.101.3.187 HTTP 80
add service psvc2 10.101.3.188 HTTP 80
add service alt-cont-svc 10.101.3.189 HTTP 80
add vserver vsvr HTTP 10.101.3.200 80
bind lb vserver vsvr psvc1
bind lb vserver vsvr psvc2
add sc policy policy10 -url /cgi-bin/slow.asp
-delay 4000000 -action ACS alt-cont-svc
/NetScaler 9000 system /barandpage.htm
bind lb vserver vsvr -policyName policy10
set lb vserver vsvr -sc ON
save config
```

Example 5 - SureConnect with Content Switching

This example illustrates how to configure SureConnect where the NetScaler content switching and load balancing features are being used. SureConnect is configured on a load balancing virtual server bound to a content switching virtual server.

The alternate content is distributed under the content switching virtual server according to the content switching rules. For more information about load balancing and content switching, see "Load Balancing" and "Content Switching."

In this case, three physical services with IP addresses 10.100.100.104, 10.100.100.105, and 10.100.100.106 are bound to three load balancing virtual servers with IP addresses 10.100.100.101, 10.100.100.102, and 10.100.100.103. These three load balancing virtual servers are bound to a content switching virtual server with IP address 10.100.100.100.

In this setup, lbvip1 contains .cgi content, lbvip2 contains .gif content, and .lbvip3 contains .html content.

The name and location of the alternate page file is specified in the file alternatepage.htm, which resides on lbvip3. The embedded objects in this file must be distributed according to the content switching rules (any embedded gif will reside on lbvip2, any embedded htm will reside on lbvip3, and so on).

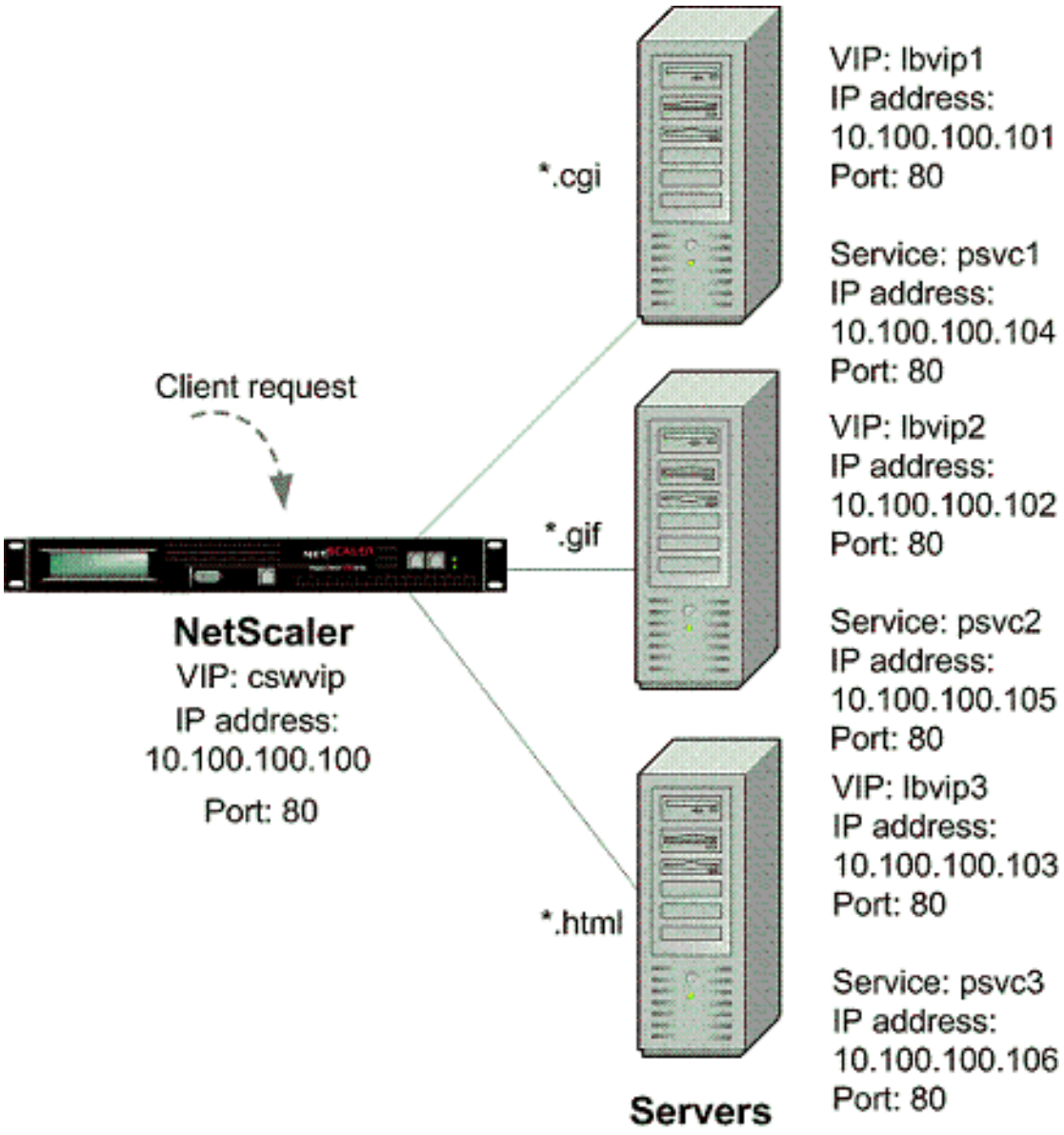


Figure 2. SureConnect Configuration - Example 5

At the NetScaler command prompt, type the following commands:

```
enable feature CS LB SC
add vserver cswvip HTTP 10.100.100.100 80 -type CONTENT
add vserver lbvip1 HTTP 10.100.100.101 80 -type ADDRESS
add vserver lbvip2 HTTP 10.100.100.102 80 -type ADDRESS
add vserver lbvip3 HTTP 10.100.100.103 80 -type ADDRESS
add service psvc1 10.100.100.104 HTTP 80
add service psvc2 10.100.100.105 HTTP 80
add service psvc3 10.100.100.106 HTTP 80
bind lb vserver lbvip1 psvc1
bind lb vserver lbvip2 psvc2
bind lb vserver lbvip3 psvc3
add cs policy CSWpolicy1 -url /*.cgi
```

```
bind cs vserver cswvip lbvip1 -policyName CSWpolicy1
add cs policy CSWpolicy2 -url /*.gif
bind cs vserver cswvip lbvip2 -policyName CSWpolicy2
add cs policy CSWpolicy3 -url /*.htm
bind cs vserver cswvip lbvip3 -policyName CSWpolicy3
add sc policy SCpol -url /cgi-bin/delay.cgi -delay 4000000 -action ACS cswvip /alternatepage.htm
bind lb vserver lbvip1 -policyName SCpol
set lb vserver lbvip1 -sc ON
save config
```

Surge Protection

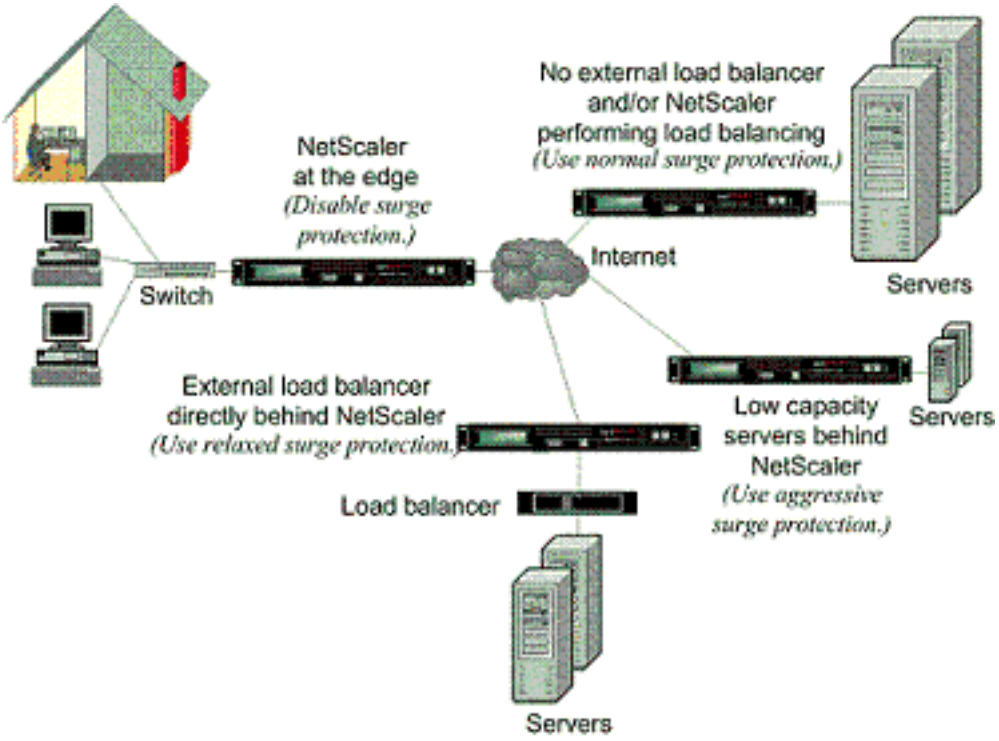
When a surge in client requests overloads a server, server response becomes slow, and the server is unable to respond to new requests. The Surge Protection feature ensures that connections to the server occur at a rate that the server can handle. The response rate depends on how surge protection is configured. The NetScaler appliance also tracks the number of connections to the server, and uses that information to adjust the rate at which it opens new server connections.

Surge protection is enabled by default. If you do not want to use surge protection, as will be the case with some special configurations, you must disable it.

The default surge protection settings are sufficient for most uses, but you can configure surge protection to tune it for your needs. First, you can set the throttle value to tell it how aggressively to manage connection attempts. Second you can set the base threshold value to control the maximum number of concurrent connections that the NetScaler appliance will allow before triggering surge protection. (The default base threshold value is set by the throttle value, but after setting the throttle value you can change it to any number you want.)

The following figure illustrates how surge protection is configured to handle traffic to a Web site.

Figure 1. A Functional Illustration of NetScaler Surge Protection



Note: If the NetScaler appliance is installed at the edge of the network, where it interacts with network devices on the client side of the Internet, the surge protection

feature must be disabled. Surge protection must also be disabled if you enable USIP (Using Source IP) mode on your appliance.

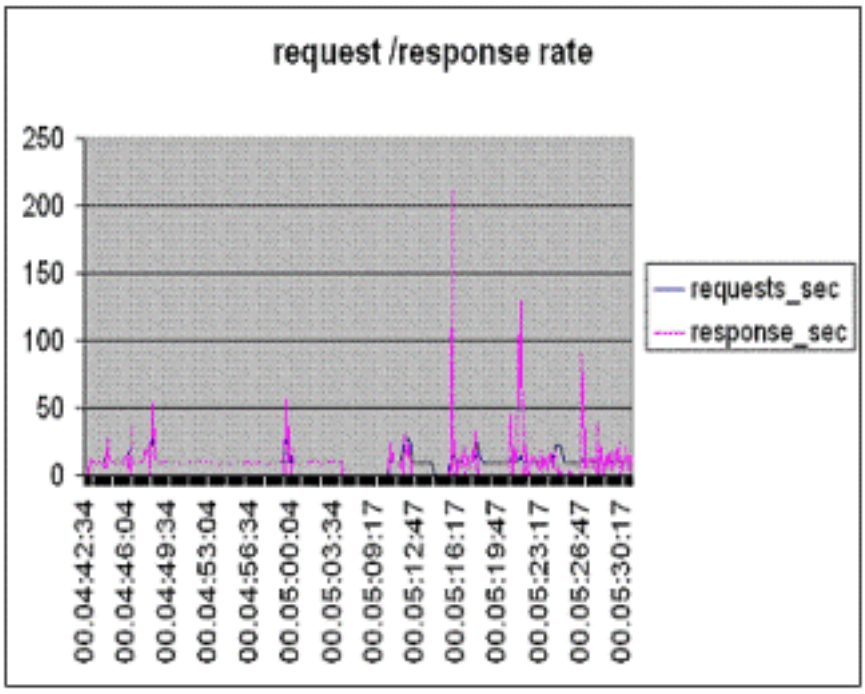
The following example and illustration show the request and response rates for two cases. In one case, surge protection is disabled, and in the other it is enabled.

When surge protection is disabled and a surge in requests occurs, the server accepts as many requests as it can process concurrently, and then begins to drop requests. As the server becomes more overloaded, it goes down and the response rate is reduced to zero. When the server recovers from the crash, usually several minutes later, it sends resets for all pending requests, which is abnormal behavior, and also responds to new requests with resets. The process repeats for each surge in requests. Therefore, a server that is under DDoS attack and receives multiple surges of requests can become unavailable to legitimate users.

When surge protection is enabled and a surge in requests occurs, surge protection manages the rate of requests to the server, sending requests to the server only as fast as the server can handle those requests. This enables the server to respond to each request correctly in the order it was received. When the surge is over, the backlogged requests are cleared as fast as the server can handle them, until the request rate matches the response rate.

The following figure compares the request and response scenarios when surge protection is enabled to that when it is disabled.

Figure 2. Request/Response Rate with and without Surge Protection



Disabling and Reenabling Surge Protection

The surge protection feature is enabled by default. When surge protection is enabled, it is active for any service that you add.

To disable or reenable surge protection by using the command line interface

At the command prompt, type one of the following sets of commands to disable or reenable surge protection and verify the configuration:

- disable ns feature SurgeProtection
- show ns feature
- enable ns feature SurgeProtection
- show ns feature

Example

```
disable ns feature SurgeProtection
 Done show ns feature

      Feature                Acronym          Status
      -------                -------          ------
 1)   Web Logging              WL               ON
 2)   Surge Protection          SP               OFF
 .
 .
 .
 23)  HTML Injection           HTMLInjection     ON
 24)  NetScaler Push           push              OFF
 Done

 enable ns feature SurgeProtection
 Done
> show ns feature

      Feature                Acronym          Status
      -------                -------          ------
 1)   Web Logging              WL               ON
 2)   Surge Protection          SP               ON
 .
 .
```

```
.

23)  HTML Injection          HTMLInjection     ON
24)  NetScaler Push          push              OFF
Done
>
```

To disable or reenable surge protection by using the configuration utility

1. In the navigation pane, expand System, and then select Settings.
2. In the details pane, click Change Advanced Features.
3. In the Configure Advanced Features dialog box, clear the selection from the Surge Protection check box to disable the surge protection feature, or select the check box to enable the feature.
4. Click OK.
5. In the Enable/Disable Feature(s) dialog box, click Yes. A message appears in the status bar, stating that the feature has been enabled or disabled.

To disable or reenable surge protection for a particular service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then select Services. The list of configured services is displayed in the details pane.
2. In the details pane, select the service for which you want to disable or reenable the surge protection feature, and then click Open.
3. In the Configure Service dialog box, click the Advanced tab and scroll down.
4. In the Others frame, clear the selection from the Surge Protection check box to disable the surge protection feature, or select the check box to enable the feature.
5. Click OK. A message appears in the status bar, stating that the feature has been enabled or disabled.

   Note: Surge protection works only when both the feature and the service setting are enabled.

Setting Thresholds for Surge Protection

To set the rate at which the NetScaler appliance opens connections to the server, you must configure the threshold and throttle values for surge protection.

The following figure shows the surge protection curves that result from setting the throttle rate to relaxed, normal, or aggressive. Depending on the configuration of the server capacity, you can set base threshold values to generate appropriate surge protection curves.

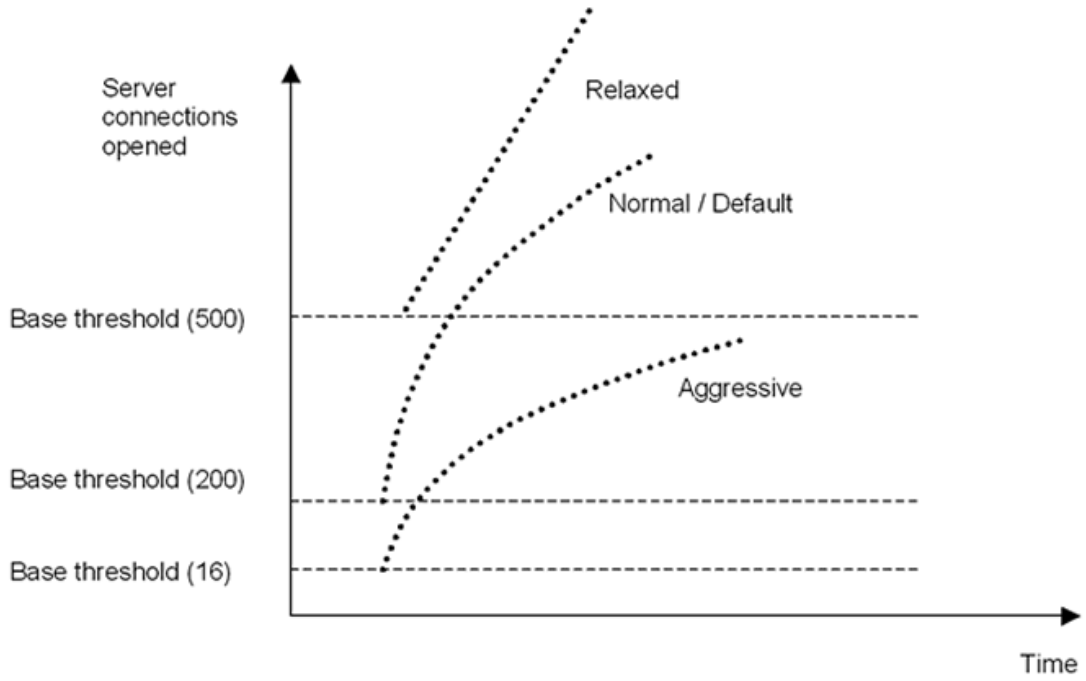


Figure 1. Surge Protection Curves

Your configuration settings affect the behavior of surge protection in the following manner:

- If you do not specify a throttle rate, it is set to normal (the default value), and the base threshold is set to 200, as shown in the preceding figure.
- If you specify a throttle rate (aggressive, normal, or relaxed) without specifying a base threshold, the curve reflects the default values of the base threshold for that throttle rate. For example, if you set the throttle rate to relaxed, the resulting curve will have the base threshold value of 500.
- If you specify only the base threshold, the entire surge protection curve shifts up or down, depending on the value you specify, as shown in the figure that follows.
- If you specify both a base threshold and a throttle rate, the resulting surge protection curve is based on the set throttle rate and adjusted according to the value set for the base threshold.

In the following figure, the lower curve (Aggressive 1) results when the throttle rate is set to aggressive but the base threshold is not set. The upper curve (Aggressive 2) results when the base threshold is set to 500, but the throttle rate is not set. The second upper curve (Aggressive 2) also results when the base threshold is set to 500, and the throttle rate is set to aggressive.

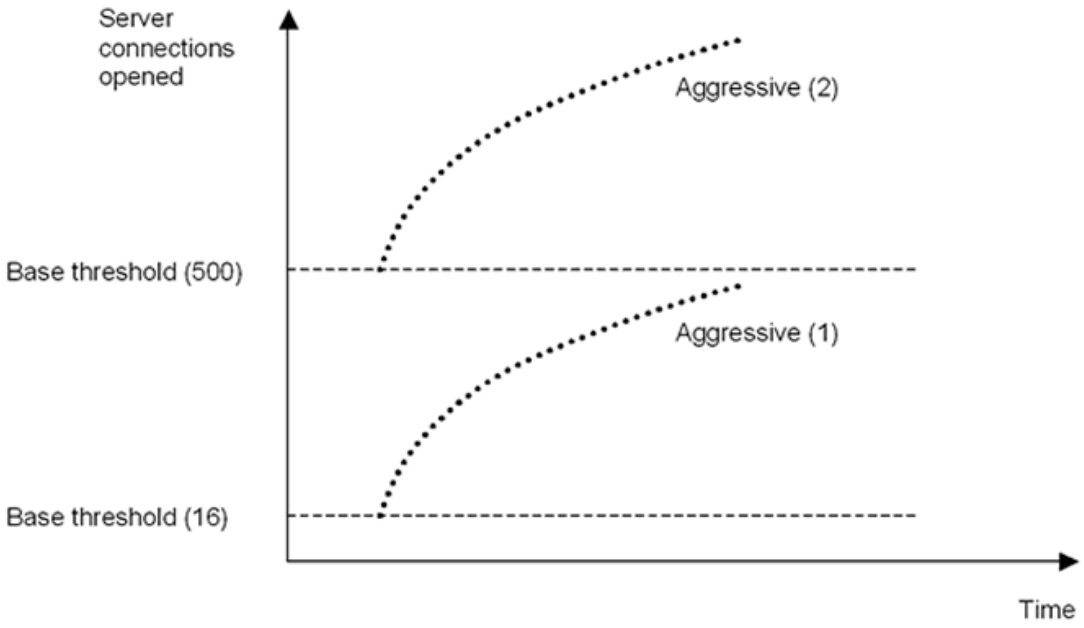


Figure 2. Aggressive Rate with the Default or a Set Base Threshold

To set the threshold for surge protection by using the configuration utility

1. In the navigation pane, expand System, and then select Settings.
2. In the details pane, click Global System Settings.
3. If you want to set a base threshold different from the default for the throttle rate, in the Configure Global Settings dialog box, Base Threshold text box, enter the maximum number of concurrent server connections allowed before surge protection is triggered. The base threshold is the maximum number of server connections that can be open before surge protection is activated. The maximum value for this setting is 32,767 server connections. The default setting for this value is controlled by the throttle rate you choose in the next step.

   Note: If you do not set an explicit value here, the default value will be used.
4. In the Throttle drop-down list, select a throttle rate. The throttle is the rate at which the NetScaler appliance allows connections to the server to be opened. The throttle can be set to the following values:

   Aggressive

   Choose this option when the connection-handling and surge-handling capacity of the server is low and the connection needs to be managed carefully. When you set the throttle to aggressive, the base threshold is set to a default value of 16, which means that surge protection is triggered whenever there are 17 or more concurrent

connections to the server.

Normal

Choose this option when there is no external load balancer behind the NetScaler appliance or downstream. The base threshold is set to a value of 200, which means that surge protection is triggered whenever there are 201 or more concurrent connections to the server. Normal is the default throttle option.

Relaxed

Choose this option when the NetScaler appliance is performing load balancing between a large number of Web servers, and can therefore handle a high number of concurrent connections. The base threshold is set to a value of 500, which means that surge protection is triggered only when there are 501 or more concurrent connections to the server.

5. Click OK. A message appears in the status bar, stating that the global settings are configured.

Flushing the Surge Queue

When a physical server receives a surge of requests, it becomes slow in responding to the currently connected clients and leaves many users dissatisfied and disgruntled. Often, the overloading also causes the clients to receive error pages. To avoid such overloading, the NetScaler appliance provides features such as surge protection, which controls the rate at which new connections to a service can be established.

The appliance does connection multiplexing between clients and physical servers. When it receives a client request to access a service on a server, the appliance looks for an already established connection to the server that is free. If it finds a free connection, it uses that connection to establish a virtual link between the client and the server. If it does not find an existing free connection, the appliance establishes a new connection with the server, and establishes a virtual link between client and the server. However, if the appliance cannot establish a new connection with the server, it sends the client request to a surge queue. If all the physical servers bound to the load balancing or content switching virtual server reach the upper limit on client connections (max client value, surge protection threshold or maximum capacity of the service), the appliance cannot establish a connection with any server. The surge protection feature uses the surge queue to regulate the speed at which connections are opened with the physical servers. The appliance maintains a different surge queue for each service bound to the virtual server.

The length of a surge queue increases whenever a request comes for which the appliance cannot establish a connection, and the length decreases whenever a request in the queue gets sent to the server or a request gets timed out and is removed from the queue.

If the surge queue for a service or service group becomes too long, you may want to flush it. You can flush the surge queue of a specific service or service group, or of all the services and service groups bound to a load balancing virtual server. Flushing a surge queue does not affect the existing connections. Only the requests present in the surge queue get deleted. For those requests, the client has to make a fresh request.

You can also flush the surge queue of a content switching virtual server. If a content switching virtual server forwards some requests to a particular load balancing virtual server, and the load balancing virtual server also receives some other requests, when you flush the surge queue of the content switching virtual server, only the requests received from this content switching virtual server are flushed; the other requests in the surge queue of the load balancing virtual server are not flushed.

Note: You cannot flush the surge queues of cache redirection, authentication, VPN or GSLB virtual servers or GSLB services.

Note: Do not use the Surge Protection feature if Use Source IP (USIP) is enabled.

To flush a surge queue by using the command line interface

The flush ns surgeQ command works in the following manner:

- You can specify the name of a service, service group, or virtual server whose surge queue has to be flushed.
- If you specify a name while executing the command, surge queue of the specified entity will be flushed. If more than one entity has the same name, the appliance flushes surge queues of all those entities.
- If you specify the name of a service group, and a server name and port while executing the command, the appliance flushes the surge queue of only the specified service group member.
- You cannot directly specify a service group member (<serverName> and <port>) without specifying the name of the service group (<name>) and you cannot specify <port> without a <serverName>. Specify the <serverName> and <port> if you want to flush the surge queue for a specific service group member.
- If you execute the command without specifying any names, the appliance flushes the surge queues of all the entities present on the appliance.
- If a service group member is identified with a server name, you must specify the server name in this command; you cannot specify its IP address.

At the command prompt, type:

flush ns surgeQ [-name <name>] [-serverName <serverName> <port>]

Examples

1.
flush ns surgeQ –name SVC1ANZGB –serverName 10.10.10.1 80
The above command flushes the surge queue of the service or virtual server that is named SVC1ANZGB and h
2.
flush ns surgeQ
The above command flushes all the surge queues on the appliance.

Parameters for flushing a surge queue

name

Name of a virtual server, service or service group

serverName

Name of a service group member

To flush a surge queue by using the configuration utility

1. In the navigation pane, expand Load Balancing.
2. To select an entity, do one of the following:
   - To flush the surge queue of a virtual server, click Virtual Servers, and then select the virtual server.
   - To flush the surge queue of a service, click Services, and then select the service.
   - To flush the surge queue of all the members in a service group, click Service Groups, and then select the service group.
   - To flush the surge queue of a specific member in a service group, click Service Groups, and in the action pane, click Manage Members. In the Manage Members of a Service Group dialog box, select the service group member.

   Note: You can select multiple entities in any window.

   Note: To flush the surge queue of a content switching virtual server, in Steps 1 and 2, expand Content Switching, and then select a virtual server.
3. In the action pane, click Flush Surge Queue.
4. Click OK.

   Note: On the appliance, if there are other entities with the same name as you selected, you are alerted that the surge queues of those entities would also be flushed. Take an appropriate action.

Getting Started with Citrix NetScaler VPX

2015-05-17 05:02:15 UTC

Contents

Getting Started with Citrix NetScaler VPX

Intended for system and network administrators who install and configure complex networking equipment, this section of the library describes initial setup and basic configuration of the Citrix® NetScaler® VPX™ product, including the following topics.

Citrix NetScaler VPX Overview	Defines NetScaler VPX and includes a description of the virtualization platforms on which NetScaler VPX can be hosted.
Understanding the NetScaler	What a NetScaler is and where it fits in a network, with descriptions of entities used in typical configurations and the order in which data is processed by the various features.
Installing NetScaler Virtual Appliances on XenServer	Prerequisites and tasks for installing NetScaler VPX on XenServer.
Installing NetScaler Virtual Appliances on VMware ESX	Prerequisites and tasks for installing NetScaler VPX on VMware ESX 4.0 and VMware ESX 3.5.
Installing NetScaler Virtual Appliances on Microsoft Server 2008 RT	Prerequisites and tasks for installing NetScaler VPX on Microsoft Server 2008 RT
Installing NetScaler VPX on AWS	Prerequisites and tasks for installing NetScaler VPX on AWS
Configuring the Basic System Settings	Tasks for setting up an initial configuration by using the NetScaler VPX Console in XenCenter and tasks for configuring a NetScaler VPX virtual appliance.
Understanding Common Network Topologies	Describes the four common deployment topologies: Two-Arm Multiple Subnet, Two-Arm Transparent, One-Arm Single Subnet, and One-Arm Multiple Subnet. Includes topology diagrams, sample values, and references.
Configuring System Management Settings	Procedures for configuring basic system management settings, such as VLANs, SNMP, and DNS.
Load Balancing Traffic on a NetScaler	Basic introduction to the load balancing feature. Includes procedures for configuring a basic load balancing setup to deliver a Web application, and procedures for configuring persistence, URL redirection, and backup vservers.
Accelerating Load Balanced Traffic by Using Compression	Basic introduction to the compression feature. Includes procedures for configuring a NetScaler to compress application traffic.

Securing Load Balanced Traffic by Using SSL	Basic introduction to the SSL offload feature. Includes procedures for configuring a NetScaler to secure application traffic by using SSL.
Features at a Glance	Brief description of all the features, with links to documentation for the features.

Citrix NetScaler Virtual Appliance Overview

The NetScaler virtual appliance product is a virtual NetScaler appliance that can be hosted on Citrix XenServer®, VMware ESX or ESXi, and Microsoft Hyper-V virtualization platforms.

A NetScaler virtual appliance supports all the features of a physical NetScaler, except virtual MAC (vMAC) addresses, Layer 2 (L2) mode, and link aggregation control protocol (LACP). VLAN tagging is supported on the NetScaler virtual appliances hosted on the XenServer and on VMware ESX platforms.

For the VLAN tagging feature to work, do one of the following:

- On the Citrix XenServer, configure tagged VLANs on a port on the switch but do NOT configure any VLANs on the XenServer interface attached to that port. The VLAN tags are passed through to the virtual appliance and you can use the tagged VLAN configuration on the virtual appliance.

- On the VMware ESX, set the port group's VLAN ID to 4095 on the VSwitch of VMware ESX server. For more information about setting a VLAN ID on the VSwitch of VMware ESX server, see http://www.vmware.com/pdf/esx3_vlan_wp.pdf.

This overview covers only aspects that are unique to NetScaler virtual appliance. For an overview of NetScaler virtual appliance functionality, see Understanding the NetScaler.

Note: The terms *NetScaler*, *NetScaler appliance*, and *appliance* are used interchangeably with *NetScaler virtual appliance* unless stated otherwise.

Citrix NetScaler Virtual Appliance Overview

The NetScaler virtual appliance product is a virtual NetScaler appliance that can be hosted on Citrix XenServer®, VMware ESX or ESXi, and Microsoft Hyper-V virtualization platforms.

A NetScaler virtual appliance supports all the features of a physical NetScaler, except virtual MAC (vMAC) addresses, Layer 2 (L2) mode, and link aggregation control protocol (LACP). VLAN tagging is supported on the NetScaler virtual appliances hosted on the XenServer and on VMware ESX platforms.

For the VLAN tagging feature to work, do one of the following:

- On the Citrix XenServer, configure tagged VLANs on a port on the switch but do NOT configure any VLANs on the XenServer interface attached to that port. The VLAN tags are passed through to the virtual appliance and you can use the tagged VLAN configuration on the virtual appliance.

- On the VMware ESX, set the port group's VLAN ID to 4095 on the VSwitch of VMware ESX server. For more information about setting a VLAN ID on the VSwitch of VMware ESX server, see http://www.vmware.com/pdf/esx3_vlan_wp.pdf.

This overview covers only aspects that are unique to NetScaler virtual appliance. For an overview of NetScaler virtual appliance functionality, see Understanding the NetScaler.

Note: The terms *NetScaler*, *NetScaler appliance*, and *appliance* are used interchangeably with *NetScaler virtual appliance* unless stated otherwise.

NetScaler Virtual Appliance Setup for the XenServer Platform

When you set up NetScaler virtual appliance on XenServer, you must use the XenCenter client to install the first NetScaler virtual appliance. Subsequent virtual appliances can be added by using either the XenCenter client or Citrix Command Center.

XenServer

The XenServer® product is a server virtualization platform that offers near bare-metal virtualization performance for virtualized server and client operating systems. XenServer uses the Xen® hypervisor to virtualize each server on which it is installed, enabling each server to host multiple virtual machines simultaneously.

The following figure shows the bare-metal solution architecture of NetScaler virtual appliance on XenServer.

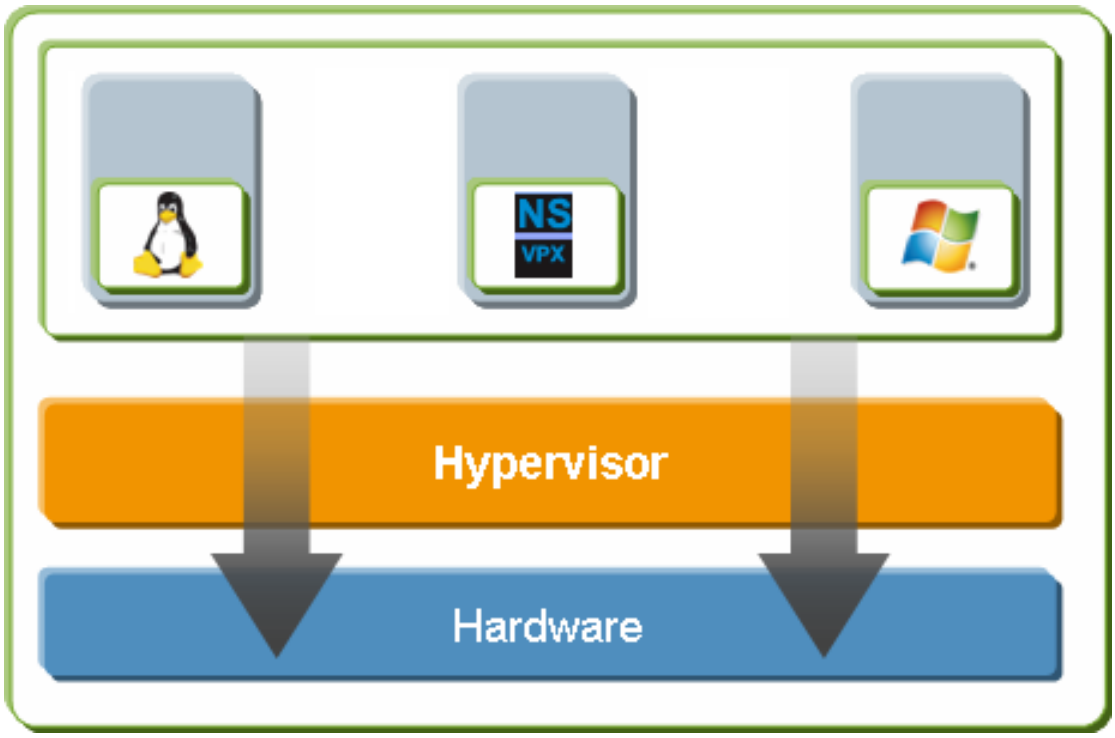


Figure 1. NetScaler Virtual Appliance on XenServer

The bare-metal solution architecture has the following components:

Hardware or physical layer:

Physical hardware components including memory, CPU, network cards, and disk drives.

Xen hypervisor:

Thin layer of software that runs on top of the hardware. The Xen hypervisor gives each virtual machine a dedicated view of the hardware.

Virtual machine:

Operating system hosted on the hypervisor and appearing to the user as a separate physical computer. However, the machine shares physical resources with other virtual machines, and it is portable because the virtual machine is abstracted from physical hardware.

A NetScaler virtual machine, or *virtual appliance*, is installed on the Xen hypervisor and uses paravirtualized drivers to access storage and network resources. It appears to the users as an independent NetScaler appliance with its own network identity, user authorization and authentication capabilities, configuration, applications, and data. The paravirtualization technique enables the virtual machines and the hypervisor to work together to achieve high performance for I/O and for CPU and memory virtualization.

For more information about XenServer, see the XenServer documentation at http://support.citrix.com/product/xens/.

XenCenter

XenCenter® is a graphical virtualization-management interface for XenServer®, enabling you to manage servers, resource pools, and shared storage, and to deploy, manage, and monitor virtual machines from your Windows desktop machine.

Use XenCenter to install NetScaler virtual appliance on XenServer.

For more information about XenCenter, see the XenServer documentation at http://support.citrix.com/product/xens/.

Command Center

Command Center is a management and monitoring solution for Citrix application networking products that include NetScaler, NetScaler virtual appliance, Access Gateway Enterprise Edition, Citrix® Branch Repeater™, Branch Repeater VPX™, and Citrix Repeater™. Command Center enables network administrators and operations teams to manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console.

This centralized management solution simplifies operations by providing administrators with enterprise-wide visibility and automating management tasks that need to be executed across multiple devices.

Command Center is available with Citrix NetScaler Enterprise and Platinum editions.

You can use Command Center to provision NetScaler virtual appliance on XenServer, and then you can manage and monitor the virtual appliances from Command Center.

Note: You must use the XenCenter client to manage XenServer. You cannot manage XenServer from Command Center.

For more information about Command Center, see the Command Center documentation.

NetScaler Virtual Appliance Setup for the VMware ESX Platform

The NetScaler virtual appliance setup for the VMware ESX platform requires a VMware ESX or ESXi server and the vSphere client.

VMware ESX and ESXi are virtualization products based on bare-metal architecture, offered by VMware, Inc. Citrix NetScaler virtual appliance can be hosted on a VMware ESX or ESXi server.

For more information about VMware ESX, see http://www.vmware.com/.

The vSphere client is a graphical interface for managing virtual machines on VMware ESX servers. You use the vSphere client to allocate resources on the ESX server to virtual appliances installed on the server or to deallocate resources. For example, you can allocate virtual network ports to a virtual appliance.

For more information about VMware vSphere client, see http://www.vmware.com/.

NetScaler Virtual Appliance Setup for the Microsoft Hyper-V Platform

Note: This feature is only available in releases 9.3.e and 10.

The NetScaler virtual appliance setup for the Microsoft Hyper-V platform requires Windows Server 2008 R2 or 2012 with the Hyper-V role installed. Like all virtualization systems, Hyper-V enables you to create a virtualized computing environment that results in better utilization of your hardware resources.

Hyper-V is a type 1 hypervisor that comes preinstalled with Windows Server 2008 R2 or 2012. It needs to be enabled as a role on the Windows Server.

For more information about Hyper-V, see http://technet.microsoft.com/en-us/library/cc816638(WS.10).aspx.

NetScaler Virtual Appliance Setup for Linux-KVM Platform

The NetScaler® VPX™ is a virtual NetScaler appliance that can be hosted on a kernel based Virtualization Machine(KVM). The host Linux operating system must be installed on suitable hardware by using virtualization tools such as KVM Module and QEMU. NetScaler VPX runs as a virtual appliance on Linux-KVM server. Like all virtualization systems, KVM enables you to create a virtualized computing environment that results in better utilization of your hardware resources.

Hypervisors Supported on a NetScaler Virtual Appliance

The following table lists the details, such as system ID (sysID) and whether support is available for multiple packet engines (multi-PE), for the different hypervisors supported on a NetScaler virtual appliance.

Table 1. Hypervisors Supported on a NetScaler Virtual Appliance

	VPX on XenServer	VPX on VMware ESX	VPX on Microsoft Hyper-V	VPX on Amazon Web Services
Hypervisor Version	6.0, 6.1	4.1, 5.1	2008, 2012	N/A
SysID	450000	450010	450020	450040
Multi-PE Supported	Yes	Yes	No	No
Clustering Supported	Yes	Yes	Yes	No
Licenses	VPX-10, VPX-200, VPX-1000, VPX-3000, VPX-8000	VPX-10, VPX-200, VPX-1000, VPX-3000, VPX-8000	VPX-10, VPX-200, VPX-1000, VPX-3000, VPX-8000	VPX-10, VPX-200, VPX-1000, VPX-BYOL

Understanding the NetScaler

The Citrix NetScaler product is an application switch that performs application-specific traffic analysis to intelligently distribute, optimize, and secure Layer 4-Layer 7 (L4–L7) network traffic for web applications. For example, a NetScaler bases load balancing decisions on individual HTTP requests instead of on long-lived TCP connections, so that the failure or slowdown of a server is managed much more quickly and with less disruption to clients. The NetScaler feature set can be broadly categorized as consisting of switching features, security and protection features, and server-farm optimization features.

Switching Features

When deployed in front of application servers, a NetScaler ensures optimal distribution of traffic by the way in which it directs client requests. Administrators can segment application traffic according to information in the body of an HTTP or TCP request, and on the basis of L4–L7 header information such as URL, application data type, or cookie. Numerous load balancing algorithms and extensive server health checks improve application availability by ensuring that client requests are directed to the appropriate servers.

Security and Protection Features

NetScaler security and protection features protect web applications from Application Layer attacks. A NetScaler allows legitimate client requests and can block malicious requests. It provides built-in defenses against denial-of-service (DoS) attacks and supports features that protect against legitimate surges in application traffic that would otherwise overwhelm the servers. An available built-in firewall protects web applications from Application Layer attacks, including buffer overflow exploits, SQL injection attempts, cross-site scripting attacks, and more. In addition, the firewall provides identity theft protection by securing confidential corporate information and sensitive customer data.

Optimization Features

Optimization features offload resource-intensive operations, such as Secure Sockets Layer (SSL) processing, data compression, client keep-alive, TCP buffering, and the caching of static and dynamic content from servers. This improves the performance of the servers in the server farm and therefore speeds up applications. A NetScaler supports several transparent TCP optimizations, which mitigate problems caused by high latency and congested network links, accelerating the delivery of applications while requiring no configuration changes to clients or servers.

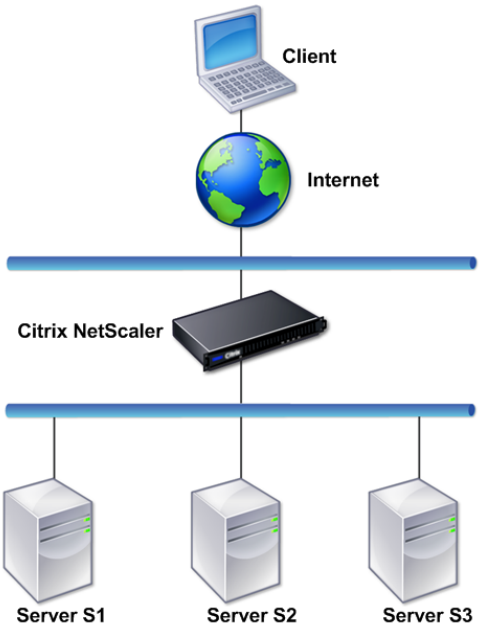
Where Does a NetScaler Appliance Fit in the Network?

A NetScaler appliance resides between the clients and the servers, so that client requests and server responses pass through it. In a typical installation, virtual servers configured on the appliance provide connection points that clients use to access the applications behind the appliance. In this case, the appliance owns public IP addresses that are associated with its virtual servers, while the real servers are isolated in a private network. It is also possible to operate the appliance in a transparent mode as an L2 bridge or L3 router, or even to combine aspects of these and other modes.

Physical Deployment Modes

A NetScaler appliance logically residing between clients and servers can be deployed in either of two physical modes: inline and one-arm. In inline mode, multiple network interfaces are connected to different Ethernet segments, and the appliance is placed between the clients and the servers. The appliance has a separate network interface to each client network and a separate network interface to each server network. The appliance and the servers can exist on different subnets in this configuration. It is possible for the servers to be in a public network and the clients to directly access the servers through the appliance, with the appliance transparently applying the L4-L7 features. Usually, virtual servers (described later) are configured to provide an abstraction of the real servers. The following figure shows a typical inline deployment.

Figure 1. Inline Deployment



In one-arm mode, only one network interface of the appliance is connected to an Ethernet segment. The appliance in this case does not isolate the client and server sides of the network, but provides access to applications through configured virtual servers. One-arm mode can simplify network changes needed for NetScaler installation in some environments.

For examples of inline (two-arm) and one-arm deployment, see "Understanding Common Network Topologies."

Citrix NetScaler as an L2 Device

A NetScaler functioning as an L2 device is said to operate in L2 mode. In L2 mode, the NetScaler forwards packets between network interfaces when all of the following conditions are met:

- The packets are destined to another device's media access control (MAC) address.
- The destination MAC address is on a different network interface.
- The network interface is a member of the same virtual LAN (VLAN).

By default, all network interfaces are members of a pre-defined VLAN, VLAN 1. Address Resolution Protocol (ARP) requests and responses are forwarded to all network interfaces that are members of the same VLAN. To avoid bridging loops, L2 mode must be disabled if another L2 device is working in parallel with the NetScaler.

For information about how the L2 and L3 modes interact, see "Configuring Modes of Packet Forwarding."

For information about configuring L2 mode, see "Enabling and Disabling Layer 2 Mode."

Citrix NetScaler as a Packet Forwarding Device

A NetScaler appliance can function as a packet forwarding device, and this mode of operation is called *L3 mode*. With L3 mode enabled, the appliance forwards any received unicast packets that are destined for an IP address that does not belong to the appliance, if there is a route to the destination. The appliance can also route packets between VLANs.

In both modes of operation, L2 and L3, the appliance generally drops packets that are in:

- Multicast frames
- Unknown protocol frames destined for an appliance's MAC address (non-IP and non-ARP)
- Spanning Tree protocol (unless BridgeBPDUs is ON)

For information about how the L2 and L3 modes interact, see "Configuring Modes of Packet Forwarding."

For information about configuring the L3 mode, see "Enabling and Disabling Layer 3 Mode."

How a NetScaler Communicates with Clients and Servers

A NetScaler appliance is usually deployed in front of a server farm and functions as a transparent TCP proxy between clients and servers, without requiring any client-side configuration. This basic mode of operation is called Request Switching technology and is the core of NetScaler functionality. Request Switching enables an appliance to multiplex and offload the TCP connections, maintain persistent connections, and manage traffic at the request (application layer) level. This is possible because the appliance can separate the HTTP request from the TCP connection on which the request is delivered.

Depending on the configuration, an appliance might process the traffic before forwarding the request to a server. For example, if the client attempts to access a secure application on the server, the appliance might perform the necessary SSL processing before sending traffic to the server.

To facilitate efficient and secure access to server resources, an appliance uses a set of IP addresses collectively known as *NetScaler-owned IP addresses*. To manage your network traffic, you assign NetScaler-owned IP addresses to virtual entities that become the building blocks of your configuration. For example, to configure load balancing, you create virtual servers to receive client requests and distribute them to services, which are entities representing the applications on your servers.

Understanding NetScaler-Owned IP Addresses

To function as a proxy, a NetScaler appliance uses a variety of IP addresses. The key NetScaler-owned IP addresses are:

NetScaler IP (NSIP) address

The NSIP address is the IP address for management and general system access to the appliance itself, and for communication between appliances in a high availability configuration.

Mapped IP (MIP) address

A MIP address is used for server-side connections. It is not the IP address of the appliance. In most cases, when the appliance receives a packet, it replaces the source IP address with a MIP address before sending the packet to the server. With the servers abstracted from the clients, the appliance manages connections more efficiently.

Virtual server IP (VIP) address

A VIP address is the IP address associated with a virtual server. It is the public IP address to which clients connect. An appliance managing a wide range of traffic may have many VIPs configured.

Subnet IP (SNIP) address

A SNIP address is used in connection management and server monitoring. You can specify multiple SNIP addresses for each subnet. SNIP addresses can be bound to a VLAN.

IP Set

An IP set is a set of IP addresses, which are configured on the appliance as SNIP . An IP set is identified with a meaningful name that helps in identifying the usage of the IP addresses contained in it.

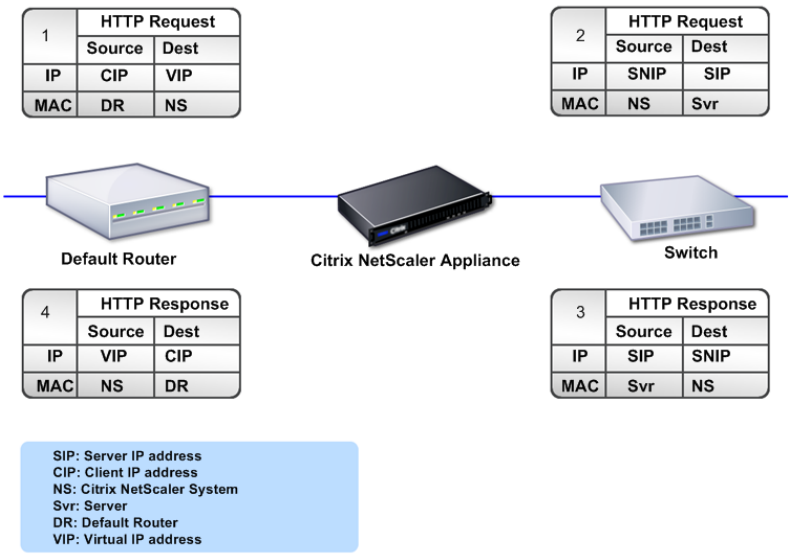
Net Profile

A net profile (or network profile) contains an IP address or an IP set. A net profile can be bound to load balancing or content switching virtual servers, services, service groups, or monitors. During communication with physical servers or peers, the appliance uses the addresses specified in the profile as source IP addresses.

How Traffic Flows Are Managed

Because a NetScaler appliance functions as a TCP proxy, it translates IP addresses before sending packets to a server. When you configure a virtual server, clients connect to a VIP address on the NetScaler instead of directly connecting to a server. As determined by the settings on the virtual server, the appliance selects an appropriate server and sends the client's request to that server. By default, the appliance uses a SNIP address to establish connections with the server, as shown in the following figure.

Figure 1. Virtual Server Based Connections



In the absence of a virtual server, when an appliance receives a request, it transparently forwards the request to the server. This is called the transparent mode of operation. When operating in transparent mode, an appliance translates the source IP addresses of incoming client requests to the SNIP address but does not change the destination IP address. For this mode to work, L2 or L3 mode has to be configured appropriately.

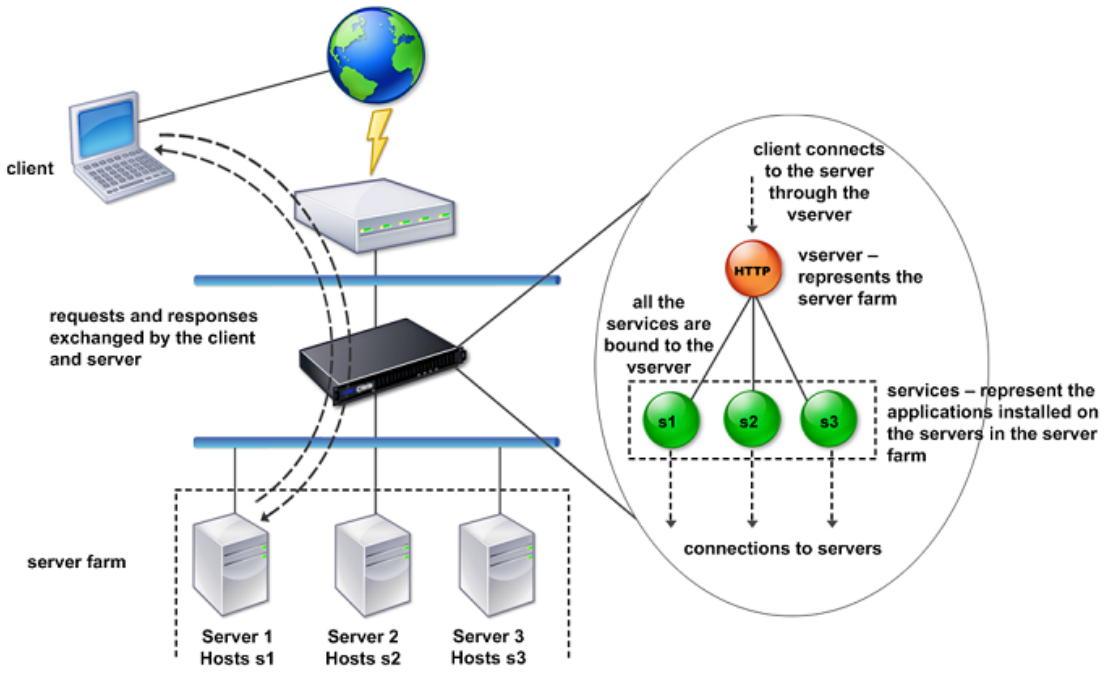
For cases in which the servers need the actual client IP address, the appliance can be configured to modify the HTTP header by inserting the client IP address as an additional field, or configured to use the client IP address instead of a SNIP address for connections to the servers.

Traffic Management Building Blocks

The configuration of a NetScaler appliance is typically built up with a series of virtual entities that serve as building blocks for traffic management. The building block approach helps separate traffic flows. Virtual entities are abstractions, typically representing IP addresses, ports, and protocol handlers for processing traffic. Clients access applications and resources through these virtual entities. The most commonly used entities are virtual servers and services. Virtual servers represent groups of servers in a server farm or remote network, and services represent specific applications on each server.

Most features and traffic settings are enabled through virtual entities. For example, you can configure an appliance to compress all server responses to a client that is connected to the server farm through a particular virtual server. To configure the appliance for a particular environment, you need to identify the appropriate features and then choose the right mix of virtual entities to deliver them. Most features are delivered through a cascade of virtual entities that are bound to each other. In this case, the virtual entities are like blocks being assembled into the final structure of a delivered application. You can add, remove, modify, bind, enable, and disable the virtual entities to configure the features. The following figure shows the concepts covered in this section.

Figure 1. How Traffic Management Building Blocks Work

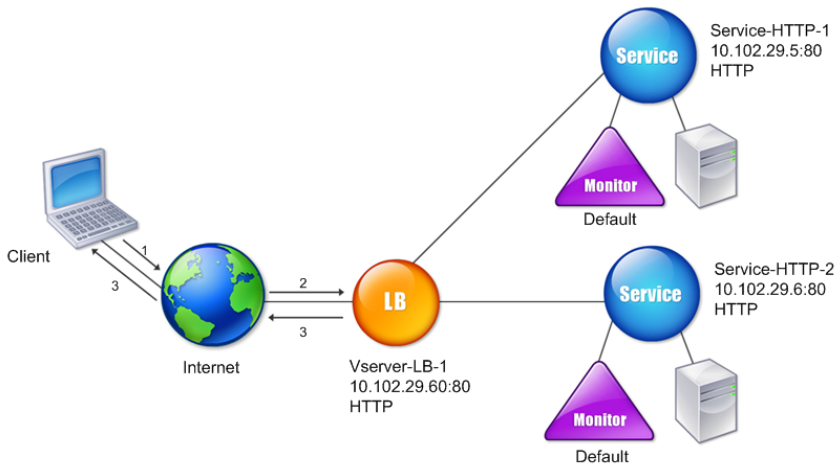


A Simple Load Balancing Configuration

In the example shown in the following figure, the NetScaler appliance is configured to function as a load balancer. For this configuration, you need to configure virtual entities specific to load balancing and bind them in a specific order. As a load balancer, an appliance distributes client requests across several servers and thus optimizes the utilization of resources.

The basic building blocks of a typical load balancing configuration are services and load balancing virtual servers. The services represent the applications on the servers. The virtual servers abstract the servers by providing a single IP address to which the clients connect. To ensure that client requests are sent to a server, you need to bind each service to a virtual server. That is, you must create services for every server and bind the services to a virtual server. Clients use the VIP address to connect to a NetScaler appliance. When the appliance receives client requests sent to the VIP address, it sends them to a server determined by the load balancing algorithm. Load balancing uses a virtual entity called a *monitor* to track whether a specific configured service (server plus application) is available to receive requests.

Figure 1. Load Balancing Virtual Server, Services, and Monitors



In addition to configuring the load balancing algorithm, you can configure several parameters that affect the behavior and performance of the load balancing configuration. For example, you can configure the virtual server to maintain persistence based on source IP address. The appliance then directs all requests from any specific IP address to the same server.

Understanding Virtual Servers

A virtual server is a named NetScaler entity that external clients can use to access applications hosted on the servers. It is represented by an alphanumeric name, virtual IP (VIP) address, port, and protocol. The name of the virtual server is of only local significance and is designed to make the virtual server easier to identify. When a client attempts to access applications on a server, it sends a request to the VIP instead of the IP address of the physical server. When the appliance receives a request at the VIP address, it terminates the connection at the virtual server and uses its own connection with the server on behalf of the client. The port and protocol settings of the virtual server determine the applications that the virtual server represents. For example, a web server can be represented by a virtual server and a service whose port and protocol are set to 80 and HTTP, respectively. Multiple virtual servers can use the same VIP address but different protocols and ports.

Virtual servers are points for delivering features. Most features, like compression, caching, and SSL offload, are normally enabled on a virtual server. When the appliance receives a request at a VIP address, it chooses the appropriate virtual server by the port on which the request was received and its protocol. The appliance then processes the request as appropriate for the features configured on the virtual server.

In most cases, virtual servers work in tandem with services. You can bind multiple services to a virtual server. These services represent the applications running on physical servers in a server farm. After the appliance processes requests received at a VIP address, it forwards them to the servers as determined by the load balancing algorithm configured on the virtual server. The following figure illustrates these concepts.

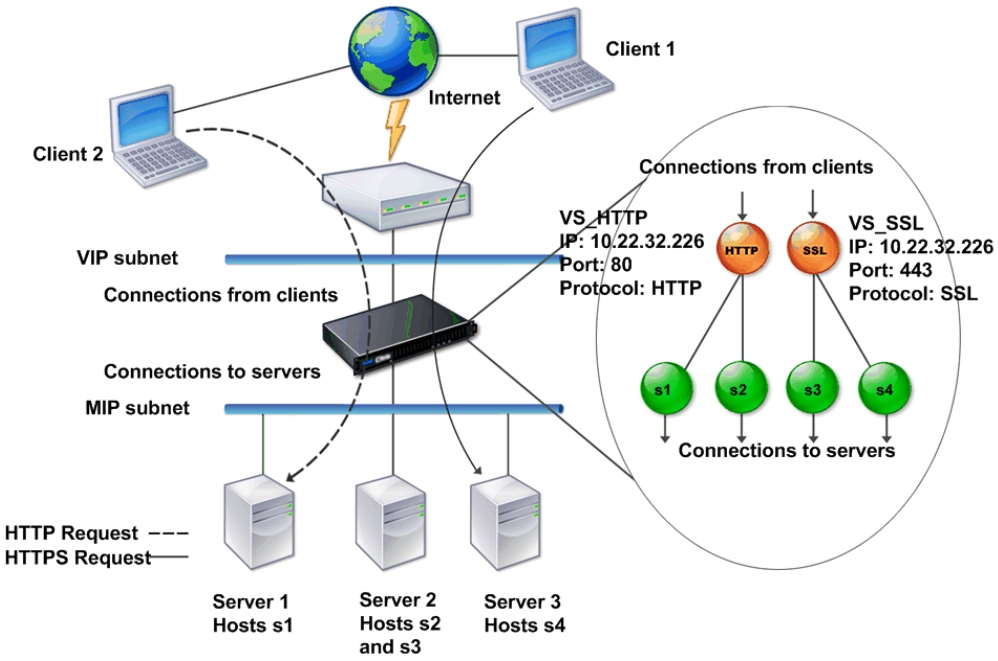


Figure 1. Multiple Virtual Servers with a Single VIP Address

The preceding figure shows a configuration consisting of two virtual servers with a common VIP address but different ports and protocols. Each of the virtual servers has two services bound to it. The services s1 and s2 are bound to VS_HTTP and represent the HTTP applications on Server 1 and Server 2. The services s3 and s4 are bound to VS_SSL and represent the SSL applications on Server 2 and Server 3 (Server 2 provides both HTTP and SSL applications). When the appliance receives an HTTP request at the VIP address, it processes the request as specified by the settings of VS_HTTP and sends it to either Server 1 or Server 2. Similarly, when the appliance receives an HTTPS request at the VIP address, it processes it as specified by the settings of VS_SSL and it sends it to either Server 2 or Server 3.

Virtual servers are not always represented by specific IP addresses, port numbers, or protocols. They can be represented by wildcards, in which case they are known as *wildcard* virtual servers. For example, when you configure a virtual server with a wildcard instead of a VIP, but with a specific port number, the appliance intercepts and processes all traffic conforming to that protocol and destined for the predefined port. For virtual servers with wildcards instead of VIPs and port numbers, the appliance intercepts and processes all traffic conforming to the protocol.

Virtual servers can be grouped into the following categories:

Load balancing virtual server

Receives and redirects requests to an appropriate server. Choice of the appropriate server is based on which of the various load balancing methods the user configures.

Cache redirection virtual server

Redirects client requests for dynamic content to origin servers, and requests for static content to cache servers. Cache redirection virtual servers often work in conjunction with load balancing virtual servers.

Content switching virtual server

Directs traffic to a server on the basis of the content that the client has requested. For example, you can create a content switching virtual server that directs all client requests for images to a server that serves images only. Content switching virtual servers often work in conjunction with load balancing virtual servers.

Virtual private network (VPN) virtual server

Decrypts tunneled traffic and sends it to intranet applications.

SSL virtual server

Receives and decrypts SSL traffic, and then redirects to an appropriate server. Choosing the appropriate server is similar to choosing a load balancing virtual server.

Understanding Services

Services represent applications on a server. While services are normally combined with virtual servers, in the absence of a virtual server, a service can still manage application-specific traffic. For example, you can create an HTTP service on a NetScaler appliance to represent a web server application. When the client attempts to access a web site hosted on the web server, the appliance intercepts the HTTP requests and creates a transparent connection with the web server.

In service-only mode, an appliance functions as a proxy. It terminates client connections, uses a SNIP address to establish a connection to the server, and translates the destination IP addresses of incoming client requests to a SNIP address. Although the clients send requests directly to the IP address of the server, the server sees them as coming from the SNIP address. The appliance translates the IP addresses, port numbers, and sequence numbers.

A service is also a point for applying features. Consider the example of SSL acceleration. To use this feature, you must create an SSL service and bind an SSL certificate to the service. When the appliance receives an HTTPS request, it decrypts the traffic and sends it, in clear text, to the server. Only a limited set of features can be configured in the service-only case.

Services use entities called monitors to track the health of applications. Every service has a default monitor, which is based on the service type, bound to it. As specified by the settings configured on the monitor, the appliance sends probes to the application at regular intervals to determine its state. If the probes fail, the appliance marks the service as down. In such cases, the appliance responds to client requests with an appropriate error message or re-routes the request as determined by the configured load balancing policies.

Understanding Policies and Expressions

A policy defines specific details of traffic filtering and management on a NetScaler. It consists of two parts: the expression and the action. The expression defines the types of requests that the policy matches. The action tells the NetScaler what to do when a request matches the expression. As an example, the expression might be to match a specific URL pattern to a type of security attack, with the action being to drop or reset the connection. Each policy has a priority, and the priorities determine the order in which the policies are evaluated.

When a NetScaler receives traffic, the appropriate policy list determines how to process the traffic. Each policy on the list contains one or more expressions, which together define the criteria that a connection must meet to match the policy.

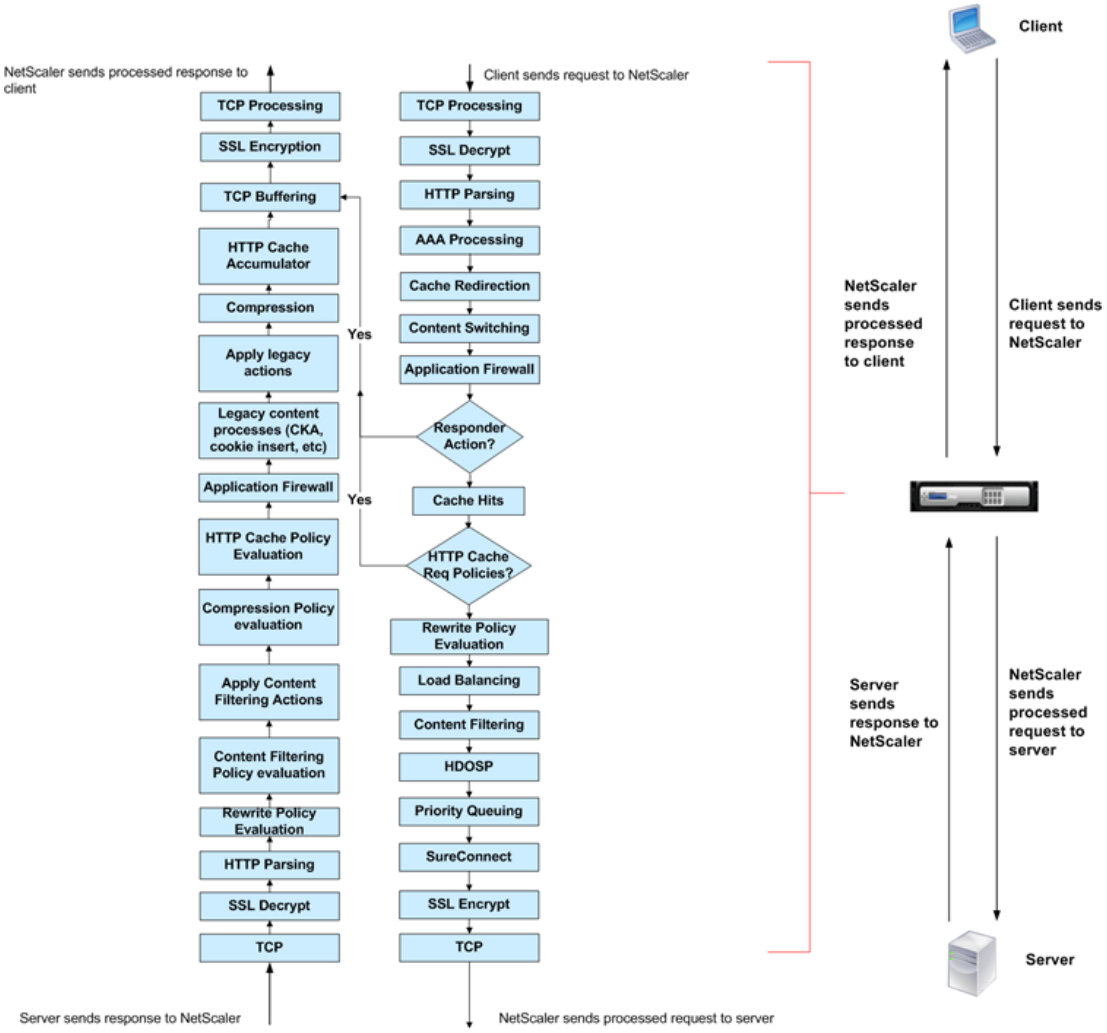
For all policy types except Rewrite policies, a NetScaler implements only the first policy that a request matches, not any additional policies that it might also match. For Rewrite policies, the NetScaler evaluates the policies in order and, in the case of multiple matches, performs the associated actions in that order. Policy priority is important for getting the results you want.

Processing Order of Features

Depending on requirements, you can choose to configure multiple features. For example, you might choose to configure both compression and SSL offload. As a result, an outgoing packet might be compressed and then encrypted before being sent to the client.

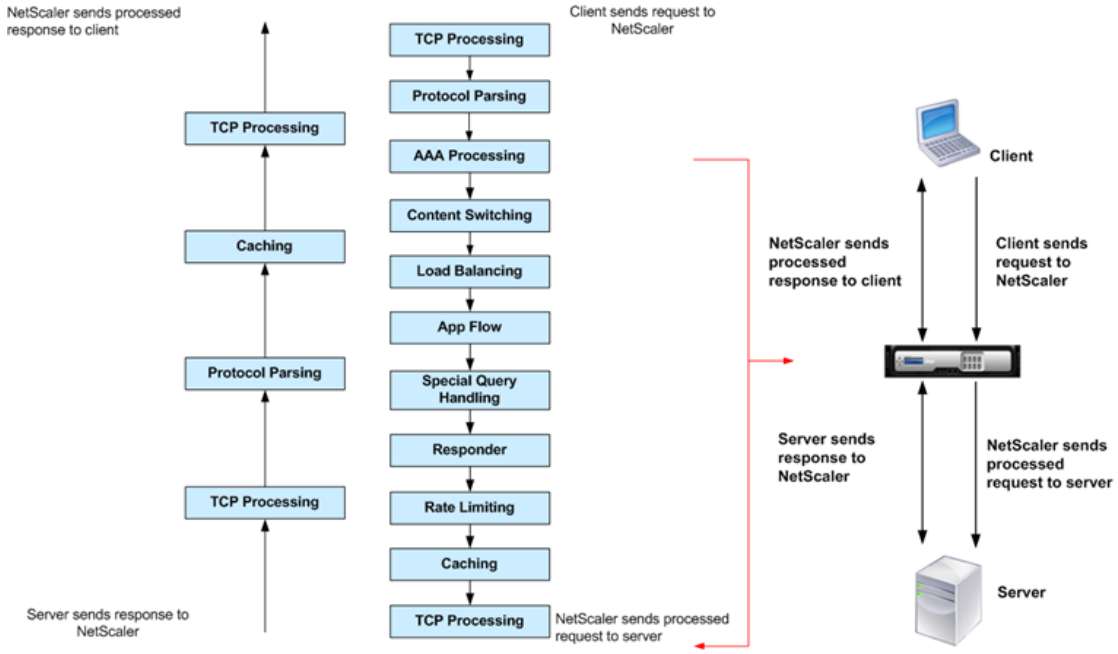
The following figure shows the L7 packet flow in the NetScaler.

Figure 1. L7 Packet Flow Diagram



The following figure shows the DataStream packet flow in the NetScaler. DataStream is supported for MySQL and MS SQL databases. For information about the DataStream feature, see "DataStream."

Figure 2. DataStream Packet Flow Diagram


NetScaler sends processed response to client
TCP Processing
Caching
Protocol Parsing
TCP Processing
Server sends response to NetScaler
TCP Processing
Protocol Parsing
AAA Processing
Content Switching
Load Balancing
App Flow
Special Query Handling
Responder
Rate Limiting
Caching
TCP Processing
Client sends request to NetScaler
NetScaler sends processed request to server
Client
NetScaler sends processed response to client
Client sends request to NetScaler
Server sends response to NetScaler
NetScaler sends processed request to server
Server

Installing NetScaler Virtual Appliances on XenServer

To install NetScaler virtual appliances on Citrix XenServer, you must first install XenServer on a machine with adequate system resources. To perform the NetScaler virtual appliance installation, you use Citrix XenCenter, which must be installed on a remote machine that can connect to the XenServer host through the network.

Note: After the initial configuration of the NetScaler appliance, if you want to upgrade the appliance to the latest software release, see Upgrading or Downgrading the System Software.

Prerequisites for Installing NetScaler Virtual Appliances on XenServer

Before you begin installing a virtual appliance, do the following:

- Install XenServer® version 5.6 or later on hardware that meets the minimum requirements.
- Install XenCenter® on a management workstation that meets the minimum system requirements.
- Obtain virtual appliance license files. For more information about virtual appliance licenses, see the *NetScaler VPX Licensing Guide* at http://support.citrix.com/article/ctx122426.

XenServer Hardware Requirements

The following table describes the minimum hardware requirements for a XenServer platform running NetScaler.

Table 1. Minimum System Requirements for XenServer Running NetScaler nCore virtual appliance

Component	Requirement
CPU	2 or more 64-bit x86 CPUs with virtualization assist (Intel-VT or AMD-V) enabled **Note:** To run NetScaler virtual appliance, hardware support for virtualization must be enabled on the XenServer host. Make sure that the BIOS option for virtualization support is not disabled. Consult your BIOS documentation for more details.
RAM	3 gigabytes (GB)
Disk space	Locally attached storage (PATA, SATA, SCSI) with 40 GB of disk space **Note:** XenServer installation creates a 4 GB partition for the XenServer host control domain; the remaining space is available for NetScaler virtual appliance and other virtual machines.
Network Interface Card (NIC)	One 1-Gbps NIC Recommended: Two 1-Gbps NICs

For information about installing XenServer, see the XenServer documentation at http://support.citrix.com/product/xens/.

The following table lists the virtual computing resources that XenServer must provide for each NetScaler nCore virtual appliance .

Table 2. Minimum Virtual Computing Resources Required for Running NetScaler ncore virtual appliance

Component	Requirement
Memory	2 GB
Virtual CPU (VCPU)	2
Virtual network interfaces	2

Note: For production use of NetScaler virtual appliance, Citrix recommends that CPU priority (in virtual machine properties) be set to the highest level, in order to improve scheduling behavior and network latency.

XenCenter System Requirements

XenCenter® is a Windows client application. It cannot run on the same machine as the XenServer® host. The following table describes the minimum system requirements.

Table 3. Minimum System Requirements for XenCenter Installation

Component	Requirement
Operating system	Windows 7, Windows XP, Windows Server 2003, or Windows Vista
.NET framework	Version 2.0 or later
CPU	750 megahertz (MHz) Recommended: 1 gigahertz (GHz) or faster
RAM	1 GB Recommended: 2 GB
Network Interface Card (NIC)	100 megabits per second (Mbps) or faster NIC

For information about installing XenCenter, see the XenServer documentation at http://support.citrix.com/product/xens/.

Installing NetScaler Virtual Appliances on XenServer by Using XenCenter

After you have installed and configured XenServer and XenCenter, you can use XenCenter to install virtual appliances on XenServer. The number of virtual appliances that you can install depends on the amount of memory available on the hardware that is running XenServer.

After you have used XenCenter to install the initial NetScaler virtual appliance (.xva image) on XenServer, you have the option to use Command Center to provision NetScaler virtual appliance. For more information, see the Command Center documentation.

To install NetScaler virtual appliances on XenServer by using XenCenter

1. Start XenCenter on your workstation.
2. On the Server menu, click Add.
3. In the Add New Server dialog box, in the Hostname text box, type the IP address or DNS name of the XenServer that you want to connect to.
4. In the User Name and Password text boxes, type the administrator credentials, and then click Connect. The XenServer name appears in the navigation pane with a green circle, which indicates that the XenServer is connected.
5. In the navigation pane, click the name of the XenServer on which you want to install NetScaler virtual appliance.
6. On the VM menu, click Import.
7. In the Import dialog box, in Import file name, browse to the location at which you saved the NetScaler virtual appliance .xva image file. Make sure that the Exported VM option is selected, and then click Next.
8. Select the XenServer on which you want to install the virtual appliance, and then click Next.
9. Select the local storage repository in which to store the virtual appliance, and then click Import to begin the import process.
10. You can add, modify, or delete virtual network interfaces as required. When finished, click Next.
11. Click Finish to complete the import process.

    Note: To view the status of the import process, click the **Log** tab.
12. If you want to install another virtual appliance, repeat steps 5 through 11.

Installing NetScaler Virtual Appliances on VMware ESX

Important: You cannot install standard VMware Tools or upgrade the VMware Tools version available on a NetScaler virtual appliance. VMware Tools for a NetScaler virtual appliance are delivered as part of the NetScaler software release.

Before installing NetScaler virtual appliances on VMware ESX, make sure that VMware ESX Server is installed on a machine with adequate system resources. To install NetScaler virtual appliances on VMware ESXi version 4.0 or later, you use VMware vSphere client. The client or tool must be installed on a remote machine that can connect to VMware ESX through the network.

After the installation, you can use vSphere client or vSphere Web Client to manage virtual appliances on VMware ESX 4.0 or later release.

Note:

The VMware vSphere client shows the guest operating system as "Sun Solaris 10" for NetScaler virtual machine. This is by design because VMware ESXi does not recognize FreeBSD.

After the initial configuration of the NetScaler appliance, if you want to upgrade the appliance to the latest software release, see "Upgrading or Downgrading the System Software."

Prerequisites for Installing NetScaler Virtual Appliances on VMware

Before you begin installing a virtual appliance, do the following:

- Install VMware ESX version 4.1 or later on hardware that meets the minimum requirements.
- Install VMware Client on a management workstation that meets the minimum system requirements.
- Download the NetScaler virtual appliance setup files.
- Label the physical network ports of VMware ESX.
- Obtain NetScaler license files. For more information about NetScaler virtual appliance licenses, see the *NetScaler VPX Licensing Guide* at http://support.citrix.com/article/ctx131110.

VMware ESX Hardware Requirements

The following table describes the minimum system requirements for VMware ESX servers running NetScaler ncore virtual appliance.

Table 1. Minimum System Requirements for VMware ESX Servers Running NetScaler nCore virtual appliance

Component	Requirement
CPU	2 or more 64-bit x86 CPUs with virtualization assist (Intel-VT or AMD-V) enabled **Note:** To run NetScaler virtual appliance, hardware support for virtualization must be enabled on the VMware ESX host. Make sure that the BIOS option for virtualization support is not disabled. For more information, see your BIOS documentation.
RAM	3 GB
Disk space	40 GB of disk space available
Network	One 1-Gbps NIC; Two 1-Gbps NICs recommended (The network interfaces must be Intel E1000.)

For information about installing VMware ESX, see http://www.vmware.com/.

The following table lists the virtual computing resources that the VMware ESX server must provide for each NetScaler ncore virtual appliance.

Table 2. Minimum Virtual Computing Resources Required for Running NetScaler ncore virtual appliance

Component	Requirement
Memory	2 GB
Virtual CPU (VCPU)	2 **Important:** Do not modify the system resources to create a virtual CPU (VCPU) in addition to the two CPUs already allotted to the virtual appliance.
Virtual network interfaces	1 **Note:** With ESX 4.0 or later, you can install a maximum of 10 virtual network interfaces if the VPX hardware is upgraded version to 7 or higher.
Disk space	20 GB **Note:** This is in addition to any disk requirements for the hypervisor.

Note: For production use of NetScaler virtual appliance, the full memory allocation must be reserved. CPU cycles (in MHz) equal to at least the speed of one CPU core of the ESX should also be reserved.

VMware vSphere Client System Requirements

VMware vSphere is a client application that can run on Windows and Linux operating systems. It cannot run on the same machine as the VMware ESX server. The following table describes the minimum system requirements.

Table 3. Minimum System Requirements for VMware vSphere Client Installation

Component	Requirement
Operating system	For detailed requirements from VMware, search for the "vSphere Compatibility Matrixes" PDF file at http://kb.vmware.com/.
CPU	750 megahertz (MHz); 1 gigahertz (GHz) or faster recommended
RAM	1 GB; 2 GB recommended
Network Interface Card (NIC)	100 Mbps or faster NIC

OVF Tool 1.0 System Requirements

OVF Tool is a client application that can run on Windows and Linux systems. It cannot run on the same machine as the VMware ESX server. The following table describes the minimum system requirements.

Table 4. Minimum System Requirements for OVF Tool Installation

Component	Requirement
Operating system	For detailed requirements from VMware, search for the "OVF Tool User Guide" PDF file at http://kb.vmware.com/.
CPU	750 MHz minimum, 1 GHz or faster recommended.
RAM	1 GB Minimum, 2 GB recommended.
Network Interface Card (NIC)	100 Mbps or faster NIC

For information about installing OVF, search for the "OVF Tool User Guide" PDF file at http://kb.vmware.com/.

Downloading the NetScaler virtual appliance Setup Files

The NetScaler virtual appliance setup package for VMware ESX follows the Open Virtual Machine (OVF) format standard. You can download the files from MyCitrix.com. You need a My Citrix account to log on. If you do not have a My Citrix account, access the home page at http://www.mycitrix.com, click the New Users link, and follow the instructions to create a new My Citrix account.

Once logged on, navigate the following path from the My Citrix home page:

MyCitrix.com > Downloads > NetScaler > Virtual Appliances.

Copy the following files to a workstation on the same network as the ESX server. Copy all three files into the same folder.

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (for example, NSVPX-ESX-9.3-39.8-disk1.vmdk)
- NSVPX-ESX-<release number>-<build number>.ovf (for example, NSVPX-ESX-9.3-39.8.ovf)
- NSVPX-ESX-<release number>-<build number>.mf (for example, NSVPX-ESX-9.3-39.8.mf)

Labeling the Physical Network Ports of VMware ESX

Before installing a NetScaler virtual appliance, label of all the interfaces that you plan to assign to virtual appliances, in a unique format. Citrix recommends the following format: NS_NIC_1_1, NS_NIC_1_2, and so on. In large deployments, labeling in a unique format helps in quickly identifying the interfaces that are allocated to the NetScaler virtual appliance among other interfaces used by other virtual machines, such as Windows and Linux. Such labeling is especially important when different types of virtual machines share the same interfaces.

To label the physical network ports of VMware ESX server

1. Log on to the VMware ESX server by using the vSphere client.
2. On the vSphere client, select the Configuration tab, and then click Networking.
3. At the top-right corner, click Add Networking.
4. In the Add Network Wizard, for **Connection Type**, select **Virtual Machine**, and then click Next.
5. Scroll through the list of vSwitch physical adapters, and choose the physical port that will map to interface 1/1 on the virtual appliances.
6. Enter NS_NIC_1_1 as the name of the vSwitch that will be associated with interface 1/1 of the virtual appliances.
7. Click Next to finish the vSwitch creation. Repeat the procedure, beginning with step 2, to add any additional interfaces to be used by your virtual appliances. Label the interfaces sequentially, in the correct format (for example, NS_NIC_1_2).

Installing NetScaler Virtual Appliances on VMware ESX 4.0 or Later

After you have installed and configured VMware ESX 4.0 or later, you can use the VMware vSphere client to install virtual appliances on the VMware ESX. The number of virtual appliances that you can install depends on the amount of memory available on the hardware that is running VMware ESX.

To install NetScaler virtual appliances on VMware ESX 4.0 or later by using VMware vSphere Client

1. Start the VMware vSphere client on your workstation.
2. In the IP address / Name text box, type the IP address of the VMware ESX server that you want to connect to.
3. In the User Name and Password text boxes, type the administrator credentials, and then click Login.
4. On the File menu, click Deploy OVF Template.
5. In the Deploy OVF Template dialog box, in Deploy from file, browse to the location at which you saved the NetScaler virtual appliance setup files, select the .ovf file, and click Next.
6. Map the networks shown in the virtual appliance OVF template to the networks that you configured on the ESX host. Click Next to start installing a virtual appliance on VMware ESX. When installation is complete, a pop-up window informs you of the successful installation.
7. You are now ready to start the NetScaler virtual appliance. In the navigation pane, select the NetScaler virtual appliance that you have just installed and, from the right-click menu, select Power On. Click the Console tab to emulate a console port.
8. If you want to install another virtual appliance, repeat steps 4 through 6.

Installing Citrix NetScaler Virtual Appliances on Microsoft Hyper-V Servers

To install Citrix NetScaler virtual appliances on Microsoft Windows Server, you must first install Windows Server, with the Hyper-V role enabled, on a machine with adequate system resources. While installing the Hyper-V role, be sure to specify the network interface cards (NICs) on the server that Hyper-V will use to create the virtual networks. You can reserve some NICs for the host. Use Hyper-V Manager to perform the NetScaler virtual appliance installation.

NetScaler virtual appliance for Hyper-V is delivered in virtual hard disk (VHD) format. It includes the default configuration for elements such as CPU, network interfaces, and hard-disk size and format. After you install NetScaler virtual appliance, you can configure the network adapters on virtual appliance, add virtual NICs, and then assign the NetScaler IP address, subnet mask, and gateway, and complete the basic configuration of the virtual appliance.

Note:

After the initial configuration of the NetScaler appliance, if you want to upgrade the appliance to the latest software release, see "Upgrading or Downgrading the System Software."

Prerequisites for Installing NetScaler Virtual Appliance on Microsoft Servers

Before you begin installing a virtual appliance, do the following:

- Enable the Hyper-V role on Windows Servers . For more information, see http://technet.microsoft.com/en-us/library/ee344837(WS.10).aspx.
- Download the virtual appliance setup files.
- Obtain NetScaler virtual appliance license files. For more information about NetScaler virtual appliance licenses, see the *NetScaler VPX Licensing Guide* at http://support.citrix.com/article/ctx131110.

Microsoft Server Hardware Requirements

The following table describes the minimum system requirements for Microsoft Servers .

Table 1. Minimum System Requirements for Microsoft Servers

Component	Requirement
CPU	1.4 GHz 64-bit processor
RAM	3 GB
Disk Space	32 GB or greater

The following table lists the virtual computing resources for each NetScaler virtual appliance.

Table 2. Minimum Virtual Computing Resources Required for Running NetScaler Virtual Appliance

Component	Requirement
RAM	2 GB
Virtual CPU	2
Disk Space	20 GB
Virtual Network Interfaces	1

Downloading the NetScaler Virtual Appliance Setup Files

NetScaler virtual appliance for Hyper-V is delivered in virtual hard disk (VHD) format. You can download the files from MyCitrix.com. You will need a My Citrix account to log on. If you do not have a My Citrix account, access the home page at http://www.mycitrix.com, click the New Users link, and follow the instructions to create a new My Citrix account.

To download the NetScaler virtual appliance setup files

1. In a Web browser, go to http://www.citrix.com/ and click My Citrix.
2. Type your user name and password.
3. Click Downloads.
4. In Search Downloads by Product, select NetScaler.
5. Under Virtual Appliances, click NetScaler VPX.
6. Copy the compressed file to your server.

Installing NetScaler Virtual Appliance on Microsoft Servers

After you have enabled the Hyper-V role on Microsoft Server and extracted the virtual appliance files, you can use Hyper-V Manager to install NetScaler virtual appliance. After you import the virtual machine, you need to configure the virtual NICs by associating them to the virtual networks created by Hyper-V.

You can configure a maximum of eight virtual NICs. Even if the physical NIC is DOWN, the virtual appliance assumes that the virtual NIC is UP, because it can still communicate with the other virtual appliances on the same host (server).

Note: You cannot change any settings while the virtual appliance is running. Shut down the virtual appliance and then make changes.

To install NetScaler Virtual Appliance on Microsoft Server by using Hyper-V Manager

1. To start Hyper-V Manager, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In the navigation pane, under Hyper-V Manager, select the server on which you want to install NetScaler virtual appliance.
3. On the **Action** menu, click **Import Virtual Machine**.
4. In the **Import Virtual Machine** dialog box, in **Location**, specify the path of the folder that contains the NetScaler virtual appliance software files, and then select **Copy the virtual machine (create a new unique ID)**. This folder is the parent folder that contains the Snapshots, Virtual Hard Disks, and Virtual Machines folders.

   Note: If you received a compressed file, make sure that you extract the files into a folder before you specify the path to the folder.
5. Click **Import**.
6. Verify that the virtual appliance that you imported is listed under **Virtual Machines**.
7. To install another virtual appliance, repeat steps 2 through 6.

   Important: Make sure that you extract the files to a different folder in step 4.

To configure virtual NICs on the NetScaler Virtual Appliance

1. Select the virtual appliance that you imported, and then on the **Action** menu, select **Settings**.
2. In the **Settings for** <virtual appliance name> dialog box, click **Add Hardware** in the left pane.
3. In the right pane, from the list of devices, select **Network Adapter**.
4. Click **Add**.
5. Verify that **Network Adapter** (**not connected**) appears in the left pane.
6. Select the network adapter in the left pane.
7. In the right pane, from the **Network** drop-down list, select the virtual network to connect the adapter to.
8. To select the virtual network for additional network adapters that you want to use, repeat steps 6 and 7.
9. Click **Apply**, and then click **OK**.

To configure NetScaler Virtual Appliance

1. Right-click the virtual appliance that you previously installed, and then select **Start**.
2. Access the console by double-clicking the virtual appliance.
3. Type the NetScaler IP address, subnet mask, and gateway for your virtual appliance.

You have completed the basic configuration of your virtual appliance. Type the IP address in a Web browser to access the virtual appliance.

Configuring the Basic System Settings

After installing a Citrix NetScaler virtual appliance, you need to access it to configure the basic settings. Initially, you must access the NetScaler command line through the respective management application of the virtualization host (either Citrix XenCenter for Citrix XenServer or VMware vSphere client for VMware ESX) to specify a NetScaler IP (NSIP) address, subnet mask, and default gateway. The NSIP is the management address at which you can then access the NetScaler command line, through an SSH client, or access the configuration utility. You can use either of these access methods, or the console, to continue with basic configuration.

To access the configuration utility, type the NSIP into the address field of any browser (for example, `http://<NSIP_address>`). You need Java RunTime Environment (JRE) version 1.6 or later.

Setting Up the Initial Configuration by Using the NetScaler Virtual Appliance Console

Your first task after installing a NetScaler virtual appliance on a virtualization host is to use the NetScaler virtual appliance console in the XenCenter client or vSphere client to configure the following initial settings.

Note: If you have installed a virtual appliance on XenServer by using Command Center, you do not have to configure these settings. Command Center implicitly configures the settings during installation. For more information about provisioning virtual appliance from Command Center, see the "Command Center" documentation.

NetScaler IP address (NSIP):

The IP address at which you access a NetScaler or a NetScaler virtual appliance for management purposes. A physical NetScaler or virtual appliance can have only one NSIP. You must specify this IP address when you configure the virtual appliance for the first time. You cannot remove an NSIP address.

Netmask:

The subnet mask associated with the NSIP address.

Default Gateway:

You must add a default gateway on the virtual appliance if you want access it through SSH or the configuration utility from an administrative workstation or laptop that is on a different network.

To configure the initial settings on the virtual appliance through the virtual appliance Console by using the management application

1. Connect to the XenServer or VMware ESX server on which the virtual appliance is installed by using XenCenter or vSphere client, respectively.
2. In the details pane, on the Console tab, log on to the virtual appliance by using the administrator credentials.
3. At the prompts, enter the NSIP address, subnet mask, and default gateway, and then save the configuration.

After you have set up an initial configuration through the NetScaler virtual appliance Console in the management application, you can use either the NetScaler command-line

interface or the configuration utility to complete the configuration or to change the initial settings.

Configuring NetScaler Virtual Appliance by Using the Command Line Interface

You can use the command line interface to set up the NSIP, Mapped IP (MIP), Subnet IP (SNIP), and hostname. You can also configure advanced network settings and change the time zone.

For information about MIP, SNIP, other NetScaler-owned IP addresses, and network settings, see "Configuring NetScaler-Owned IP Addresses."

To complete initial configuration by using the command line interface

1. Use either the SSH client or the NetScaler virtual appliance Console in XenCenter to access the command line interface.
2. Log on to the virtual appliance, using the administrator credentials.
3. At the command prompt, type `config ns` to run the configuration script.
4. To complete the initial configuration, follow the prompts.

You have now completed the basic configuration of the virtual appliance. To continue the configuration process, choose one of the following options:

Citrix NetScaler Load Balancing Switch

If you are configuring the virtual appliance as a standard NetScaler load balancing switch with other licensed features, see "Traffic Management."

Citrix® Application Firewall™

If you are configuring the virtual appliance as a standalone application firewall, see "Application Firewall."

For more information about the various features supported on the NetScaler virtual appliance, see Features at a Glance.

Configuring NetScaler Virtual Appliance by Using the Configuration Utility

To use the Setup Wizard to set up the NetScaler virtual appliance, you must access the configuration utility from your Web browser. You can use the Setup Wizard to configure the NSIP, MIP, SNIP, hostname, and default gateway. You can also configure settings for a Web application by using an application template. You can also configure the appliance as a load balancer for Citrix XenDesktop or Citrix XenApp.

For information about MIP, SNIP, other NetScaler-owned IP addresses, and network settings, see "Configuring NetScaler-Owned IP Addresses."

For information about application templates, see "AppExpert."

For information about the load balancing feature of a virtual appliance, see "Traffic Management."

To configure initial settings by using the configuration utility

1. In the address field of a Web browser, type: `http://<NSIP address>`
2. In User Name and Password, type the administrator credentials.
3. In Start in, select Configuration, and then click Login.
4. In the Setup Wizard, click Next and follow the instructions.

You have now completed the basic configuration of the virtual appliance. To continue the configuration process, choose one of the following options:

Citrix NetScaler Load Balancing Switch

If you are configuring the virtual appliance as a standard NetScaler load balancing switch with other licensed features, see "Traffic Management."

Citrix® Application Firewall™

If you are configuring the virtual appliance as a standalone application firewall, see "Application Firewall."

For more information about the various features supported on the NetScaler virtual appliance, see Features at a Glance.

Understanding Common Network Topologies

As described in "Physical Deployment Modes," you can deploy the Citrix NetScaler appliance either inline between the clients and servers or in one-arm mode. Inline mode uses a two-arm topology, which is the most common type of deployment.

Setting Up Common Two-Arm Topologies

In a two-arm topology, one network interface is connected to the client network and another network interface is connected to the server network, ensuring that all traffic flows through the appliance. This topology might require you to reconnect your hardware and also might result in a momentary downtime. The basic variations of two-arm topology are multiple subnets, typically with the appliance on a public subnet and the servers on a private subnet, and transparent mode, with both the appliance and the servers on the public network.

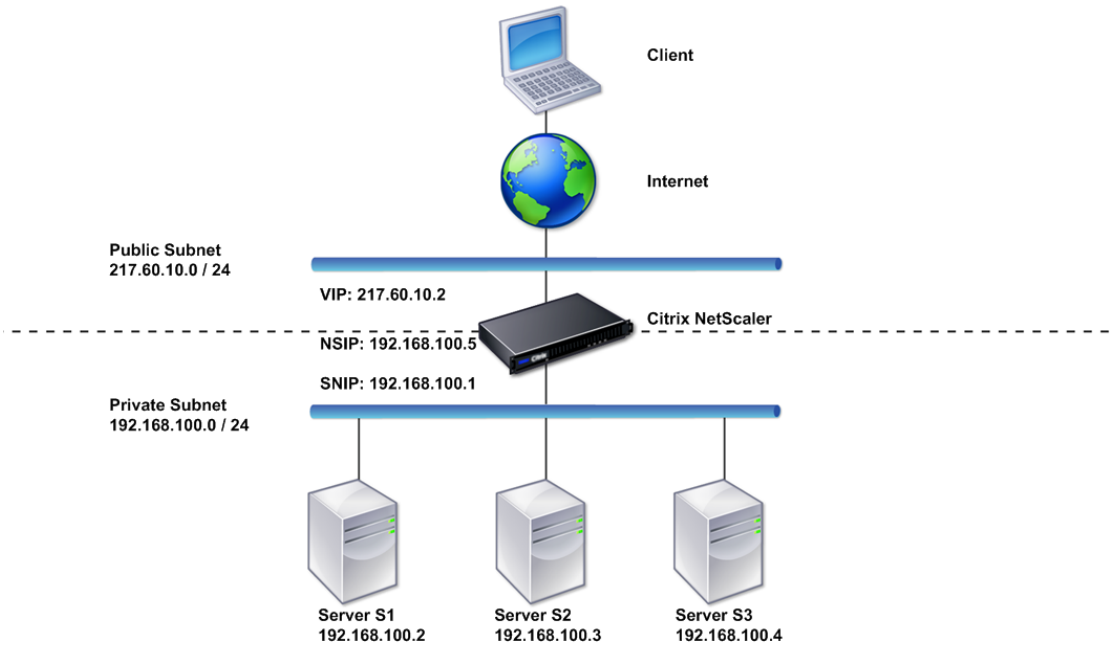
Setting Up a Simple Two-Arm Multiple Subnet Topology

One of the most commonly used topologies has the NetScaler appliance inline between the clients and the servers, with a virtual server configured to handle the client requests. This configuration is used when the clients and servers reside on different subnets. In most cases, the clients and servers reside on public and private subnets, respectively.

For example, consider an appliance deployed in two-arm mode for managing servers S1, S2, and S3, with a virtual server of type HTTP configured on the appliance, and with HTTP services running on the servers. The servers are on a private subnet and a SNIP is configured on the appliance to communicate with the servers. The Use SNIP (USNIP) option must be enabled on the appliance so that it uses the SNIP instead of the MIP.

As shown in the following figure, the VIP is on public subnet 217.60.10.0, and the NSIP, the servers, and the SNIP are on private subnet 192.168.100.0/24.

Figure 1. Topology Diagram for Two-Arm Mode, Multiple Subnets



Task overview: To deploy a NetScaler appliance in two-arm mode with multiple subnets

1. Configure the NSIP and default gateway, as described in "Configuring the NetScaler IP Address (NSIP)."

2. Configure the SNIP, as described in "Configuring Subnet IP Addresses."

3. Enable the USNIP option, as described in "To enable or disable USNIP mode."

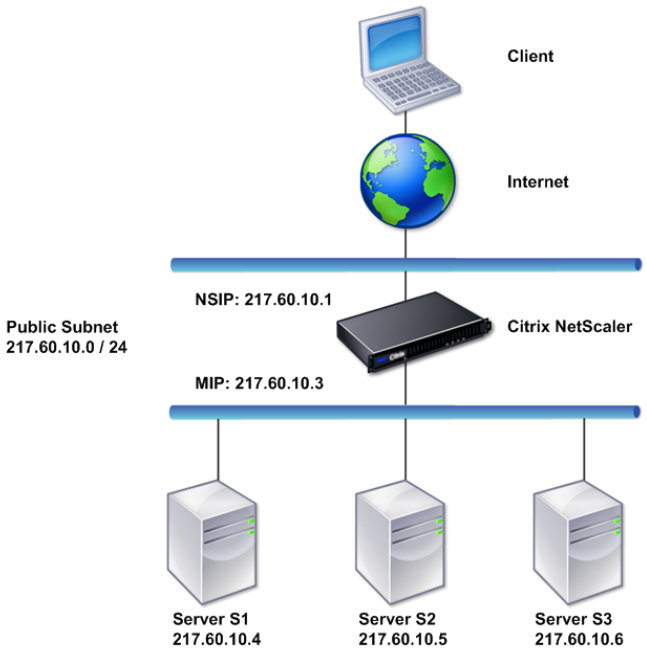
4. Configure the virtual server and the services, as described in "Creating a Virtual Server" and "Configuring Services."

5. Connect one of the network interfaces to a private subnet and the other interface to a public subnet.

Setting Up a Simple Two-Arm Transparent Topology

Use transparent mode if the clients need to access the servers directly, with no intervening virtual server. The server IP addresses must be public because the clients need to be able to access them. In the example shown in the following figure, a NetScaler appliance is placed between the client and the server, so the traffic must pass through the appliance. You must enable L2 mode for bridging the packets. The NSIP and MIP are on the same public subnet, 217.60.10.0/24.

Figure 1. Topology Diagram for Two-Arm, Transparent Mode



Task overview: To deploy a NetScaler in two-arm, transparent mode

1. Configure the NSIP, MIP, and default gateway, as described in "Configuring a NetScaler by Using the Command Line Interface."
2. Enable L2 mode, as described in "Enabling and Disabling Layer 2 Mode."
3. Configure the default gateway of the managed servers as the MIP.
4. Connect the network interfaces to the appropriate ports on the switch.

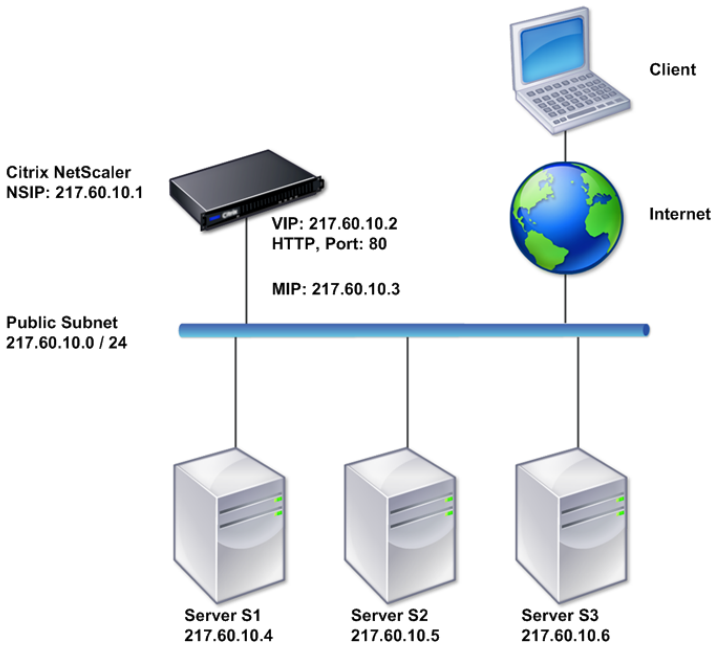
Setting Up Common One-Arm Topologies

The two basic variations of one-arm topology are with a single subnet and with multiple subnets.

Setting Up a Simple One-Arm Single Subnet Topology

You can use a one-arm topology with a single subnet when the clients and servers reside on the same subnet. For example, consider a NetScaler deployed in one-arm mode for managing servers S1, S2, and S3. A virtual server of type HTTP is configured on a NetScaler, and HTTP services are running on the servers. As shown in the following figure, the NetScaler IP address (NSIP), the Mapped IP address (MIP), and the server IP addresses are on the same public subnet, 217.60.10.0/24.

Figure 1. Topology Diagram for One-Arm Mode, Single Subnet



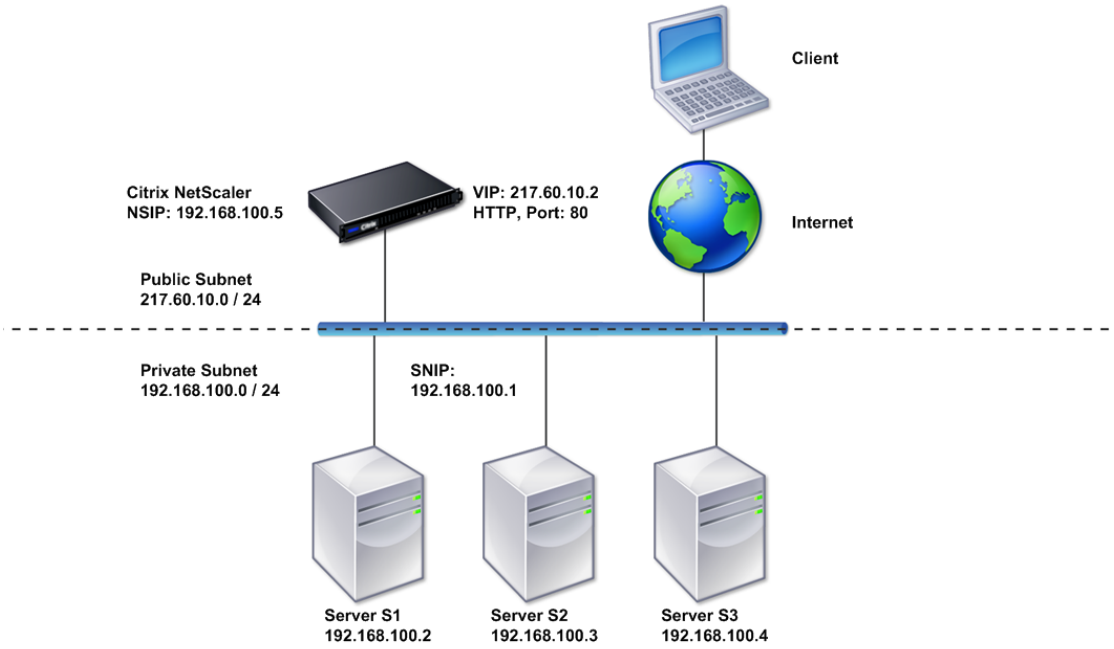
Task overview: To deploy a NetScaler in one-arm mode with a single subnet

1. Configure the NSIP, MIP, and the default gateway, as described in "Configuring the NetScaler IP Address (NSIP)".
2. Configure the virtual server and the services, as described in "Creating a Virtual Server" and "Configuring Services".
3. Connect one of the network interfaces to the switch.

Setting Up a Simple One-Arm Multiple Subnet Topology

You can use a one-arm topology with multiple subnets when the clients and servers reside on the different subnets. For example, consider a NetScaler appliance deployed in one-arm mode for managing servers S1, S2, and S3, with the servers connected to switch SW1 on the network. A virtual server of type HTTP is configured on the appliance, and HTTP services are running on the servers. These three servers are on the private subnet, so a subnet IP address (SNIP) is configured to communicate with them. The Use Subnet IP address (USNIP) option must be enabled so that the appliance uses the SNIP instead of a MIP. As shown in the following figure, the virtual IP address (VIP) is on public subnet 217.60.10.0/24; the NSIP, SNIP, and the server IP addresses are on private subnet 192.168.100.0/24.

Figure 1. Topology Diagram for One-Arm Mode, Multiple Subnets



Task overview: To deploy a NetScaler appliance in one-arm mode with multiple subnets

1. Configure the NSIP and the default gateway, as described in "Configuring the NetScaler IP Address (NSIP)".

2. Configure the SNIP and enable the USNIP option, as described in "Configuring Subnet IP Addresses".

3. Configure the virtual server and the services, as described in "Creating a Virtual Server" and "Configuring Services".

4. Connect one of the network interfaces to the switch.

Configuring System Management Settings

Once your initial configuration is in place, you can configure settings to define the behavior of the Citrix NetScaler appliance and facilitate connection management. You have a number of options for handling HTTP requests and responses. Routing, bridging, and MAC based forwarding modes are available for handling packets not addressed to the NetScaler. You can define the characteristics of your network interfaces and can aggregate the interfaces. To prevent timing problems, you can synchronize the NetScaler clock with a Network Time Protocol (NTP) server. The NetScaler can operate in various DNS modes, including as an authoritative domain name server (ADNS). You can set up SNMP for system management and customize syslog logging of system events. Before deployment, verify that your configuration is complete and correct.

Configuring System Settings

Configuration of system settings includes basic tasks such as configuring HTTP ports to enable connection keep-alive and server offload, setting the maximum number of connections for each server, and setting the maximum number of requests per connection. You can enable client IP address insertion for situations in which a proxy IP address is not suitable, and you can change the HTTP cookie version.

You can also configure a NetScaler appliance to open FTP connections on a controlled range of ports instead of ephemeral ports for data connections. This improves security, because opening all ports on the firewall is insecure. You can set the range anywhere from 1,024 to 64,000.

Before deployment, go through the verification checklists to verify your configuration. To configure HTTP parameters and the FTP port range, use the NetScaler configuration utility.

You can modify the types of HTTP parameters described in the following table.

Table 1. HTTP Parameters

Parameter Type	Specifies
HTTP Port Information	The web server HTTP ports used by your managed servers. If you specify the ports, the appliance performs request switching for any client request that has a destination port matching a specified port. **Note:** If an incoming client request is not destined for a service or a virtual server that is specifically configured on the appliance, the destination port in the request must match one of the globally configured HTTP ports. This allows the appliance to perform connection keep-alive and server off-load.

Limits	The maximum number of connections to each managed server, and the maximum number of requests sent over each connection. For example, if you set Max Connections to 500, and the appliance is managing three servers, it can open a maximum of 500 connections to each of the three servers. By default, the appliance can create an unlimited number of connections to any of the servers it manages. To specify an unlimited number of requests per connection, set Max Requests to 0. **Note:** If you are using the Apache HTTP server, you must set Max Connections equal to the value of the MaxClients parameter in the Apache httpd.conf file. Setting this parameter is optional for other web servers.
Client IP Insertion	Enable/disable insertion of the client's IP address into the HTTP request header. You can specify a name for the header field in the adjacent text box. When a web server managed by an appliance receives a mapped IP address or a subnet IP address, the server identifies it as the client's IP address. Some applications need the client's IP address for logging purposes or to dynamically determine the content to be served by the web server. You can enable insertion of the actual client IP address into the HTTP header request sent from the client to one, some, or all servers managed by the appliance. You can then access the inserted address through a minor modification to the server (using an Apache module, ISAPI interface, or NSAPI interface).
Cookie Version	The HTTP cookie version to use when COOKIEINSERT persistence is configured on a virtual server. The default, version 0, is the most common type on the Internet. Alternatively, you can specify version 1.
Requests/Responses	Options for handling certain types of requests, and enable/disable logging of HTTP error responses.
Server Header Insertion	Insert a server header in NetScaler-generated HTTP responses.

To configure HTTP parameters by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Settings, click Change HTTP parameters.
3. In the Configure HTTP parameters dialog box, specify values for some or all of the parameters that appear under the headings listed in the table above.
4. Click OK.

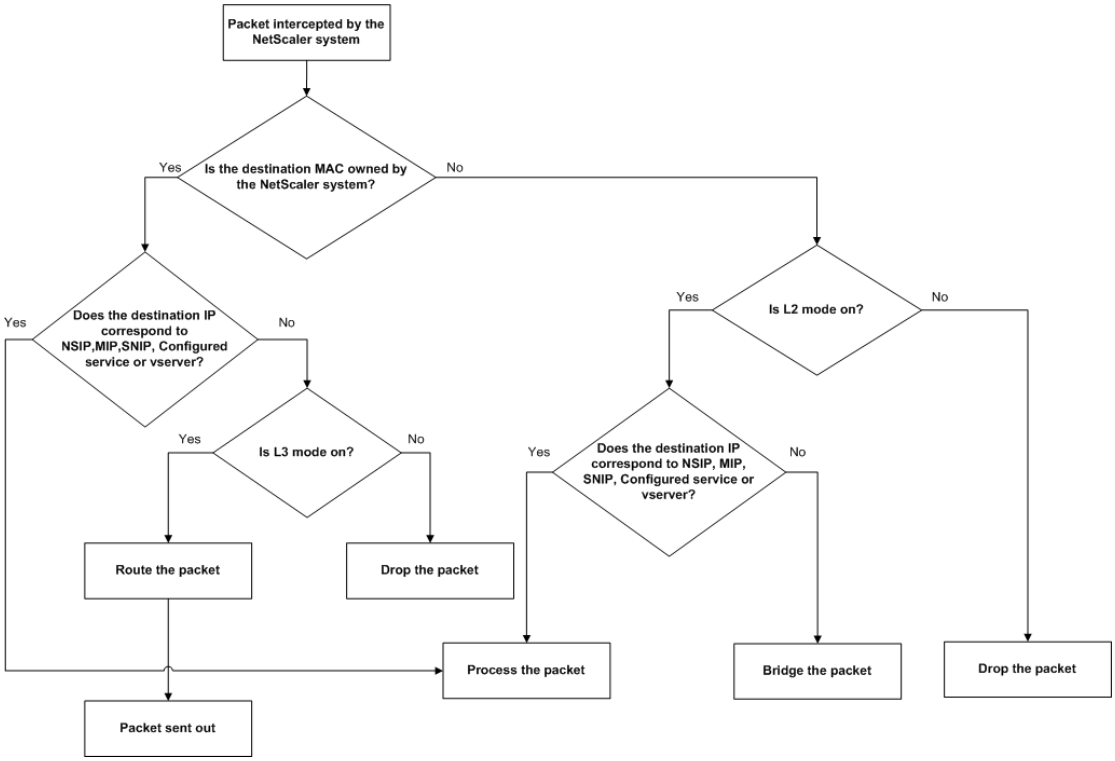
To set the FTP port range by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Settings, click Change global system settings.
3. Under FTP Port Range, in the Start Port and End Port text boxes, type the lowest and highest port numbers, respectively, for the range you want to specify (for example, 5000 and 6000).
4. Click OK.

Configuring Modes of Packet Forwarding

The NetScaler appliance can either route or bridge packets that are not destined for an IP address owned by the appliance (that is, the IP address is not the NSIP, a MIP, a SNIP, a configured service, or a configured virtual server). By default, L3 mode (routing) is enabled and L2 mode (bridging) is disabled, but you can change the configuration. The following flow chart shows how the appliance evaluates packets and either processes, routes, bridges, or drops them.

Figure 1. Interaction between Layer 2 and Layer 3 Modes



An appliance can use the following modes to forward the packets it receives:

- Layer 2 (L2) Mode
- Layer 3 (L3) Mode
- MAC-Based Forwarding Mode

Enabling and Disabling Layer 2 Mode

Layer 2 mode controls the Layer 2 forwarding (bridging) function. You can use this mode to configure a NetScaler appliance to behave as a Layer 2 device and bridge the packets that are not destined for it. When this mode is enabled, packets are not forwarded to any of the MAC addresses, because the packets can arrive on any interface of the appliance and each interface has its own MAC address.

With Layer 2 mode disabled (which is the default), the appliance drops packets that are not destined for one of its MAC address. If another Layer 2 device is installed in parallel with the appliance, Layer 2 mode must be disabled to prevent bridging (Layer 2) loops. You can use the configuration utility or the command line to enable Layer 2 mode.

Note: The appliance does not support spanning tree protocol. To avoid loops, if you enable L2 mode, do not connect two interfaces on the appliance to the same broadcast domain.

To enable or disable Layer 2 mode by using the command line interface

At the command prompt, type the following commands to enable/disable Layer 2 mode and verify that it has been enabled/disabled:

- `enable ns mode <Mode>`
- `disable ns mode <Mode>`
- `show ns mode`

Examples

```
> enable ns mode l2
 Done
> show ns mode

     Mode              Acronym        Status
     -------           -------        ------
 1)  Fast Ramp           FR            ON
 2)  Layer 2 mode         L2            ON
 .
 .
 .
 Done
>

> disable ns mode l2
 Done
> show ns mode
```

```
    Mode                Acronym        Status
    -------             -------        ------
1)  Fast Ramp             FR             ON
2)  Layer 2 mode          L2             OFF
.
.
.
Done
>
```

To enable or disable Layer 2 mode by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features, click Configure modes.
3. In the Configure Modes dialog box, to enable Layer 2 mode, select the Layer 2 Mode check box. To disable Layer 2 mode, clear the check box.
4. Click OK. The Enable/Disable Mode(s)? message appears in the details pane.
5. Click Yes.

Enabling and Disabling Layer 3 Mode

Layer 3 mode controls the Layer 3 forwarding function. You can use this mode to configure a NetScaler appliance to look at its routing table and forward packets that are not destined for it. With Layer 3 mode enabled (which is the default), the appliance performs route table lookups and forwards all packets that are not destined for any appliance-owned IP address. If you disable Layer 3 mode, the appliance drops these packets.

To enable or disable Layer 3 mode by using the command line interface

At the command prompt, type the following commands to enable/disable Layer 3 mode and verify that it has been enabled/disabled:

- `enable ns mode <Mode>`
- `disable ns mode <Mode>`
- `show ns mode`

Examples

```
> enable ns mode l3
 Done
> show ns mode

    Mode                    Acronym        Status
    -------                 -------        ------
 1)  Fast Ramp                FR            ON
 2)  Layer 2 mode             L2            OFF
 .
 .
 .
 9)  Layer 3 mode (ip forwarding)  L3            ON
 .
 .
 .
 Done
>

> disable ns mode l3
 Done
> show ns mode

    Mode                    Acronym        Status
    -------                 -------        ------
 1)  Fast Ramp                FR            ON
 2)  Layer 2 mode             L2            OFF
```

```
.
.
.
9)  Layer 3 mode (ip forwarding)  L3              OFF
.
.
.
Done
>
```

To enable or disable Layer 3 mode by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features, click Configure modes.
3. In the Configure Modes dialog box, to enable Layer 3 mode, select the Layer 3 Mode (IP Forwarding) check box. To disable Layer 3 mode, clear the check box.
4. Click OK. The Enable/Disable Mode(s)? message appears in the details pane.
5. Click Yes.

Enabling and Disabling MAC-Based Forwarding Mode

You can use MAC-based forwarding to process traffic more efficiently and avoid multiple-route or ARP lookups when forwarding packets, because the NetScaler appliance remembers the MAC address of the source. To avoid multiple lookups, the appliance caches the source MAC address of every connection for which it performs an ARP lookup, and it returns the data to the same MAC address.

MAC-based forwarding is useful when you use VPN devices because the appliance ensures that all traffic flowing through a particular VPN passes through the same VPN device.

The following figure shows the process of MAC-based forwarding.

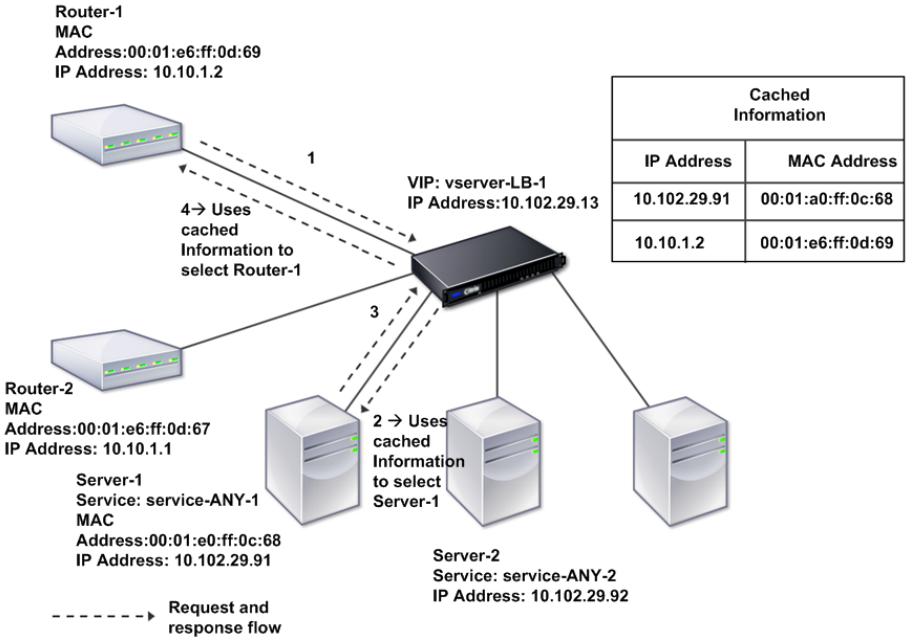


Figure 1. MAC-Based Forwarding Process

When MAC-based forwarding is enabled, the appliance caches the MAC address of:

- The source (a transmitting device such as router, firewall, or VPN device) of the inbound connection.
- The server that responds to the requests.

When a server responds through an appliance, the appliance sets the destination MAC address of the response packet to the cached address, ensuring that the traffic flows in a symmetric manner, and then forwards the response to the client. The process bypasses the route table lookup and ARP lookup functions. However, when an appliance initiates a connection, it uses the route and ARP tables for the lookup function. To enable MAC-based forwarding, use the configuration utility or the command line.

Some deployments require the incoming and outgoing paths to flow through different routers. In these situations, MAC-based forwarding breaks the topology design. For a global server load balancing (GSLB) site that requires the incoming and outgoing paths to flow through different routers, you must disable MAC-based forwarding and use the appliance's default router as the outgoing router.

With MAC-based forwarding disabled and Layer 2 or Layer 3 connectivity enabled, a route table can specify separate routers for outgoing and incoming connections. To disable MAC-based forwarding, use the configuration utility or the command line.

To enable or disable MAC-based forwarding by using the command line interface

At the command prompt, type the following commands to enable/disable MAC-based forwarding mode and verify that it has been enabled/disabled:

- `enable ns mode <Mode>`
- `disable ns mode <Mode>`
- `show ns mode`

Example

```
> enable ns mode mbf
 Done
> show ns mode

    Mode                  Acronym         Status
    -------               -------         ------
 1) Fast Ramp               FR              ON
 2) Layer 2 mode            L2              OFF
 .
 .
 .
 6) MAC-based forwarding    MBF             ON
 .
 .
 .
 Done
>

> disable ns mode mbf
 Done
> show ns mode
```

```
   Mode                  Acronym         Status
   -------               -------         ------
1) Fast Ramp               FR              ON
2) Layer 2 mode            L2              OFF
.
.
.
6) MAC-based forwarding    MBF             OFF
.
.
.
Done
>
```

To enable or disable MAC-based forwarding by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features group, click Configure modes.
3. In the Configure Modes dialog box, to enable MAC-based forwarding mode, select the MAC Based Forwarding check box. To disable MAC-based forwarding mode, clear the check box.
4. Click OK. The Enable/Disable Mode(s)? message appears in the details pane.
5. Click Yes.

Configuring Network Interfaces

NetScaler interfaces are numbered in slot/port notation. In addition to modifying the characteristics of individual interfaces, you can configure virtual LANs to restrict traffic to specific groups of hosts. You can also aggregate links into high-speed channels.

Virtual LANs

The NetScaler supports (Layer 2) port and IEEE802.1Q tagged virtual LANs (VLANs). VLAN configurations are useful when you need to restrict traffic to certain groups of stations. You can configure a network interface to belong to multiple VLANs by using IEEE 802.1q tagging.

You can bind your configured VLANs to IP subnets. The NetScaler (if it is configured as the default router for the hosts on the subnets) then performs IP forwarding between these VLANs. A NetScaler supports the following types of VLANs.

Default VLAN

By default, the network interfaces on a NetScaler are included in a single, port-based VLAN as untagged network interfaces. This default VLAN has a VID of 1 and exists permanently. It cannot be deleted, and its VID cannot be changed.

Port-Based VLANs

A set of network interfaces that share a common, exclusive, Layer 2 broadcast domain define the membership of a port-based VLAN. You can configure multiple port-based VLANs. When you add an interface to a new VLAN as an untagged member, it is automatically removed from the default VLAN.

Tagged VLAN

A network interface can be a tagged or untagged member of a VLAN. Each network interface is an untagged member of only one VLAN (its native VLAN). The untagged network interface forwards the frames for the native VLAN as untagged frames. A tagged network interface can be a part of more than one VLAN. When you configure tagging, be sure that both ends of the link have matching VLAN settings. You can use the configuration utility to define a tagged VLAN (nsvlan) that can have any ports bound as tagged members of the VLAN. Configuring this VLAN requires a reboot of the NetScaler and therefore must be done during initial network configuration.

Link Aggregate Channels

Link aggregation combines incoming data from multiple ports into a single high speed link. Configuring the link aggregate channel increases the capacity and availability of the communication channel between a NetScaler and other connected devices. An aggregated link is also referred to as a channel.

When a network interface is bound to a channel, the channel parameters have precedence over the network interface parameters. A network interface can be bound to only one channel. Binding a network interface to a link aggregate channel changes the VLAN configuration. That is, binding network interfaces to a channel removes them from the VLANs that they originally belonged to and adds them to the default VLAN. However, you can bind the channel back to the old VLAN, or to a new one. For example, if you have bound network interfaces 1/2 and 1/3 to a VLAN with ID 2, and then you bind them to link aggregate channel LA/1, the network interfaces are moved to the default VLAN, but you can bind them to VLAN 2.

Note: You can also use Link Aggregation Control Protocol (LACP) to configure link aggregation. For more information, see "Configuring Link Aggregation by Using the Link Aggregation Control Protocol."

Configuring Clock Synchronization

You can configure your NetScaler appliance to synchronize its local clock with a Network Time Protocol (NTP) server. This ensures that its clock has the same date and time settings as the other servers on your network. NTP uses User Datagram Protocol (UDP) port 123 as its transport layer. You have to add NTP servers in the NTP configuration file so that the appliance periodically gets updates from these servers.

If you do not have a local NTP server, you can find a list of public, open access, NTP servers at the official NTP site at http://www.ntp.org.

To configure clock synchronization on your appliance

1. Log on to the command line and enter the `shell` command.

2. At the shell prompt, copy the ntp.conf file from the /etc directory to the /nsconfig directory. If the file already exists in the /nsconfig directory, make sure that you remove the following entries from the ntp.conf file:

   ```
   restrict localhost

   restrict 127.0.0.2
   ```

   These entries are required only if you want to run the device as a time server. However, this feature is not supported on the NetScaler.

3. Edit /nsconfig/ntp.conf by typing the IP address for the desired NTP server under the file's server and restrict entries.

4. Create a file named rc.netscaler in the /nsconfig directory, if the file does not already exist in the directory.

5. Edit /nsconfig/rc.netscaler by adding the following entry: `/usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ntpd.log &`

   This entry starts the ntpd service, checks the ntp.conf file, and logs messages in the /var/log directory.

   Note: If the time difference between the NetScaler and the time server is more than 1000 sec, the ntpd service terminates with a message to the NetScaler log. To avoid this, you need to start ntpd with the -g option, which forcibly syncs the time. Add the following entry in /nsconfig/rc.netscaler:

   ```
   /usr/sbin/ntpd -g -c /nsconfig/ntp.conf -l /var/log/ntpd.log &
   ```

   If you do not want to forcibly sync the time when there is a large difference, you can set the date manually and then start ntpd again. You can check the time difference between the appliance and the time server by running the following command in the shell:

   ntpdate -q <IP address or domain name of the NTP server>

6. Reboot the appliance to enable clock synchronization.

   Note: If you want to start time synchronization before you restart the appliance, enter the following command (which you added to the rc.netscaler file in step 5) at the shell prompt:

   /usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ ntpd.log &

Configuring DNS

You can configure a NetScaler appliance to function as an Authoritative Domain Name Server (ADNS), DNS proxy server, End Resolver, or Forwarder. You can add DNS resource records such as SRV Records, AAAA Records, A Records, MX Records, NS Records, CNAME Records, PTR Records, and SOA Records. Also, the appliance can balance the load on external DNS servers.

A common practice is to configure an appliance as a forwarder. For this configuration, you need to add external name servers. After you have added the external servers, you should verify that your configuration is correct.

You can add, remove, enable, and disable external name servers. You can create a name server by specifying its IP address, or you can configure an existing virtual server as the name server.

When adding name servers, you can specify IP addresses or virtual IP addresses (VIPs). If you use IP addresses, the appliance load balances requests to the configured name servers in a round robin manner. If you use VIPs, you can specify any load balancing method. For information about using a VIP, see "Load Balancing DNS Servers."

To add a name server by using the command line interface

At the command prompt, type the following commands to add a name server and verify the configuration:

- `add dns nameServer <IP>`
- `show dns nameServer <IP>`

Example

```
> add dns nameServer 10.102.29.10
 Done
> show dns nameServer 10.102.29.10
1)      10.102.29.10  -  State: DOWN
 Done
>
```

To add a name server by using the configuration utility

1. In the navigation pane, expand DNS, and then click Name Servers.
2. In the details pane, click Add.
3. In the Create Name Server dialog box, select IP Address.
4. In the IP Address text box, type the IP address of the name server (for example, `10.102.29.10`). If you are adding an external name server, clear the Local check box.
5. Click Create, and then click Close.
6. Verify that the name server you added appears in the Name Servers pane.

Configuring SNMP

The Simple Network Management Protocol (SNMP) network management application, running on an external computer, queries the SNMP agent on the NetScaler. The agent searches the management information base (MIB) for data requested by the network management application and sends the data to the application.

SNMP monitoring uses traps messages and alarms. SNMP traps messages are asynchronous events that the agent generates to signal abnormal conditions, which are indicated by alarms. For example, if you want to be informed when CPU utilization is above 90 percent, you can set up an alarm for that condition. The following figure shows a network with a NetScaler that has SNMP enabled and configured.

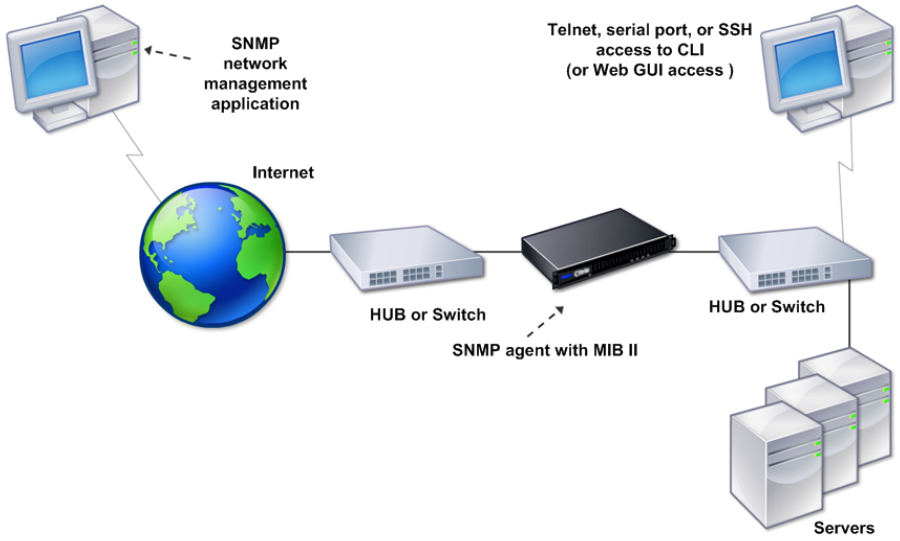


Figure 1. SNMP on the NetScaler

The SNMP agent on a NetScaler supports SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2), and SNMP version 3 (SNMPv3). Because it operates in bilingual mode, the agent can handle SNMPv2 queries, such as Get-Bulk, and SNMPv1 queries. The SNMP agent also sends traps compliant with SNMPv2 and supports SNMPv2 data types, such as counter64. SNMPv1 managers (programs on other servers that request SNMP information from the NetScaler) use the NS-MIB-smiv1.mib file when processing SNMP queries. SNMPv2 managers use the NS-MIB-smiv2.mib file.

The NetScaler supports the following enterprise-specific MIBs:

A subset of standard MIB-2 groups

Provides MIB-2 groups SYSTEM, IF, ICMP, UDP, and SNMP.

A system enterprise MIB

Provides system-specific configuration and statistics.

To configure SNMP, you specify which managers can query the SNMP agent, add SNMP trap listeners that will receive the SNMP trap messages, and configure SNMP Alarms.

Adding SNMP Managers

You can configure a workstation running a management application that complies with SNMP version 1, 2, or 3 to access an appliance. Such a workstation is called an SNMP manager. If you do not specify an SNMP manager on the appliance, the appliance accepts and responds to SNMP queries from all IP addresses on the network. If you configure one or more SNMP managers, the appliance accepts and responds to SNMP queries from only those specific IP addresses. When specifying the IP address of an SNMP manager, you can use the netmask parameter to grant access from entire subnets. You can add a maximum of 100 SNMP managers or networks.

To add an SNMP manager by using the command line interface

At the command prompt, type the following commands to add an SNMP manager and verify the configuration:

- `add snmp manager <IPAddress> ... [-netmask <netmask>]`
- `show snmp manager <IPAddress>`

Example

```
> add snmp manager 10.102.29.5 -netmask 255.255.255.255
 Done
> show snmp manager 10.102.29.5
1)     10.102.29.5        255.255.255.255
 Done
>
```

To add an SNMP manager by using the configuration utility

1. In the navigation pane, expand System, expand SNMP, and then click Managers.
2. In the details pane, click Add.
3. In the Add SNMP Manager dialog box, in the IP Address text box, type the IP address of the workstation running the management application (for example, `10.102.29.5`).
4. Click Create, and then click Close.
5. Verify that the SNMP manager you added appears in the Details section at the bottom of the pane.

Adding SNMP Traps Listeners

After configuring the alarms, you need to specify the trap listener to which the appliance will send the trap messages. Apart from specifying parameters like IP address and the destination port of the trap listener, you can specify the type of trap (either generic or specific) and the SNMP version.

You can configure a maximum of 20 trap listeners for receiving either generic or specific traps.

To add an SNMP trap listener by using the command line interface

At the command prompt, type the following command to add an SNMP trap and verify that it has been added:

- `add snmp trap specific <IP>`
- `show snmp trap`

Example

```
> add snmp trap specific 10.102.29.3
 Done
> show snmp trap
Type    DestinationIP   DestinationPort  Version  SourceIP     Min-Severity  Community
----    -------------   ---------------  -------  --------     ------------  ---------
generic  10.102.29.9    162           V2      NetScaler IP  N/A          public
generic  10.102.29.5    162           V2      NetScaler IP  N/A          public
generic  10.102.120.101  162           V2      NetScaler IP  N/A          public
.
.
.
specific 10.102.29.3    162           V2      NetScaler IP   -           public
 Done
>
```

To add an SNMP trap listener by using the configuration utility

1. In the navigation pane, expand System, expand SNMP, and then click Traps.
2. In the details pane, click Add.
3. In the Create SNMP Trap Destination dialog box, in the Destination IP Address text box, type the IP address (for example, `10.102.29.3`).
4. Click Create and then click Close.
5. Verify that the SNMP trap you added appears in the Details section at the bottom of the pane.

Configuring SNMP Alarms

You configure alarms so that the appliance generates a trap message when an event corresponding to one of the alarms occurs. Configuring an alarm consists of enabling the alarm and setting the severity level at which a trap is generated. There are five severity levels: Critical, Major, Minor, Warning, and Informational. A trap is sent only when the severity of the alarm matches the severity specified for the trap.

Some alarms are enabled by default. If you disable an SNMP alarm, the appliance will not generate trap messages when corresponding events occur. For example, if you disable the Login-Failure SNMP alarm, the appliance will not generate a trap message when a login failure occurs.

To enable or disable an alarm by using the command line interface

At the command prompt, type the following commands to enable or disable an alarm and verify that it has been enabled or disabled:

- `set snmp alarm <trapName> [-state ENABLED | DISABLED ]`
- `show snmp alarm <trapName>`

Example

```
> set snmp alarm LOGIN-FAILURE -state ENABLED
 Done
> show snmp alarm LOGIN-FAILURE
  Alarm          Alarm Threshold  Normal Threshold  Time  State    Severity   Logging
  -----          ---------------  ----------------  ----  --------  ---------  --------
 1) LOGIN-FAILURE  N/A           N/A           N/A   ENABLED   -       ENABLED
 Done
>
```

To set the severity of the alarm by using the command line interface

At the command prompt, type the following commands to set the severity of the alarm and verify that the severity has been set correctly:

- `set snmp alarm <trapName> [-severity <severity>]`
- `show snmp alarm <trapName>`

Example

```
> set snmp alarm LOGIN-FAILURE -severity Major
 Done
> show snmp alarm LOGIN-FAILURE
   Alarm          Alarm Threshold  Normal Threshold  Time  State     Severity   Logging
   -----          ---------------  ----------------  ----  --------  ---------  --------
 1) LOGIN-FAILURE  N/A             N/A               N/A   ENABLED   Major      ENABLED
 Done
>
```

To configure alarms by using the configuration utility

1. In the navigation pane, expand System, expand SNMP, and then click Alarms.
2. In the details pane, select an alarm (for example, LOGIN-FAILURE), and then click Open.
3. In the Configure SNMP Alarm dialog box, to enable the alarm, select the Enable check box. To disable the alarm, clear the Enable check box.
4. In the Severity drop-down list, select a severity option (for example, Major).
5. Click OK, and then click Close.
6. Verify that the parameters for the SNMP alarm you configured are correctly configured by viewing the Details section at the bottom of the pane.

Configuring Syslog

You can customize logging of NetScaler and Access Gateway Enterprise Edition access events for the needs of your site. You can direct these logs either to files on the NetScaler or to external log servers. The NetScaler uses the Audit Server Logging feature for logging the states and status information collected by different modules in the kernel and by user-level daemons.

Syslog is used to monitor a NetScaler and to log connections, statistics, and so on. You can customize the two logging functions for system events messaging and syslog. The NetScaler internal event message generator passes log entries to the syslog server. The syslog server accepts these log entries and logs them. For more information about the Audit Server Logging feature, see "Audit Logging."

Verifying the Configuration

After you finish configuring your system, complete the following checklists to verify your configuration.

Configuration Checklist

- The build running is:
- There are no incompatibility issues. (Incompatibility issues are documented in the build's release notes.)
- The port settings (speed, duplex, flow control, monitoring) are the same as the switch's port.
- Enough mapped IP addresses have been configured to support all server-side connections during peak times.
  - The number of configured mapped IP addresses is: ____
  - The expected number of simultaneous server connections is:

    [ ] 62,000 [ ] 124,000 [ ] Other____

Topology Configuration Checklist

- The routes have been used to resolve servers on other subnets.

  The routes entered are:

  _____
- If the NetScaler is in a public-private topology, reverse NAT has been configured.
- The failover (high availability) settings configured on the NetScaler resolve in a one arm or two-arm configuration. All unused network interfaces have been disabled:

  _____
- If the NetScaler is placed behind an external load balancer, then the load balancing policy on the external load balancer is not "least connection."

  The load balancing policy configured on the external load balancer is:

  _____
- If the NetScaler is placed in front of a firewall, the session time-out on the firewall is set to a value greater than or equal to 300 seconds.

  Note: The TCP idle connection timeout on a NetScaler appliance is 360 seconds. If the timeout on the firewall is also set to 300 seconds or more, then the appliance can

perform TCP connection multiplexing effectively because connections will not be closed earlier.

The value configured for the session time-out is: _____

Server Configuration Checklist

- "Keep-alive" has been enabled on all the servers.

  The value configured for the keep-alive time-out is: _____

- The default gateway has been set to the correct value. (The default gateway should either be a NetScaler or upstream router.) The default gateway is:

  _____

- The server port settings (speed, duplex, flow control, monitoring) are the same as the switch port settings.

  _____

- If the Microsoft® Internet Information Server is used, buffering is enabled on the server.

- If an Apache Server is used, the MaxConn (maximum number of connections) parameter is configured on the server and on the NetScaler.

  The MaxConn (maximum number of connections) value that has been set is:

  _____

- If a Netscape® Enterprise Server™ is used, the maximum requests per connection parameter is set on the NetScaler. The maximum requests per connection value that has been set is:

  _____

Software Features Configuration Checklist

- Does the Layer 2 mode feature need to be disabled? (Disable if another Layer 2 device is working in parallel with a NetScaler.)

  Reason for enabling or disabling:

  _____

- Does the MAC-based forwarding feature need to be disabled? (If the MAC address used by return traffic is different, it should be disabled.)

  Reason for enabling or disabling:

  _____

- Does host-based reuse need to be disabled? (Is there virtual hosting on the servers?)

Reason for enabling or disabling:

_____

- Do the default settings of the surge protection feature need to be changed?

Reason for changing or not changing:

_____

Access Checklist

- The system IPs can be pinged from the client-side network.
- The system IPs can be pinged from the server-side network.
- The managed server(s) can be pinged through the NetScaler.
- Internet hosts can be pinged from the managed servers.
- The managed server(s) can be accessed through the browser.
- The Internet can be accessed from managed server(s) using the browser.
- The system can be accessed using SSH.
- Admin access to all managed server(s) is working.

Note: When you are using the ping utility, ensure that the pinged server has ICMP ECHO enabled, or your ping will not succeed.

Firewall Checklist

The following firewall requirements have been met:

- UDP 161 (SNMP)
- UDP 162 (SNMP trap)
- TCP/UDP 3010 (GUI)
- HTTP 80 (GUI)
- TCP 22 (SSH)

Load Balancing Traffic on a NetScaler Appliance

The load balancing feature distributes client requests across multiple servers to optimize resource utilization. In a real-world scenario with a limited number of servers providing service to a large number of clients, a server can become overloaded and degrade the performance of the server farm. A Citrix NetScaler appliance uses load balancing criteria to prevent bottlenecks by forwarding each client request to the server best suited to handle the request when it arrives.

To configure load balancing, you define a virtual server to proxy multiple servers in a server farm and balance the load among them.

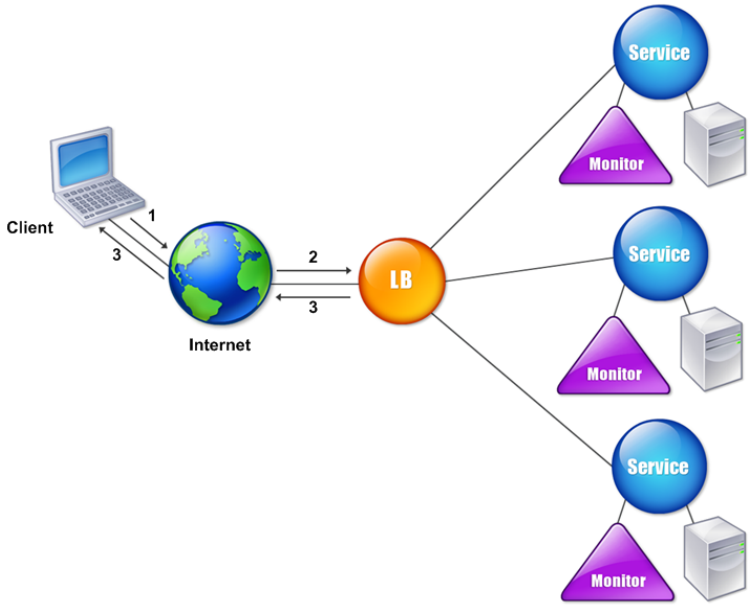
How Load Balancing Works

When a client initiates a connection to the server, a virtual server terminates the client connection and initiates a new connection with the selected server, or reuses an existing connection with the server, to perform load balancing. The load balancing feature provides traffic management from Layer 4 (TCP and UDP) through Layer 7 (FTP, HTTP, and HTTPS).

The NetScaler appliance uses a number of algorithms, called load balancing methods, to determine how to distribute the load among the servers. The default load balancing method is the Least Connections method.

A typical load balancing deployment consists of the entities described in the following figure.

Figure 1. Load Balancing Architecture



The entities function as follows:

- **Virtual server**. An entity that is represented by an IP address, a port, and a protocol. The virtual server IP address (VIP) is usually a public IP address. The client sends connection requests to this IP address. The virtual server represents a bank of servers.

- **Service**. A logical representation of a server or an application running on a server. Identifies the server's IP address, a port, and a protocol. The services are bound to the virtual servers.

- **Server object**. An entity that is represented by an IP address. The server object is created when you create a service. The IP address of the service is taken as the name of the server object. You can also create a server object and then create services by using the server object.

- **Monitor**. An entity that tracks the health of the services. The appliance periodically probes the servers using the monitor bound to each service. If a server does not respond within a specified response timeout, and the specified number of probes fails, the service is marked DOWN. The appliance then performs load balancing among the remaining services.

Configuring Load Balancing

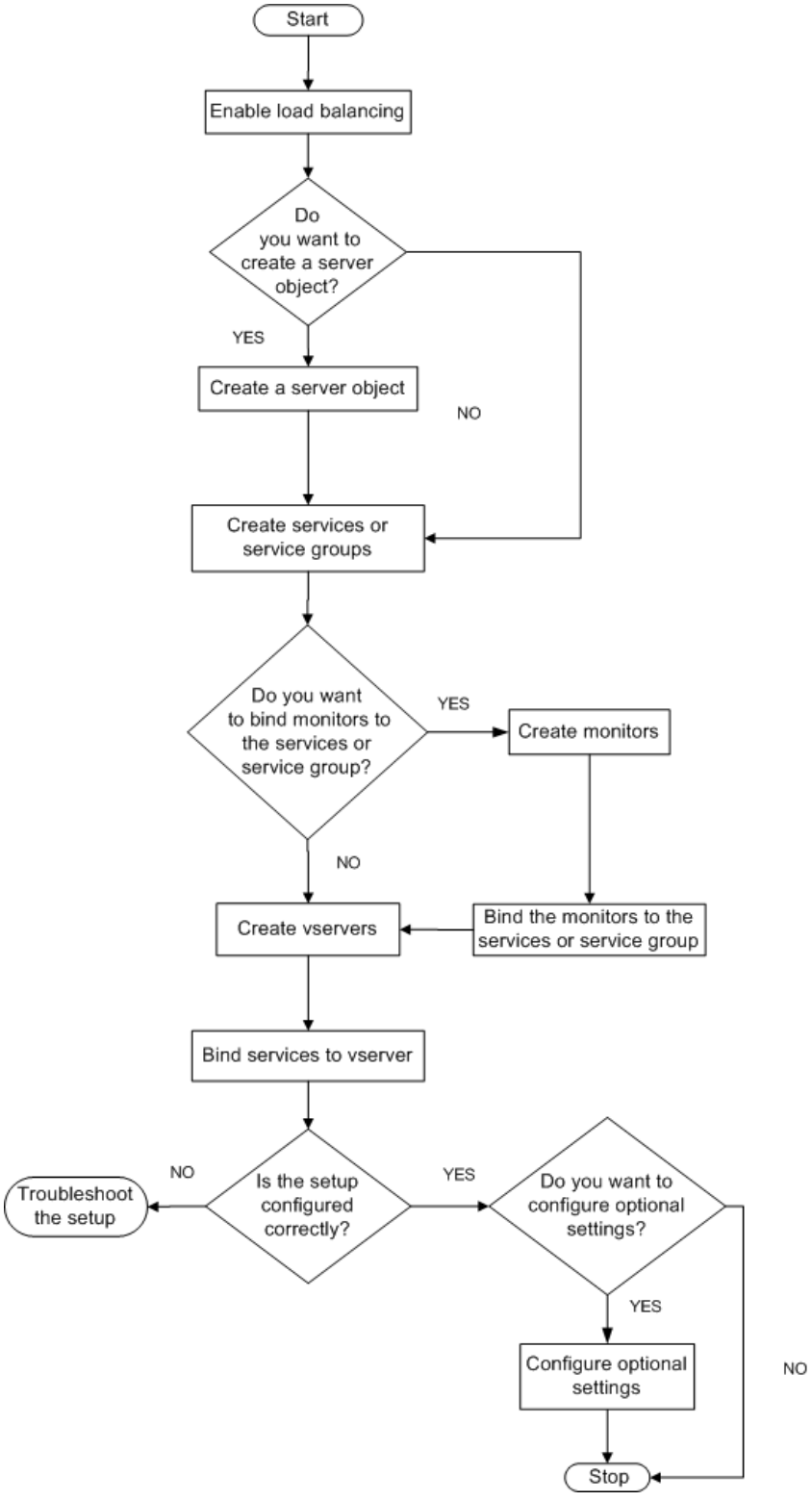
To configure load balancing, you must first create services. Then, you create virtual servers and bind the services to the virtual servers. By default, the NetScaler appliance binds a monitor to each service. After binding the services, verify your configuration by making sure that all of the settings are correct.

Note: After you deploy the configuration, you can display statistics that show how the entities in the configuration are performing. Use the statistical utility or the `stat lb vserver <vserverName>` command.

Optionally, you can assign weights to a service. The load balancing method then uses the assigned weight to select a service. For getting started, however, you can limit optional tasks to configuring some basic persistence settings, for sessions that must maintain a connection to a particular server, and some basic configuration-protection settings.

The following flow chart illustrates the sequence of the configuration tasks.

Figure 1. Sequence of Tasks to Configure Load Balancing


Start
Enable load balancing
Do you want to create a server object?
YES
Create a server object
NO
Create services or service groups
Do you want to bind monitors to the services or service group?
YES
Create monitors
NO
Create vservers
Bind the monitors to the services or service group
Bind services to vserver
Is the setup configured correctly?
NO
Troubleshoot the setup
YES
Do you want to configure optional settings?
YES
Configure optional settings
NO
Stop

Enabling Load Balancing

Before configuring load balancing, make sure that the load balancing feature is enabled.

To enable load balancing by using the command line interface

At the command prompt, type the following commands to enable load balancing and verify that it is enabled:

- `enable feature lb`
- `show feature`

Example

```
> enable feature lb
 Done
> show feature

    Feature              Acronym        Status
    -------             -------        ------
 1)  Web Logging          WL             OFF
 2)  Surge Protection      SP             OFF
 3)  Load Balancing        LB             ON
 .
 .
 .
 9)  SSL Offloading        SSL            ON
 .
 .
 .
Done
```

To enable load balancing by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features, click Change basic features.
3. In the Configure Basic Features dialog box, select the Load Balancing check box, and then click OK.
4. In the Enable/Disable Feature(s)? message, click Yes.

Configuring Services and a Virtual Server

When you have identified the services you want to load balance, you can implement your initial load balancing configuration by creating the service objects, creating a load balancing virtual server, and binding the service objects to the virtual server.

To implement the initial load balancing configuration by using the command line interface

At the command prompt, type the following commands to implement and verify the initial configuration:

- add service <name> <IPaddress> <serviceType> <port>
- add lb vserver <vServerName> <serviceType> [<IPaddress> <port>]
- bind lb vserver <name> <serviceName>
- show service bindings <serviceName>

  Example

```
> add service service-HTTP-1 10.102.29.5 HTTP 80
 Done
> add lb vserver vserver-LB-1 HTTP 10.102.29.60 80
 Done
> bind lb vserver vserver-LB-1 service-HTTP-1
 Done
> show service bindings service-HTTP-1
   service-HTTP-1 (10.102.29.5:80) - State : DOWN

     1)      vserver-LB-1 (10.102.29.60:80) - State : DOWN
 Done
```

To implement the initial load balancing configuration by using the configuration utility

1. In the navigation pane, click Load Balancing.
2. In the details pane, under Getting Started, click Load Balancing wizard, and follow the instructions to create a basic load balancing setup.
3. Return to the navigation pane, expand Load Balancing, and then click Virtual Servers.
4. Select the virtual server that you configured and verify that the parameters displayed at the bottom of the page are correctly configured.
5. Click Open.
6. Verify that each service is bound to the virtual server by confirming that the Active check box is selected for each service on the Services tab.

Choosing and Configuring Persistence Settings

You must configure persistence on a virtual server if you want to maintain the states of connections on the servers represented by that virtual server (for example, connections used in e-commerce). The appliance then uses the configured load balancing method for the initial selection of a server, but forwards to that same server all subsequent requests from the same client.

If persistence is configured, it overrides the load balancing methods once the server has been selected. If the configured persistence applies to a service that is down, the appliance uses the load balancing methods to select a new service, and the new service becomes persistent for subsequent requests from the client. If the selected service is in an Out Of Service state, it continues to serve the outstanding requests but does not accept new requests or connections. After the shutdown period elapses, the existing connections are closed. The following table lists the types of persistence that you can configure.

Table 1. Limitations on Number of Simultaneous Persistent Connections

Persistence Type	Persistent Connections
Source IP, SSL Session ID, Rule, DESTIP, SRCIPDESTIP	250K
CookieInsert, URL passive, Custom Server ID	Memory limit. In case of CookieInsert, if time out is not 0, any number of connections is allowed until limited by memory.

If the configured persistence cannot be maintained because of a lack of resources on an appliance, the load balancing methods are used for server selection. Persistence is maintained for a configured period of time, depending on the persistence type. Some persistence types are specific to certain virtual servers. The following table shows the relationship.

Table 2. Persistence Types Available for Each Type of Virtual Server

Persistence TypeHeader 1	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge
Source IP	YES	YES	YES	YES	YES
CookieInsert	YES	YES	NO	NO	NO
SSL Session ID	NO	YES	NO	NO	YES
URL Passive	YES	YES	NO	NO	NO
Custom Server ID	YES	YES	NO	NO	NO
Rule	YES	YES	NO	NO	NO
SRCIPDESTIP	N/A	N/A	YES	YES	N/A

DESTIP	N/A	N/A	YES	YES	N/A

You can also specify persistence for a group of virtual servers. When you enable persistence on the group, the client requests are directed to the same selected server regardless of which virtual server in the group receives the client request. When the configured time for persistence elapses, any virtual server in the group can be selected for incoming client requests.

Two commonly used persistence types are persistence based on cookies and persistence based on server IDs in URLs. For more information about all persistence types, see "Persistence and Persistent Connections."

Configuring Persistence Based on Cookies

When you enable persistence based on cookies, the NetScaler adds an HTTP cookie into the Set-Cookie header field of the HTTP response. The cookie contains information about the service to which the HTTP requests must be sent. The client stores the cookie and includes it in all subsequent requests, and the NetScaler uses it to select the service for those requests. You can use this type of persistence on virtual servers of type HTTP or HTTPS.

The NetScaler inserts the cookie <NSC_XXXX>= <ServiceIP> <ServicePort>

where:

- <NSC_XXXX> is the virtual server ID that is derived from the virtual server name.
- <ServiceIP> is the hexadecimal value of the IP address of the service.
- <ServicePort> is the hexadecimal value of the port of the service.

The NetScaler encrypts ServiceIP and ServicePort when it inserts a cookie, and decrypts them when it receives a cookie.

Note: If the client is not allowed to store the HTTP cookie, the subsequent requests do not have the HTTP cookie, and persistence is not honored.

By default, the NetScaler sends HTTP cookie version 0, in compliance with the Netscape specification. It can also send version 1, in compliance with RFC 2109.

You can configure a timeout value for persistence that is based on HTTP cookies. Note the following:

- If HTTP cookie version 0 is used, the NetScaler inserts the absolute Coordinated Universal Time (GMT) of the cookie's expiration (the expires attribute of the HTTP cookie), calculated as the sum of the current GMT time on a NetScaler, and the timeout value.
- If an HTTP cookie version 1 is used, the NetScaler inserts a relative expiration time (Max-Age attribute of the HTTP cookie). In this case, the client software calculates the actual expiration time.

Note: Most client software currently installed (Microsoft Internet Explorer and Netscape browsers) understand HTTP cookie version 0; however, some HTTP proxies understand HTTP cookie version 1.

If you set the timeout value to 0, the NetScaler does not specify the expiration time, regardless of the HTTP cookie version used. The expiration time then depends on the client software, and such cookies are not valid if that software is shut down. This persistence type does not consume any system resources. Therefore, it can accommodate an unlimited number of persistent clients.

An administrator can use the procedure in the following table to change the HTTP cookie version.

To change the HTTP cookie version by using the configuration utility

1. Navigate to System > Settings.
2. In the details pane, click Change HTTP Parameters.
3. In the Configure HTTP Parameters dialog box, under Cookie, select Version 0 or Version 1.

Note: For information about the parameters, see "Configuring Persistence Based on Cookies."

To configure persistence based on cookies by using the command line interface

At the command prompt, type the following commands to configure persistence based on cookies and verify the configuration:

- set lb vserver <name> -persistenceType COOKIEINSERT
- show lb vserver <name>

Example

```
> set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT
 Done
> show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    .
    .
    .
    Persistence: COOKIEINSERT (version 0)   Persistence Timeout: 2 min
    .
    .
    .
 Done
>
```

To configure persistence based on cookies by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure persistence (for example, vserver-LB-1), and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, on the Method and Persistence tab, in the Persistence list, select COOKIEINSERT.
4. In the Time-out (min) text box, type the time-out value (for example, 2).
5. Click OK.
6. Verify that the virtual server for which you configured persistence is correctly configured by selecting the virtual server and viewing the Details section at the bottom of the pane.

Configuring Persistence Based on Server IDs in URLs

The NetScaler can maintain persistence based on the server IDs in the URLs. In a technique called URL passive persistence, the NetScaler extracts the server ID from the server response and embeds it in the URL query of the client request. The server ID is an IP address and port specified as a hexadecimal number. The NetScaler extracts the server ID from subsequent client requests and uses it to select the server.

URL passive persistence requires configuring either a payload expression or a policy infrastructure expression specifying the location of the server ID in the client requests. For more information about expressions, see "Policy Configuration and Reference."

Note: If the server ID cannot be extracted from the client requests, server selection is based on the load balancing method.

Example: Payload Expression

The expression, URLQUERY contains sid= configures the system to extract the server ID from the URL query of a client request, after matching token sid=. Thus, a request with the URL http://www.citrix.com/index.asp?&sid;=c0a864100050 is directed to the server with the IP address10.102.29.10 and port 80.

The timeout value does not affect this type of persistence, which is maintained as long as the server ID can be extracted from the client requests. This persistence type does not consume any system resources, so it can accommodate an unlimited number of persistent clients.

Note: For information about the parameters, see "Load Balancing."

To configure persistence based on server IDs in URLs by using the command line interface

At the command prompt, type the following commands to configure persistence based on server IDs in URLs and verify the configuration:

- `set lb vserver <name> -persistenceType URLPASSIVE`
- `show lb vserver <name>`

Example

```
> set lb vserver vserver-LB-1 -persistenceType URLPASSIVE
 Done
> show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
```

```
    .
    .
    .
    Persistence: URLPASSIVE Persistence Timeout: 2 min
    .
    .
    .
 Done
>
```

To configure persistence based on server IDs in URLs by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure persistence (for example, vserver-LB-1), and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, on the Method and Persistence tab, in the Persistence list, select URLPASSIVE.
4. In the Time-out (min) text box, type the time-out value (for example, 2).
5. In the Rule text box, enter a valid expression. Alternatively, click Configure next to the Rule text box and use the Create Expression dialog box to create an expression.
6. Click OK.
7. Verify that the virtual server for which you configured persistence is correctly configured by selecting the virtual server and viewing the Details section at the bottom of the pane.

Configuring Features to Protect the Load Balancing Configuration

You can configure URL redirection to provide notifications of virtual server malfunctions, and you can configure backup virtual servers to take over if a primary virtual server becomes unavailable.

Configuring URL Redirection

You can configure a redirect URL to communicate the status of the appliance in the event that a virtual server of type HTTP or HTTPS is down or disabled. This URL can be a local or remote link. The appliance uses HTTP 302 redirect.

Redirects can be absolute URLs or relative URLs. If the configured redirect URL contains an absolute URL, the HTTP redirect is sent to the configured location, regardless of the URL specified in the incoming HTTP request. If the configured redirect URL contains only the domain name (relative URL), the HTTP redirect is sent to a location after appending the incoming URL to the domain configured in the redirect URL.

Note: If a load balancing virtual server is configured with both a backup virtual server and a redirect URL, the backup virtual server takes precedence over the redirect URL. In this case, a redirect is used when both the primary and backup virtual servers are down.

To configure a virtual server to redirect client requests to a URL by using the command line interface

At the command prompt, type the following commands to configure a virtual server to redirect client requests to a URL and verify the configuration:

- set lb vserver <name> -redirectURL <URL>
- show lb vserver <name>

Example

```
> set lb vserver vserver-LB-1 -redirectURL http://www.newdomain.com/mysite/maintenance
 Done
> show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    State: DOWN
    Last state change was at Wed Jun 17 08:56:34 2009 (+666 ms)
    .
    .
    .
    Redirect URL: http://www.newdomain.com/mysite/maintenance
    .
    .
    .
 Done
>
```

To configure a virtual server to redirect client requests to a URL by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure URL redirection (for example, vserver-LB-1), and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, on the Advanced tab, in the Redirect URL text box, type the URL (for example, `http://www.newdomain.com/mysite/maintenance`), and then click OK.
4. Verify that the redirect URL you configured for the server appears in the Details section at the bottom of the pane.

Configuring Backup Virtual Servers

If the primary virtual server is down or disabled, the appliance can direct the connections or client requests to a backup virtual server that forwards the client traffic to the services. The appliance can also send a notification message to the client regarding the site outage or maintenance. The backup virtual server is a proxy and is transparent to the client.

You can configure a backup virtual server when you create a virtual server or when you change the optional parameters of an existing virtual server. You can also configure a backup virtual server for an existing backup virtual server, thus creating a cascaded backup virtual server. The maximum depth of cascading backup virtual servers is 10. The appliance searches for a backup virtual server that is up and accesses that virtual server to deliver the content.

You can configure URL redirection on the primary for use when the primary and the backup virtual servers are down or have reached their thresholds for handling requests.

Note: If no backup virtual server exists, an error message appears, unless the virtual server is configured with a redirect URL. If both a backup virtual server and a redirect URL are configured, the backup virtual server takes precedence.

To configure a backup virtual server by using the command line interface

At the command prompt, type the following commands to configure a backup server and verify the configuration:

- set lb vserver <name> [-backupVserver <string>]
- show lb vserver <name>

Example

```
> set lb vserver vserver-LB-1 -backupVserver vserver-LB-2
 Done
> show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    State: DOWN
    Last state change was at Wed Jun 17 08:56:34 2009 (+661 ms)
    .
    .
    .
    Backup: vserver-LB-2
    .
    .
    .
 Done
>
```

To set up a backup virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure the backup virtual server (for example, vserver-LB-1), and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, on the Advanced tab, in the Backup Virtual Server list, select the backup virtual server (for example, vserver-LB-2, and then click OK.
4. Verify that the backup virtual server you configured appears in the Details section at the bottom of the pane.

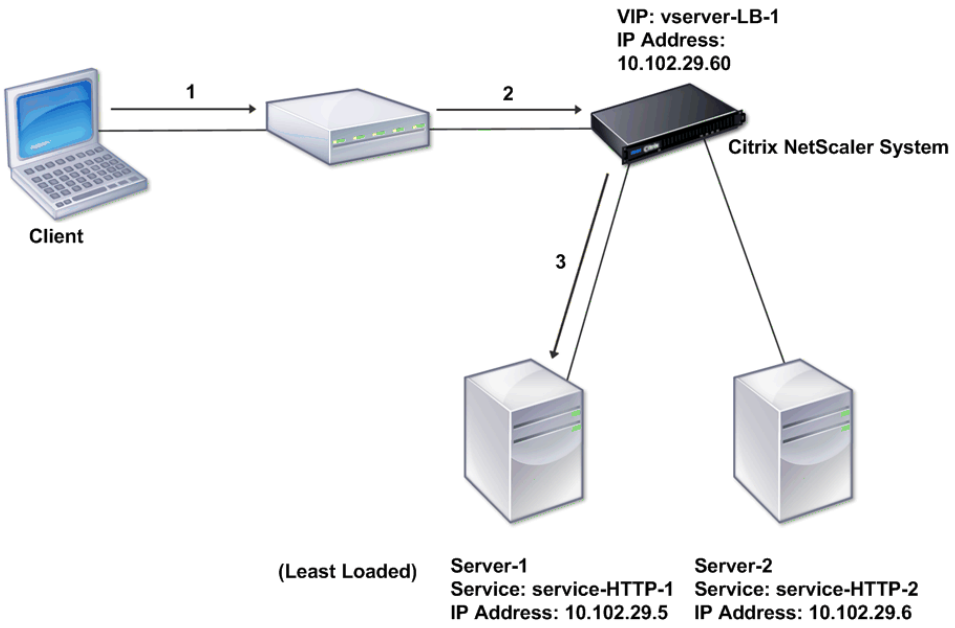
   Note: If the primary server goes down and then comes back up, and you want the backup virtual server to function as the primary server until you explicitly reestablish the primary virtual server, select the Disable Primary When Down check box.

A Typical Load Balancing Scenario

In a load balancing setup, the NetScaler appliances are logically located between the client and the server farm, and they manage traffic flow to the servers.

The following figure shows the topology of a basic load balancing configuration.

Figure 1. Basic Load Balancing Topology



The virtual server selects the service and assigns it to serve client requests. Consider the scenario in the preceding figure, where the services service-HTTP-1 and service-HTTP-2 are created and bound to the virtual server named virtual server-LB-1. Virtual server-LB-1 forwards the client request to either service-HTTP-1 or service-HTTP-2. The system selects the service for each request by using the Least Connections load balancing method. The following table lists the names and values of the basic entities that must be configured on the system.

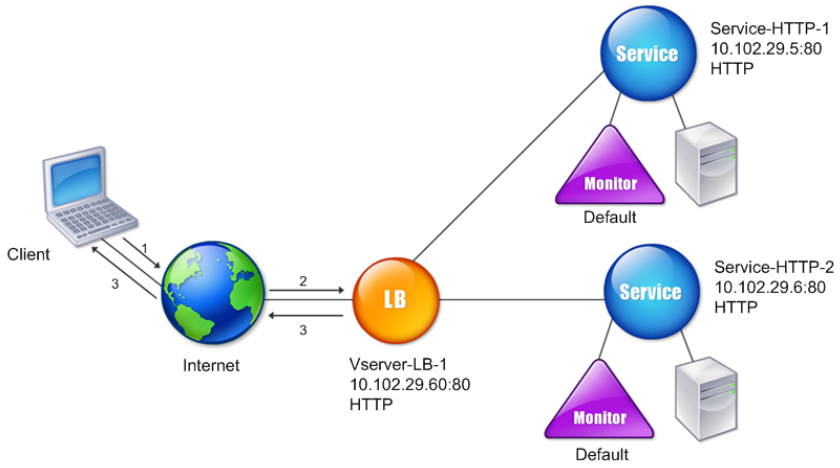
Table 1. LB Configuration Parameter Values

Entity Type	Required parameters and sample values			
	Name	IP Address	Port	Protocol
Virtual Server	vserver-LB-1	10.102.29.60	80	HTTP
Services	service-HTTP-1	10.102.29.5	8083	HTTP
	service-HTTP-2	10.102.29.6	80	HTTP

Monitors	Default	None	None	None

The following figure shows the load balancing sample values and required parameters that are described in the preceding table.

Figure 2. Load Balancing Entity Model



The following tables list the commands used to configure this load balancing setup by using the command line interface.

Table 2. Initial Configuration Tasks

Task	Command
To enable load balancing	enable feature lb
To create a service named service-HTTP-1	add service service-HTTP-1 10.102.29.5 HTTP 80
To create a service named service-HTTP-2	add service service-HTTP-2 10.102.29.6 HTTP 80
To create a virtual server named vserver-LB-1	add lb vserver vserver-LB-1 HTTP 10.102.29.60 80
To bind a service named service-HTTP-1 to a virtual server named vserver-LB-1	bind lb vserver vserver-LB-1 service-HTTP-1
To bind a service named service-HTTP-2 to a virtual server named vserver-LB-1	bind lb vserver vserver-LB-1 service-HTTP-2

For more information about the initial configuration tasks, see "Enabling Load Balancing" and "Configuring Services and a Vserver."

Table 3. Verification Tasks

Task	Command
To view the properties of a virtual server named vserver-LB-1	show lb vserver vserver-LB-1
To view the statistics of a virtual server named vserver-LB-1	stat lb vserver vserver-LB-1
To view the properties of a service named service-HTTP-1	show service service-HTTP-1
To view the statistics of a service named service-HTTP-1	stat service service-HTTP-1
To view the bindings of a service named service-HTTP-1	show service bindings service-HTTP-1

Table 4. Customization Tasks

Task	Command
To configure persistence on a virtual server named vserver-LB-1	set lb vserver vserver-LB-1 -persistenceType SOURCEIP -persistenceMask 255.255.255.255 -timeout 2
To configure COOKIEINSERT persistence on a virtual server named vserver-LB-1	set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT
To configure URLPassive persistence on a virtual server named vserver-LB-1	set lb vserver vserver-LB-1 -persistenceType URLPASSIVE
To configure a virtual server to redirect the client request to a URL on a virtual server named vserver-LB-1	set lb vserver vserver-LB-1 -redirectURL http://www.newdomain.com/mysite/maintenance
To set a backup virtual server on a virtual server named vserver-LB-1	set lb vserver vserver-LB-1 -backupVserver vserver-LB-2

For more information about configuring persistence, see "Choosing and Configuring Persistence Settings." For information about configuring a virtual server to redirect a client request to a URL and setting up a backup virtual server, see "Configuring Features to Protect the Load Balancing Configuration."

Accelerating Load Balanced Traffic by Using Compression

Compression is a popular means of optimizing bandwidth usage, and most web browsers support compressed data. If you enable the compression feature, the NetScaler appliance intercepts requests from clients and determines whether the client can accept compressed content. After receiving the HTTP response from the server, the appliance examines the content to determine whether it is compressible. If the content is compressible, the appliance compresses it, modifies the response header to indicate the type of compression performed, and forwards the compressed content to the client.

NetScaler compression is a policy-based feature. A policy filters requests and responses to identify responses to be compressed, and specifies the type of compression to apply to each response. The appliance provides several built-in policies to compress common MIME types such as text/html, text/plain, text/xml, text/css, text/rtf, application/msword, application/vnd.ms-excel, and application/vnd.ms-powerpoint. You can also create custom policies. The appliance does not compress compressed MIME types such as application/octet-stream, binary, bytes, and compressed image formats such as GIF and JPEG.

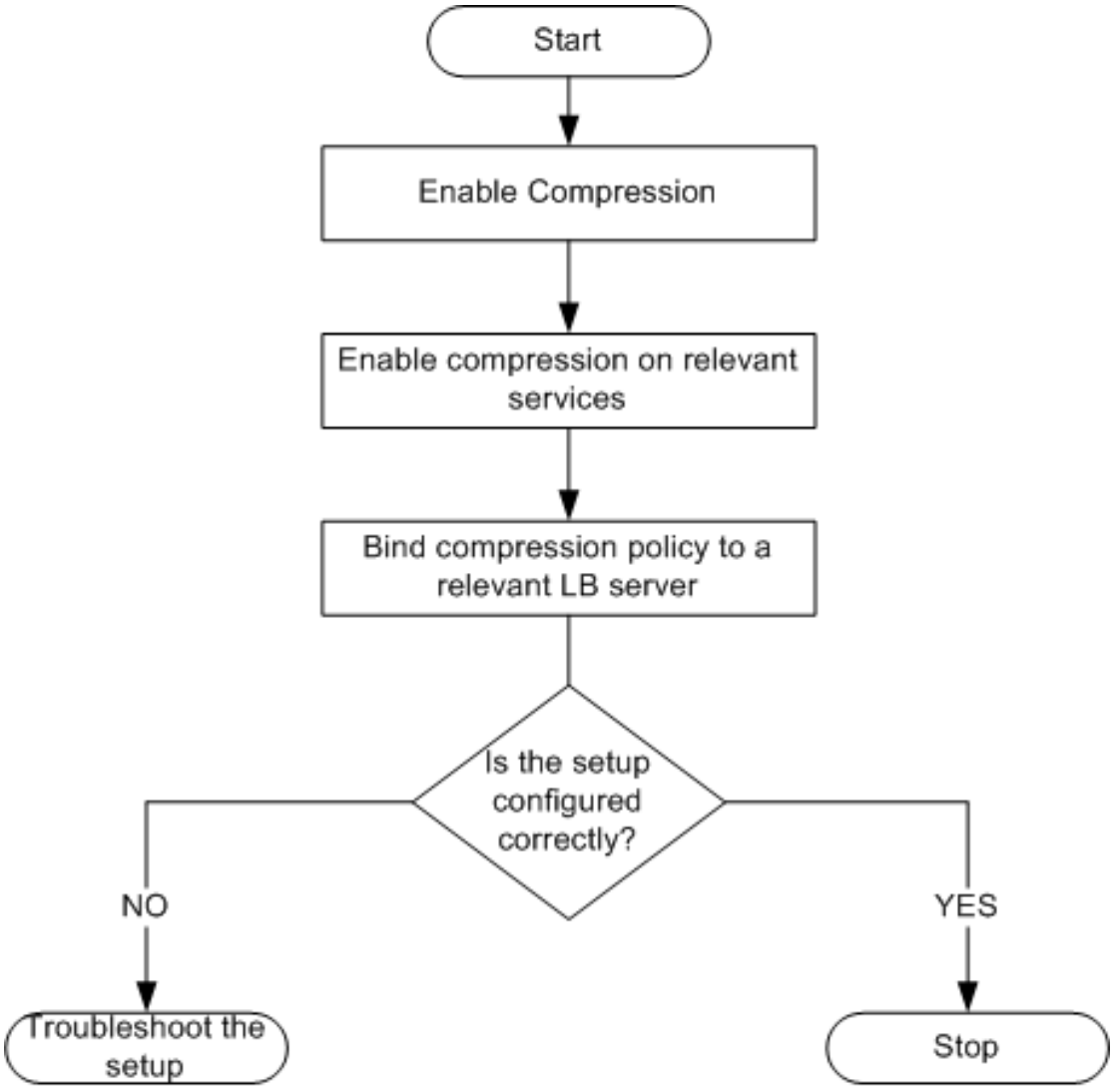
To configure compression, you must enable it globally and on each service that will provide responses that you want compressed. If you have configured virtual servers for load balancing or content switching, you should bind the polices to the virtual servers. Otherwise, the policies apply to all traffic that passes through the appliance.

Note: For more information about compression, see "Compression."

Compression Configuration Task Sequence

The following flow chart shows the sequence of tasks for configuring basic compression in a load balancing setup.

Figure 1. Sequence of Tasks to Configure Compression



Note: The steps in the above figure assume that load balancing has already been configured. For information about configuring load balancing, or for more information about services, see "Load Balancing."

If you want to configure something other than a basic compression setup, (for example, if you need to configure optional parameters in addition to the required parameters) see "Compression."

Enabling Compression

By default, compression is not enabled. You must enable the compression feature to allow compression of HTTP responses that are sent to the client.

To enable compression by using the command line interface

At the command prompt, type the following commands to enable compression and verify the configuration:

- `enable ns feature CMP`
- `show ns feature`

Example

```
> enable ns feature CMP
Done
> show ns feature

     Feature                Acronym          Status
     -------                -------          ------
1)   Web Logging             WL               ON
2)   Surge Protection        SP               OFF
.
7)   Compression Control     CMP              ON
8)   Priority Queuing        PQ               OFF
.
Done
```

To enable compression by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features, click Change basic features.
3. In the Configure Basic Features dialog box, select the Compression check box, and then click OK.
4. In the Enable/Disable Feature(s)? dialog box, click Yes.

Configuring Services to Compress Data

In addition to enabling compression globally, you must enable it on each service that will deliver files to be compressed. To create a service, see "Configuring Services."

To enable compression on a service by using the command line

At the command prompt, type the following commands to enable compression on a service and verify the configuration:

- set service <name> -CMP YES
- show service <name>

Example

```
> show service SVC_HTTP1
SVC_HTTP1 (10.102.29.18:80) - HTTP
State: UP
Last state change was at Tue Jun 16 06:19:14 2009 (+737 ms)
Time since last state change: 0 days, 03:03:37.200
Server Name: 10.102.29.18
Server ID : 0   Monitor Threshold : 0
Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
Use Source IP: NO
Client Keepalive(CKA): NO
Access Down Service: NO
TCP Buffering(TCPB): NO
HTTP Compression(CMP): YES
Idle timeout: Client: 180 sec   Server: 360 sec
Client IP: DISABLED
Cacheable: NO
SC: OFF
SP: OFF
Down state flush: ENABLED

1)      Monitor Name: tcp-default
State: DOWN     Weight: 1
Probes: 1095    Failed [Total: 1095 Current: 1095]
Last response: Failure - TCP syn sent, reset received.
Response Time: N/A
Done
```

To enable compression on a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to configure compression (for example, service-HTTP-1), and then click Open.
3. On the Advanced tab, under Settings, select the Compression check box, and then click OK.
4. Verify that, when the service is selected, `HTTP Compression(CMP): ON` appears in the **Details** section at the bottom of the pane.

Binding a Compression Policy to a Virtual Server

If you bind a policy to a virtual server, the policy is evaluated only by the services associated with that virtual server. You can bind compression policies to a virtual server either from the Configure Virtual Server (Load Balancing) dialog box or from the Compression Policy Manager dialog box. This topic includes instructions to bind compression policies to a load balancing virtual server by using the Configure Virtual Server (Load Balancing) dialog box. For information about how you can bind a compression policy to a load balancing virtual server by using the Compression Policy Manager dialog box, see "Configuring and Binding Policies with the Policy Manager."

To bind or unbind a compression policy to a virtual server by using the command line

At the command prompt, type the following commands to bind or unbind a compression policy to a load balancing virtual server and verify the configuration:

- `(bind|unbind) lb vserver <name> -policyName <string>`
- `show lb vserver <name>`

Example

```
> bind lb vserver lbvip -policyName ns_cmp_msapp
Done
> show lb vserver lbvip
lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
State: UP
Last state change was at Thu May 28 05:37:21 2009 (+685 ms)
Time since last state change: 19 days, 04:26:50.470
Effective State: UP
Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
Port Rewrite : DISABLED
No. of Bound Services :  1 (Total)      1 (Active)
Configured Method: LEASTCONNECTION
Current Method: Round Robin, Reason: Bound service's state changed to UP
Mode: IP
Persistence: NONE
Vserver IP and Port insertion: OFF
Push: DISABLED  Push VServer:
Push Multi Clients: NO
Push Label Rule:
```

Bound Service Groups:
1) Group Name: Service-Group-1

1) Service-Group-1 (10.102.29.252: 80) - HTTP State: UP Weight: 1

1) Policy : ns_cmp_msapp Priority:0
Done

To bind or unbind a compression policy to a load balancing virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server to which you want to bind or unbind a compression policy (for example, Vserver-LB-1), and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, on the Policies tab, click Compression.
4. Do one of the following:
   - To bind a compression policy, click Insert Policy, and then select the policy you want to bind to the virtual server.
   - To unbind a compression policy, click the name of the policy you want to unbind from the virtual server, and then click Unbind Policy.
5. Click OK.

Securing Load Balanced Traffic by Using SSL

The Citrix NetScaler SSL offload feature transparently improves the performance of web sites that conduct SSL transactions. By offloading CPU-intensive SSL encryption and decryption tasks from the local web server to the appliance, SSL offloading ensures secure delivery of web applications without the performance penalty incurred when the server processes the SSL data. Once the SSL traffic is decrypted, it can be processed by all standard services. The SSL protocol works seamlessly with various types of HTTP and TCP data and provides a secure channel for transactions using such data.

To configure SSL, you must first enable it. Then, you configure HTTP or TCP services and an SSL virtual server on the appliance, and bind the services to the virtual server. You must also add a certificate-key pair and bind it to the SSL virtual server. If you use Outlook Web Access servers, you must create an action to enable SSL support and a policy to apply the action. An SSL virtual server intercepts incoming encrypted traffic and decrypts it by using a negotiated algorithm. The SSL virtual server then forwards the decrypted data to the other entities on the appliance for appropriate processing.

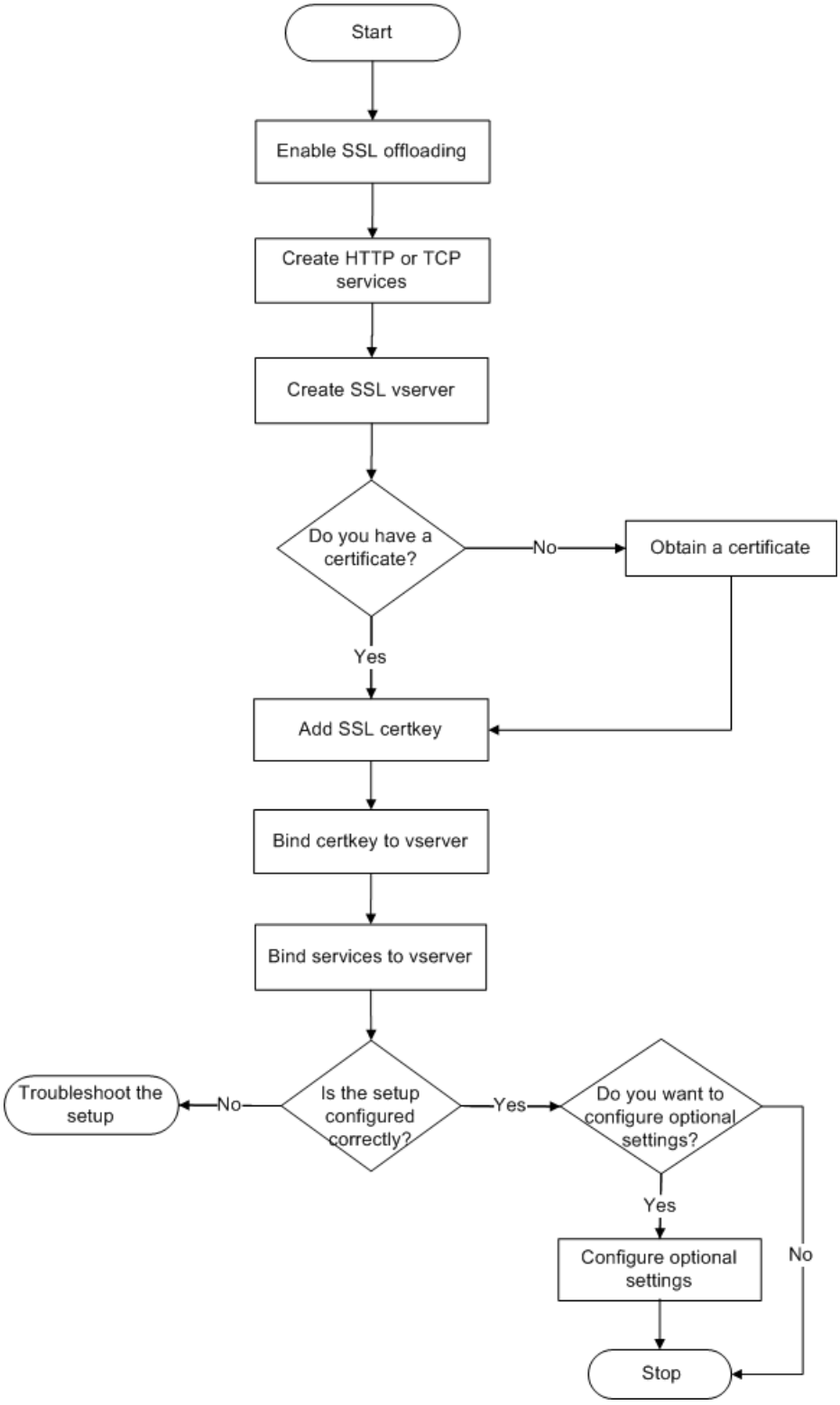
SSL Configuration Task Sequence

To configure SSL, you must first enable it. Then, you must create an SSL virtual server and HTTP or TCP services on the NetScaler. Finally, you must bind a valid SSL certificate and the configured services to the SSL virtual server.

An SSL virtual server intercepts incoming encrypted traffic and decrypts it using a negotiated algorithm. The SSL virtual server then forwards the decrypted data to the other entities on the NetScaler for appropriate processing.

The following flow chart shows the sequence of tasks for configuring a basic SSL offload setup.

Figure 1. Sequence of Tasks to Configure SSL Offloading


Start
Enable SSL offloading
Create HTTP or TCP services
Create SSL vserver
Do you have a certificate?
No
Obtain a certificate
Yes
Add SSL certkey
Bind certkey to vserver
Bind services to vserver
Troubleshoot the setup
No
Is the setup configured correctly?
Yes
Do you want to configure optional settings?
Yes
Configure optional settings
No
Stop

Enabling SSL Offload

You should enable the SSL feature before configuring SSL offload. You can configure SSL-based entities on the appliance without enabling the SSL feature, but they will not work until you enable SSL.

To enable SSL by using the command line interface

At the command prompt, type the following commands to enable SSL Offload and verify the configuration:

- `enable ns feature SSL`
- `show ns feature`

Example

```
> enable ns feature ssl
Done
> show ns feature
Feature Acronym Status
------- ------- ------
1) Web Logging WL ON
2) SurgeProtection SP OFF
3) Load Balancing LB ON . . .
 9) SSL Offloading SSL ON
10) Global Server Load Balancing GSLB ON . .
Done >
```

To enable SSL by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features, click Change basic features.
3. Select the SSL Offloading check box, and then click OK.
4. In the Enable/Disable Feature(s)? message box, click Yes.

Creating HTTP Services

A service on the appliance represents an application on a server. Once configured, services are in the disabled state until the appliance can reach the server on the network and monitor its status. This topic covers the steps to create an HTTP service.

Note: For TCP traffic, perform the procedures in this and the following topics, but create TCP services instead of HTTP services.

To add an HTTP service by using the command line interface

At the command prompt, type the following commands to add a HTTP service and verify the configuration:

- `add service <name> (<IP> | <serverName>) <serviceType> <port>`
- `show service <name>`

```
> add service SVC_HTTP1 10.102.29.18 HTTP 80
 Done
> show service SVC_HTTP1
        SVC_HTTP1 (10.102.29.18:80) - HTTP
        State: UP
        Last state change was at Wed Jul 15 06:13:05 2009
        Time since last state change: 0 days, 00:00:15.350
        Server Name: 10.102.29.18
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): YES
        Idle timeout: Client: 180 sec   Server: 360 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: tcp-default
              State: UP       Weight: 1
              Probes: 4       Failed [Total: 0 Current: 0]
              Last response: Success - TCP syn+ack received.
              Response Time: N/A
 Done
```

To add an HTTP service by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Services.
2. In details pane, click Add.
3. In the Create Service dialog box, in the Service Name, Server, and Port text boxes, type the name of the service, IP address, and port (for example, `SVC_HTTP1`, `10.102.29.18`, and `80`).
4. In the Protocol list, select the type of the service (for example, `HTTP`).
5. Click Create, and then click Close. The HTTP service you configured appears in the Services page.
6. Verify that the parameters you configured are correctly configured by selecting the service and viewing the Details section at the bottom of the pane.

For more information about services, see "Configuring Services."

Adding an SSL-Based Virtual Server

In a basic SSL offloading setup, the SSL virtual server intercepts encrypted traffic, decrypts it, and sends the clear text messages to the services that are bound to the virtual server. Offloading CPU-intensive SSL processing to the appliance allows the back-end servers to process a greater number of requests.

To add an SSL-based virtual server by using the command line interface

At the command prompt, type the following commands to create an SSL-based virtual server and verify the configuration:

- `add lb vserver <name> <serviceType> [<IPAddress> <port>]`
- `show lb vserver <name>`

Example

```
> add lb vserver vserver-SSL-1 SSL 10.102.29.50 443
Done
> show lb vserver vserver-SSL-1
vserver-SSL-1 (10.102.29.50:443) - SSL Type: ADDRESS
State: DOWN[Certkey not bound] Last state change was at Tue Jun 16 06:33:08 2009 (+176 ms)
Time since last state change: 0 days, 00:03:44.120
Effective State: DOWN Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
No. of Bound Services : 0 (Total) 0 (Active)
Configured Method: LEASTCONNECTION Mode: IP
Persistence: NONE
Vserver IP and Port insertion: OFF
Push: DISABLED Push VServer: Push Multi Clients: NO Push Label Rule: Done
```

Caution: To ensure secure connections, you must bind a valid SSL certificate to the SSL-based virtual server before you enable it.

To add an SSL-based virtual server by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (SSL Offload) dialog box, in the Name, IP Address, and Port text boxes, type the name of the virtual server, IP address, and port (for example, `Vserver-SSL-1`, `10.102.29.50`, and `443`).
4. In the Protocol list, select the type of the virtual server, for example, SSL.
5. Click Create, and then click Close.
6. Verify that the parameters you configured are correctly configured by selecting the virtual server and viewing the Details section at the bottom of the pane. The virtual server is marked as DOWN because a certificate-key pair and services have not been bound to it.

Caution: To ensure secure connections, you must bind a valid SSL certificate to the SSL-based virtual server before you enable it.

Binding Services to the SSL Virtual Server

After decrypting the incoming data, the SSL virtual server forwards the data to the services that you have bound to the virtual server.

Data transfer between the appliance and the servers can be encrypted or in clear text. If the data transfer between the appliance and the servers is encrypted, the entire transaction is secure from end to end. For more information about configuring the system for end-to-end security, see "SSL Offload and Acceleration."

To bind a service to a virtual server by using the command line interface

At the command prompt, type the following commands to bind service to the SSL virtual server and verify the configuration:

- `bind lb vserver <name> <serviceName>`
- `show lb vserver <name>`

Example

```
> bind lb vserver vserver-SSL-1 SVC_HTTP1
Done
> show lb vserver vserver-SSL-1 vserver-SSL-1 (10.102.29.50:443) - SSL Type:
ADDRESS State: DOWN[Certkey not bound]
Last state change was at Tue Jun 16 06:33:08 2009 (+174 ms)
Time since last state change: 0 days, 00:31:53.70
Effective State: DOWN Client Idle
Timeout: 180 sec
Down state flush: ENABLED Disable Primary Vserver On Down :
DISABLED No. of Bound Services : 1 (Total) 0 (Active)
Configured Method: LEASTCONNECTION Mode: IP Persistence: NONE Vserver IP and
Port insertion: OFF Push: DISABLED Push VServer: Push Multi Clients: NO Push Label Rule:

1) SVC_HTTP1 (10.102.29.18: 80) - HTTP
State: DOWN Weight: 1
Done
```

To bind a service to a virtual server by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. In the details pane, select a virtual server, and then click Open.
3. On the Services tab, in the Active column, select the check boxes next to the services that you want to bind to the selected virtual server.
4. Click OK.
5. Verify that the Number of Bound Services counter in the Details section at the bottom of the pane is incremented by the number of services that you bound to the virtual server.

Adding a Certificate Key Pair

An SSL certificate is an integral element of the SSL Key-Exchange and encryption/decryption process. The certificate is used during SSL handshake to establish the identity of the SSL server. You can use a valid, existing SSL certificate that you have on the NetScaler appliance, or you can create your own SSL certificate. The appliance supports RSA/DSA certificates of up to 4096 bits.

Note: Citrix recommends that you use a valid SSL certificate that has been issued by a trusted certificate authority. Invalid certificates and self-created certificates are not compatible with all SSL clients.

Before a certificate can be used for SSL processing, you must pair it with its corresponding key. The certificate key pair is then bound to the virtual server and used for SSL processing.

To add a certificate key pair by using the command line interface

At the command prompt, type the following commands to create a certificate key pair and verify the configuration:

- add ssl certKey <certkeyName> -cert <string> [-key <string>]
- show sslcertkey <name>

Example

```
> add ssl certKey CertKey-SSL-1 -cert ns-root.cert -key ns-root.key
 Done
> show sslcertkey CertKey-SSL-1
   Name: CertKey-SSL-1 Status: Valid,
   Days to expiration:4811 Version: 3
   Serial Number: 00 Signature Algorithm: md5WithRSAEncryption Issuer: C=US,ST=California,L=San
   Jose,O=Citrix ANG,OU=NS Internal,CN=de fault
   Validity Not Before: Oct 6 06:52:07 2006 GMT Not After : Aug 17 21:26:47 2022 GMT
   Subject: C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS Internal,CN=d efault Public Key
   Algorithm: rsaEncryption Public Key
   size: 1024
 Done
```

To add a certificate key pair by using the configuration utility

1. In the navigation pane, expand SSL, and then click Certificates.
2. In the details pane, click Add.
3. In the Install Certificate dialog box, in the Certificate-Key Pair Name text box, type a name for the certificate key pair you want to add, for example, `Certkey-SSL-1`.
4. Under Details, in Certificate File Name, click Browse (Appliance) to locate the certificate. Both the certificate and the key are stored in the /nsconfig/ssl/ folder on the appliance. To use a certificate present on the local system, select Local.
5. Select the certificate you want to use, and then click Select.
6. In Private Key File Name, click Browse (Appliance) to locate the private key file. To use a private key present on the local system, select Local.
7. Select the key you want to use and click Select. To encrypt the key used in the certificate key pair, type the password to be used for encryption in the Password text box.
8. Click Install.
9. Double-click the certificate key pair and, in the Certificate Details window, verify that the parameters have been configured correctly and saved.

Binding an SSL Certificate Key Pair to the Virtual Server

After you have paired an SSL certificate with its corresponding key, you must bind the certificate key pair to the SSL virtual server so that it can be used for SSL processing. Secure sessions require establishing a connection between the client computer and an SSL-based virtual server on the appliance. SSL processing is then carried out on the incoming traffic at the virtual server. Therefore, before enabling the SSL virtual server on the appliance, you need to bind a valid SSL certificate to the SSL virtual server.

To bind an SSL certificate key pair to a virtual server by using the command line interface

At the command prompt, type the following commands to bind an SSL certificate key pair to a virtual server and verify the configuration:

- bind ssl vserver <vServerName> -certkeyName <string>
- show ssl vserver <name>

Example

```
 > bind ssl vserver Vserver-SSL-1 -certkeyName CertKey-SSL-1
Done
> show ssl vserver Vserver-SSL-1

    Advanced SSL configuration for VServer Vserver-SSL-1:
    DH: DISABLED
    Ephemeral RSA: ENABLED Refresh Count: 0
    Session Reuse: ENABLED Timeout: 120 seconds
    Cipher Redirect: ENABLED
    SSLv2 Redirect: ENABLED
    ClearText Port: 0
    Client Auth: DISABLED
    SSL Redirect: DISABLED
    Non FIPS Ciphers: DISABLED
    SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED

1) CertKey Name: CertKey-SSL-1 Server Certificate
1) Cipher Name: DEFAULT
  Description: Predefined Cipher Alias
Done
```

To bind an SSL certificate key pair to a virtual server by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. Select the virtual server to which you want to bind the certificate key pair, for example, Vserver-SSL-1, and click Open.
3. In the Configure Virtual Server (SSL Offload) dialog box, on the SSL Settings tab, under Available, select the certificate key pair that you want to bind to the virtual server (for example, Certkey-SSL-1), and then click Add.
4. Click OK.
5. Verify that the certificate key pair that you selected appears in the Configured area.

Configuring Support for Outlook Web Access

If you use Outlook Web Access (OWA) servers on your NetScaler appliance, you must configure the appliance to insert a special header field, FRONT-END-HTTPS: ON, in HTTP requests directed to the OWA servers, so that the servers generate URL links as https:// instead of http://.

Note: You can enable OWA support for HTTP-based SSL virtual servers and services only. You cannot apply it for TCP-based SSL virtual servers and services.

To configure OWA support, do the following:

- Create an SSL action to enable OWA support.
- Create an SSL policy.
- Bind the policy to the SSL virtual server.

Creating an SSL Action to Enable OWA Support

Before you can enable Outlook Web Access (OWA) support, you must create an SSL action. SSL actions are bound to SSL policies and triggered when incoming data matches the rule specified by the policy.

To create an SSL action to enable OWA support by using the command line interface

At the command prompt, type the following commands to create an SSL action to enable OWA support and verify the configuration:

- add ssl action <name> -OWASupport ENABLED
- show SSL action <name>

```
 > add ssl action Action-SSL-OWA -OWASupport enabled
Done
> show SSL action Action-SSL-OWA
  Name: Action-SSL-OWA
  Data Insertion Action: OWA
  Support: ENABLED
Done
```

To create an SSL action to enable OWA support by using the configuration utility

1. In the navigation pane, expand SSL, and then click Policies.
2. In the details pane, on the Actions tab, click Add.
3. In the Create SSL Action dialog box, in the Name text box, type `Action-SSL-OWA`.
4. Under Outlook Web Access, select Enabled.
5. Click Create, and then click Close.
6. Verify that Action-SSL-OWA appears in the **SSL Actions** page.

Creating SSL Policies

SSL policies are created by using the policy infrastructure. Each SSL policy has an SSL action bound to it, and the action is carried out when incoming traffic matches the rule that has been configured in the policy.

To create an SSL policy by using the command line interface

At the command prompt, type the following commands to configure an SSL policy and verify the configuration:

- add ssl policy <name> -rule <expression> -reqAction <string>
- show ssl policy <name>

Example

```
> add ssl policy Policy-SSL-1 -rule ns_true -reqaction Action-SSL-OWA
Done
> show ssl policy Policy-SSL-1
Name: Policy-SSL-1      Rule: ns_true
Action: Action-SSL-OWA  Hits: 0
Policy is bound to following entities
1)      PRIORITY : 0
Done
```

To create an SSL policy by using the configuration utility

1. In the navigation pane, expand SSL, and then click Policies.
2. In the details pane, click Add.
3. In the Create SSL Policy dialog box, in the Name text box, type the name of the SSL Policy (for example, `Policy-SSL-1`).
4. In Request Action, select the configured SSL action that you want to associate with this policy (for example, Action-SSL-OWA). The `ns_true` general expression applies the policy to all successful SSL handshake traffic. However, if you need to filter specific responses, you can create policies with a higher level of detail. For more information about configuring granular policy expressions, see "Understanding Policies and Expressions."
5. In Named Expressions, choose the built-in general expression `ns_true` and click Add Expression. The expression `ns_true` now appears in the Expression text box.
6. Click Create, and then click Close.
7. Verify that the policy is correctly configured by selecting the policy and viewing the Details section at the bottom of the pane.

Binding the SSL Policy to an SSL Virtual Server

After you configure an SSL policy for Outlook Web Access, bind the policy to a virtual server that will intercept incoming Outlook traffic. If the incoming data matches any of the rules configured in the SSL policy, the policy is triggered and the action associated with it is carried out.

To bind an SSL policy to an SSL virtual server by using the command line interface

At the command prompt, type the following commands to bind an SSL policy to an SSL virtual server and verify the configuration:

- bind ssl vserver <vServerName> -policyName <string>
- show ssl vserver <name>

Example

```
> bind ssl vserver Vserver-SSL-1 -policyName Policy-SSL-1
 Done
> show ssl vserver Vserver-SSL-1
        Advanced SSL configuration for VServer Vserver-SSL-1:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 0
        Session Reuse: ENABLED          Timeout: 120 seconds
        Cipher Redirect: ENABLED
        SSLv2 Redirect: ENABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED

1)      CertKey Name: CertKey-SSL-1 Server Certificate

1)      Policy Name: Policy-SSL-1
                        Priority: 0
1)      Cipher Name: DEFAULT
        Description: Predefined Cipher Alias
 Done
>
```

To bind an SSL policy to an SSL virtual server by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. In the details pane, select the virtual server (for example, Vserver-SSL-1), and then click Open.
3. In the Configure Virtual Server (SSL Offload) dialog box, click Insert Policy, and then select the policy that you want to bind to the SSL virtual server. Optionally, you can double-click the Priority field and type a new priority level.
4. Click OK.

Features at a Glance

Citrix NetScaler features can be configured independently or in combinations to address specific needs. Although some features fit more than one category, the numerous NetScaler features can generally be categorized as application switching and traffic management features, application acceleration features, and application security and firewall features, and an application visibility feature.

To understand the order in which the features perform their processing, see "Processing Order of Features."

Application Switching and Traffic Management Features

SSL Offloading

Transparently offloads SSL encryption and decryption from web servers, freeing server resources to service content requests. SSL places a heavy burden on an application's performance and can render many optimization measures ineffective. SSL offload and acceleration allow all the benefits of Citrix Request Switching technology to be applied to SSL traffic, ensuring secure delivery of web applications without degrading end-user performance.

For more information, see "SSL Offload and Acceleration."

Access Control Lists

Compares incoming packets to Access Control Lists (ACLs). If a packet matches an ACL rule, the action specified in the rule is applied to the packet. Otherwise, the default action (ALLOW) is applied and the packet is processed normally. For the appliance to compare incoming packets to the ACLs, you have to apply the ACLs. All ACLs are enabled by default, but you have to apply them in order for the NetScaler to compare incoming packets against them. If an ACL is not required to be a part of the lookup table, but still needs to be retained in the configuration, it should be disabled before the ACLs are applied. A NetScaler does not compare incoming packets to disabled ACLs.

For more information, see "Access Control Lists."

Load Balancing

Load balancing decisions are based on a variety of algorithms, including round robin, least connections, weighted least bandwidth, weighted least packets, minimum response time, and hashing based on URL, domain source IP, or destination IP. Both the TCP and UDP protocols are supported, so the NetScaler can load balance all traffic that uses those protocols as the underlying carrier (for example, HTTP, HTTPS, UDP, DNS, NNTP, and general firewall traffic). In addition, the NetScaler can maintain session persistence based on source IP, cookie, server, group, or SSL session. It allows users to apply custom Extended Content Verification (ECV) to servers, caches, firewalls and other infrastructure devices to ensure that these systems are functioning properly and are providing the right content to users. It can also perform health checks using ping, TCP, or HTTP URL, and the user can create monitors based on Perl scripts. To provide high-scale WAN optimization, the CloudBridge appliances deployed at data centers can be load balanced through NetScaler appliances. The bandwidth and number of concurrent sessions can be improved significantly.

For more information, see "Load Balancing."

Content Switching

Determines the server to which to send the request on the basis of configured content switching policies. Policy rules can be based on the IP address, URL, and HTTP headers.

This allows switching decisions to be based on user and device characteristics such as who the user is, what type of agent is being used, and what content the user requested.

For more information, see "Content Switching."

Global Server Load Balancing (GSLB)

Extends the traffic management capabilities of a NetScaler to include distributed Internet sites and global enterprises. Whether installations are spread across multiple network locations or multiple clusters in a single location, the NetScaler maintains availability and distributes traffic across them. It makes intelligent DNS decisions to prevent users from being sent to a site that is down or overloaded. When the proximity-based GSLB method is enabled, the NetScaler can make load balancing decisions based on the proximity of the client's local DNS server (LDNS) in relation to different sites. The main benefit of the proximity-based GSLB method is faster response time resulting from the selection of the closest available site.

For more information, see "Global Server Load Balancing."

Dynamic Routing

Enables routers to obtain topology information, routes, and IP addresses from neighboring routers automatically. When dynamic routing is enabled, the corresponding routing process listens to route updates and advertises routes. The routing processes can also be placed in passive mode. Routing protocols enable an upstream router to load balance traffic to identical virtual servers hosted on two standalone NetScaler units using the Equal Cost Multipath technique.

For more information, see "Configuring Dynamic Routes."

Link Load Balancing

Load balances multiple WAN links and provides link failover, further optimizing network performance and ensuring business continuity. Ensures that network connections remain highly available, by applying intelligent traffic control and health checks to distribute traffic efficiently across upstream routers. Identifies the best WAN link to route both incoming and outbound traffic based on policies and network conditions, and protects applications against WAN or Internet link failure by providing rapid fault detection and failover.

For more information, see " Link Load Balancing."

TCP Optimization

You can use TCP profiles to optimize TCP traffic. TCP profiles define the way that NetScaler virtual servers process TCP traffic. Administrators can use the built-in TCP profiles or configure custom profiles. After defining a TCP profile, you can bind it to a single virtual server or to multiple virtual servers.

Web Interface on NetScaler

Provides access to XenApp and XenDesktop resources, which include applications, content, and desktops. Users access resources through a standard Web browser or by using the Citrix XenApp plug-in. The Web Interface runs as a service on port 8080 on the NetScaler appliance. To create Web Interface sites, Java is executed on Apache Tomcat Web server version 6.0.26 on the NetScaler appliance.

Note: Web Interface is supported only on NetScaler nCore releases.

For more information, see "Web Interface."

CloudBridge

The Citrix NetScaler CloudBridge feature, a fundamental part of the Citrix OpenCloud framework, is a tool used to build a cloud-extended data center. The OpenCloud Bridge enables you to connect one or more NetScaler appliances or NetScaler virtual appliances on the cloud-to your network without reconfiguring your network. Cloud hosted applications appear as though they are running on one contiguous enterprise network. The primary purpose of the OpenCloud Bridge is to enable companies to move their applications to the cloud while reducing costs and the risk of application failure. In addition, the OpenCloud Bridge increases network security in cloud environments. An OpenCloud Bridge is a Layer-2 network bridge that connects a NetScaler appliance or NetScaler virtual appliance on a cloud instance to a NetScaler appliance or NetScaler virtual appliance on your LAN. The connection is made through a tunnel that uses the Generic Routing Encapsulation (GRE) protocol. The GRE protocol provides a mechanism for encapsulating packets from a wide variety of network protocols to be forwarded over another protocol. Then Internet Protocol security (IPsec) protocol suite is used to secure the communication between the peers in the OpenCloud Bridge.

For more information, see "CloudBridge."

DataStream

The NetScaler DataStream feature provides an intelligent mechanism for request switching at the database layer by distributing requests on the basis of the SQL query being sent.

When deployed in front of database servers, a NetScaler ensures optimal distribution of traffic from the application servers and Web servers. Administrators can segment traffic according to information in the SQL query and on the basis of database names, user names, character sets, and packet size.

You can configure load balancing to switch requests according to load balancing algorithms, or you can elaborate the switching criteria by configuring content switching to make a decision based on SQL query parameters, such as user name, database names, and command parameters. You can further configure monitors to track the states of database servers.

The advanced policy infrastructure on the NetScaler appliance includes expressions that you can use to evaluate and process the requests. The advanced expressions evaluate traffic associated with MySQL database servers. You can use request-based expressions (expressions that begin with `MYSQL.CLIENT` and `MYSQL.REQ`) in advanced policies to make request switching decisions at the content switching virtual server bind point and response-based expressions (expressions that begin with `MYSQL.RES`) to evaluate server responses to user-configured health monitors.

Note: DataStream is supported for MySQL and MS SQL databases.

For more information, see "DataStream."

Application Acceleration Features

AppCompress

Uses the gzip compression protocol to provide transparent compression for HTML and text files. The typical 4:1 compression ratio yields up to 50% reduction in bandwidth requirements out of the data center. It also results in significantly improved end-user response time, because it reduces the amount of data that must be delivered to the user's browser.

For more information, see "Compression."

Cache Redirection

Manages the flow of traffic to a reverse proxy, transparent proxy, or forward proxy cache farm. Inspects all requests, and identifies non-cacheable requests and sends them directly to the origin servers over persistent connections. By intelligently redirecting non-cacheable requests back to the origin web servers, the NetScaler appliance frees cache resources and increases cache hit rates while reducing overall bandwidth consumption and response delays for these requests.

For more information, see "Cache Redirection."

AppCache

Helps optimize web content and application data delivery by providing a fast in-memory HTTP/1.1 and HTTP/1.0 compliant web caching for both static and dynamic content. This on-board cache stores the results of incoming application requests even when an incoming request is secured or the data compressed, and then reuses the data to fulfill subsequent requests for the same information. By serving data directly from the on-board cache, the appliance can reduce page regeneration times by eliminating the need to funnel static and dynamic content requests to the server.

For more information, see "Integrated Caching."

TCP Buffering

Buffers the server's response and delivers it to the client at the client's speed, thus offloading the server faster and thereby improving the performance of web sites.

For more information, see "TCP Buffering."

Application Security and Firewall Features

Denial of Service Attack (DoS) Defense

Detects and stops malicious distributed denial-of-service (DDoS) attacks and other types of malicious attacks before they reach your servers, preventing them from affecting network and application performance. The NetScaler appliance identifies legitimate clients and elevates their priority, leaving suspect clients unable to consume a disproportionate percentage of resources and cripple your site. The appliance provides application-level protection from the following types of malicious attacks:

- SYN flood attacks
- Pipeline attacks
- Teardrop attacks
- Land attacks
- Fraggle attacks
- Zombie connection attacks

The appliance aggressively defends against these types of attacks by preventing the allocation of server resources for these connections. This insulates servers from the overwhelming flood of packets associated with these events.

The appliance also protects network resources from ICMP based attacks by using ICMP rate limiting and aggressive ICMP packet inspection. It performs strong IP reassembly, drops a variety of suspicious and malformed packets, and applies Access Control Lists (ACLs) to site traffic for further protection.

For more information, see "HTTP Denial-of-Service Protection."

Content Filtering

Provides protection from malicious attacks for web sites at the Layer 7 level. The appliance inspects each incoming request according to user-configured rules based on HTTP headers, and performs the action the user configured. Actions can include resetting the connection, dropping the request, or sending an error message to the user's browser. This allows the appliance to screen unwanted requests and reduces your servers' exposure to attacks.

This feature can also analyze HTTP GET and POST requests and filter out known bad signatures, allowing it to defend your servers against HTTP-based attacks.

For more information, see "Content Filtering."

Responder

Functions like an advanced filter and can be used to generate responses from the appliance to the client. Some common uses of this feature are generation of redirect

responses, user defined responses, and resets.

For more information, see "Responder."

Rewrite

Modifies HTTP headers and body text. You can use the rewrite feature to add HTTP headers to an HTTP request or response, make modifications to individual HTTP headers, or delete HTTP headers. It also enables you to modify the HTTP body in requests and responses.

When the appliance receives a request or sends a response, it checks for rewrite rules, and if applicable rules exist, it applies them to the request or response before passing it on to the web server or client computer.

For more information, see "Rewrite."

Priority Queuing

Prioritizes user requests to ensure that the most important traffic is serviced first during surges in request volume. You can establish priority based on request URLs, cookies, or a variety of other factors. The appliance places requests in a three-tier queue based on their configured priority, enabling business-critical transactions to flow smoothly even during surges or site attacks.

For more information, see "Priority Queuing."

Surge Protection

Regulates the flow of user requests to servers and controls the number of users that can simultaneously access the resources on the servers, queuing any additional requests once your servers have reached their capacity. By controlling the rate at which connections can be established, the appliance blocks surges in requests from being passed on to your servers, thus preventing site overload.

For more information, see "Surge Protection."

Access Gateway

Access Gateway is a secure application access solution that provides administrators granular application-level policy and action controls to secure access to applications and data while allowing users to work from anywhere. It gives IT administrators a single point of control and tools to help ensure compliance with regulations and the highest levels of information security across and outside the enterprise. At the same time, it empowers users with a single point of access—optimized for roles, devices, and networks—to the enterprise applications and data they need. This unique combination of capabilities helps maximize the productivity of today's mobile workforce.

For more information, see "Access Gateway."

Application Firewall

Protects applications from misuse by hackers and malware, such as cross site scripting attacks, buffer overflow attacks, SQL injection attacks, and forceful browsing, by filtering traffic between each protected web server and users that connect to any web site on that web server. The application firewall examines all traffic for evidence of

attacks on web server security or misuse of web server resources, and takes the appropriate action to prevent these attacks from succeeding.

For more information, see "Application Firewall."

Application Visibility Feature

NetScaler Insight Center

NetScaler Insight Center is a high performance collector that provides end-to-end user experience visibility across Web and HDX (ICA) traffic. It collects HTTP and ICA AppFlow records generated by NetScaler ADC appliances and populates analytical reports covering Layer 3 to Layer 7 statistics. NetScaler Insight Center provides in-depth analysis for the last five minutes of real-time data, and for historical data collected for the last one hour, one day, one week, and one month.

HDX (ICA) analytic dashboard enables you to drill down from HDX Users, Applications, Desktops, and even from gateway-level information. Similarly, HTTP analytics provide a bird's eye view of Web Applications, URLs Accessed, Client IP Addresses and Server IP Addresses, and other dashboards. The administrator can drill down and identify the pain points from any of these dashboards, as appropriate for the use case.

EdgeSight for NetScaler

Support for application performance monitoring based on end user experience. This solution leverages the HTML injection feature to obtain various time values, which are used by EdgeSight server for analysis and report generation. EdgeSight for NetScaler provides a way to monitor the performance benefits of a NetScaler and determine potential bottlenecks in a network.

For more information, see "EdgeSight Monitoring for NetScaler."

Enhanced Application Visibility Using AppFlow

The Citrix NetScaler appliance is a central point of control for all application traffic in the data center. It collects flow and user-session level information valuable for application performance monitoring, analytics, and business intelligence applications. AppFlow transmits this information by using the Internet Protocol Flow Information eXport (IPFIX) format, which is an open Internet Engineering Task Force (IETF) standard defined in RFC 5101. IPFIX (the standardized version of Cisco's NetFlow) is widely used to monitor network flow information. AppFlow defines new Information Elements to represent application-level information.

Using UDP as the transport protocol, AppFlow transmits the collected data, called *flow records*, to one or more IPv4 collectors. The collectors aggregate the flow records and generate real-time or historical reports.

AppFlow provides visibility at the transaction level for HTTP, SSL, TCP, and SSL_TCP flows. You can sample and filter the flow types that you want to monitor.

To limit the types of flows to monitor, by sampling and filtering the application traffic, you can enable AppFlow for a virtual server. AppFlow can also provide statistics for the virtual server.

You can also enable AppFlow for a specific service, representing an application server, and monitor the traffic to that application server.

For more information, see "AppFlow."

Stream Analytics

The performance of your web site or application depends on how well you optimize the delivery of the most frequently requested content. Techniques such as caching and compression help accelerate the delivery of services to clients, but you need to be able to identify the resources that are requested most frequently, and then cache or compress those resources. You can identify the most frequently used resources by aggregating real-time statistics about website or application traffic. Statistics such as how frequently a resource is accessed relative to other resources and how much bandwidth is consumed by those resources help you determine whether those resources need to be cached or compressed to improve server performance and network utilization. Statistics such as response times and the number of concurrent connections to the application help you determine whether you must enhance server-side resources.

If the web site or application does not change frequently, you can use products that collect statistical data, and then manually analyze the statistics and optimize the delivery of content. However, if you do not want to perform manual optimizations, or if your web site or application is dynamic in nature, you need infrastructure that can not only collect statistical data but can also automatically optimize the delivery of resources on the basis of the statistics. On the NetScaler appliance, this functionality is provided by the Stream Analytics feature. The feature operates on a single NetScaler appliance and collects run-time statistics on the basis of criteria that you define. When used with NetScaler policies, the feature also provides you with the infrastructure that you need for automatic, real-time traffic optimization.

For more information, see "Stream Analytics."

Optimization

2015-05-18 16:55:22 UTC

Contents

Optimization

The NetScaler optimization features reduce transaction times between the clients and the servers, and they reduce bandwidth consumption. They also enhance server performance by offloading some tasks and making others more efficient. This collection includes the following topics:

Client keep-alive	Handles multiple requests on a single client connection. The client does not have to negotiate a new connection for each request to the server.
Compression	Compresses HTTP responses sent from the servers to compression-aware browsers. The smaller responses reduce download time and save bandwidth.
Integrated Caching	Stores responses to client requests. Subsequent requests for the same content are served from the NetScaler cache instead of being forwarded to the origin server.
TCP-Buffering	Buffers the server's response and sends it to the client at the client's speed. The server can quickly offload the requested data and then devote its resources to other tasks.
TCP keep-alive	Sends TCP keep-alive probes to check the operational state of the peer.

Client Keep-Alive

The Citrix NetScaler appliance provides features such as client keep-alive to improve the performance of a transaction management environment. Performance of any transaction management environment depends on factors such as bandwidth usage, download time, speed of the server and the client networks, and time consumed to complete a transaction. Client keep-alive improves performance by reducing the time consumed in a transaction. Two other settings that affect connection management include the maximum number of HTTP connections retained in the connection reuse pool and whether or not connection multiplexing is enabled. These variables are configured with HTTP profiles.

Client keep-alive enables multiple client requests to be sent on a single client connection. This feature helps in a transaction management environment where the server closes the client connection after serving the response to the client. The client has to open a new connection for each request to the server leading to a lot of time being consumed for a transaction. The client keep-alive feature of the appliance alleviates this problem by keeping the client-side connection open between the client and the appliance even after the server closes the client connection. This allows multiple client requests to be sent using a single connection. Keeping the client-side connection open saves the packet round trips associated with opening and closing a connection. This is most beneficial to SSL sessions because this eliminates unnecessary termination and open sequences, thus reducing the time taken for a transaction to occur.

Client keep-alive is useful under either of the following conditions:

- When the server does not support client keep-alive.
- When the server supports client keep-alive but an application on the server does not support client keep-alive.

Client keep-alive can be applied to all HTTP services globally, or to a specific service, such as HTTP or SSL. Note that client keep-alive applies only to HTTP and HTTPS services.

The following figure illustrates a typical client keep-alive deployment.

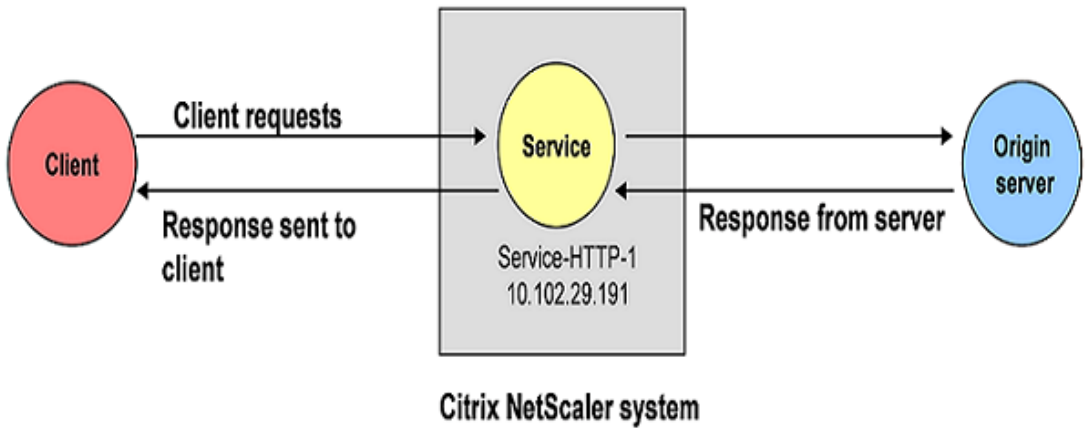


Figure 1. Client Keep-Alive Entity Model

As shown in the figure, to configure client keep-alive, you need to define services and enable client keep-alive for those services. Services represent applications on physical servers. The traffic from the client is intercepted by the configured service and the client request is directed to the origin server. The server sends the response and closes the connection between the server and the appliance. If a “Connection: Close” header is sent, this header is corrupted in the client-side response, and the client-side connection is kept open. As a result, the client does not have to open a new connection for the next request; instead, the connection to the server is reopened.

Note: If a server sends back two “Connection: Close” headers, only one is edited. This results in significant delays on the client rendering of the object because a client does not assume that the object has been delivered completely until the connection is actually closed.

Client Keep-Alive

The Citrix NetScaler appliance provides features such as client keep-alive to improve the performance of a transaction management environment. Performance of any transaction management environment depends on factors such as bandwidth usage, download time, speed of the server and the client networks, and time consumed to complete a transaction. Client keep-alive improves performance by reducing the time consumed in a transaction. Two other settings that affect connection management include the maximum number of HTTP connections retained in the connection reuse pool and whether or not connection multiplexing is enabled. These variables are configured with HTTP profiles.

Client keep-alive enables multiple client requests to be sent on a single client connection. This feature helps in a transaction management environment where the server closes the client connection after serving the response to the client. The client has to open a new connection for each request to the server leading to a lot of time being consumed for a transaction. The client keep-alive feature of the appliance alleviates this problem by keeping the client-side connection open between the client and the appliance even after the server closes the client connection. This allows multiple client requests to be sent using a single connection. Keeping the client-side connection open saves the packet round trips associated with opening and closing a connection. This is most beneficial to SSL sessions because this eliminates unnecessary termination and open sequences, thus reducing the time taken for a transaction to occur.

Client keep-alive is useful under either of the following conditions:

- When the server does not support client keep-alive.
- When the server supports client keep-alive but an application on the server does not support client keep-alive.

Client keep-alive can be applied to all HTTP services globally, or to a specific service, such as HTTP or SSL. Note that client keep-alive applies only to HTTP and HTTPS services.

The following figure illustrates a typical client keep-alive deployment.

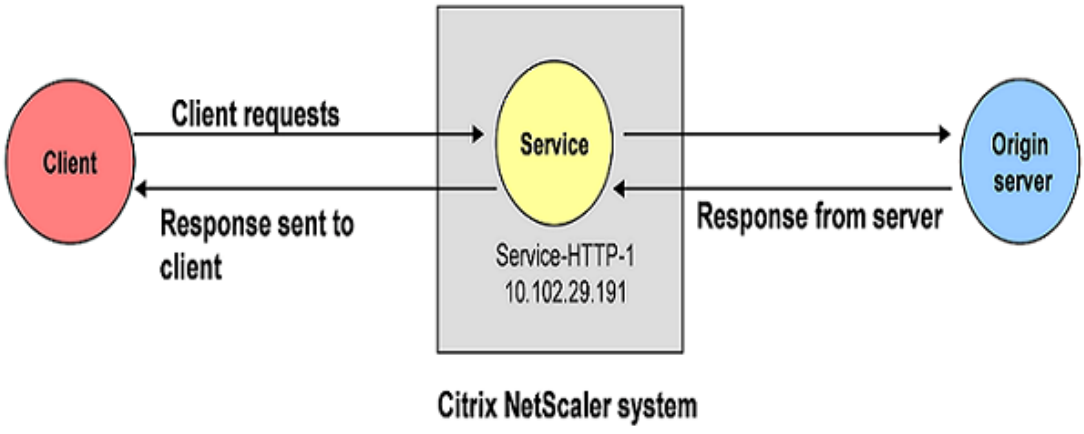


Figure 1. Client Keep-Alive Entity Model

As shown in the figure, to configure client keep-alive, you need to define services and enable client keep-alive for those services. Services represent applications on physical servers. The traffic from the client is intercepted by the configured service and the client request is directed to the origin server. The server sends the response and closes the connection between the server and the appliance. If a “Connection: Close” header is sent, this header is corrupted in the client-side response, and the client-side connection is kept open. As a result, the client does not have to open a new connection for the next request; instead, the connection to the server is reopened.

Note: If a server sends back two “Connection: Close” headers, only one is edited. This results in significant delays on the client rendering of the object because a client does not assume that the object has been delivered completely until the connection is actually closed.

Configuring Client Keep-Alive

To configure the client keep-alive feature, you need to create a service and enable client keep-alive for that service.

The service you configure enables the NetScaler appliance to keep the client-side connection open even after the server has closed the connection between the server and the appliance.

Note that while configuring a service, if the client keep-alive option is not explicitly specified, the service uses the global setting for the client keep-alive connection. For more information, see "Enabling or Disabling Client Keep-Alive Globally."

To create a service with client keep-alive enabled by using the command line interface

At the command prompt, type:

add service (<name> | <IPaddress>) <serviceType> <port> -CKA (YES | NO)

Example

> add service Service-HTTP-1 10.102.29.191 HTTP 80 -CKA YES

To create a service with client keep-alive enabled by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, amongst other service-related configurations, in the Advanced tab, under Settings, select Override Global and then select Client Keep-Alive.
4. Click Create, and then click Close.

Parameter Descriptions (of commands listed in the CLI procedure)

add service

CKA

The state of the Client Keep-Alive feature for the service. Possible values: YES, NO

View description(s) in command reference Top

Enabling or Disabling Client Keep-Alive Globally

The client keep-alive feature is disabled by default. If you enable client keep-alive globally, all new services inherit the global settings by default. The following procedure describes the steps to enable or disable client keep-alive globally.

To enable or disable the client keep-alive mode globally by using the command line interface

At the command prompt, type one of the following commands:

- enable ns mode cka
- disable ns mode cka

To enable or disable the client keep-alive mode globally by using the configuration utility

1. Navigate to System > Settings.
2. In the details pane, under Modes and Features, click Configure modes.
3. In the Configure Modes dialog box, select or clear the Client Keep-Alive check box.
4. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns mode

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable ns mode

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Enabling or Disabling Client Keep-Alive for a Service

You can enable or disable client keep-alive at the service level. Note that the service level settings take precedence over the global settings. The following procedure describes the steps to enable or disable client keep-alive at the service level.

To enable or disable the client keep-alive mode for a service by using the command line interface

At the command prompt, type:

set service (<name> | <IPaddress>) -CKA (YES | NO)

Example

> set service Service-HTTP-1 -CKA YES

To enable or disable the client keep-alive mode for a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click the service for which you want to enable or disable client keep-alive, and then click Open.
3. In the Configure Service dialog box, on the Advanced tab, under Settings, select or clear the Client Keep-Alive check box.
4. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set service

name

The name of the service.

IPaddress

The new IP address of the service.

CKA

The state of the Client Keep-Alive feature for the service. Possible values: YES, NO

View description(s) in command reference Top

Configuring Connection Options with HTTP Profiles

An HTTP profile is a collection of configuration settings that is used to control HTTP requests to and responses from virtual servers on a NetScaler appliance. You can use HTTP profiles to configure the maximum number of HTTP connections retained in the connection reuse pool. You can also use HTTP profiles to enable connection multiplexing if you are not sure that it is already enabled (By default, connection multiplexing is enabled.), and to enable Persistence ETag.

When Persistent ETag is enabled, the ETag header includes information about the server that served the content. This ensures that cache validation conditional requests or browser requests, for that content, always reaches the same server. By default, Persistent ETag is disabled.

For more information about HTTP profiles, see "Configuring HTTP Profiles."

To configure the number of connections in the reuse pool by using the command line interface

At the command prompt, type:

set ns httpProfile <name> -maxReusePool <value>

To configure the number of connections in the reuse pool by using the configuration utility

1. Navigate to System > Profiles.
2. In the details pane, on the HTTP Profiles tab, select the HTTP profile for which you want to configure the number of connections, and then click Open.
3. In the Configure HTTP Profiles dialog box, in Max connections in reusepool, specify the maximum number of connections you want to allow in connection reuse pool.
4. Click OK.

To enable connection multiplexing by using the command line interface

At the command prompt, type:

set ns httpProfile <name> -conMultiplex ENABLED

To enable connection multiplexing by using the configuration utility

1. Navigate to System > Profiles.
2. In the details pane, on the HTTP Profiles tab, select the HTTP profile for which you want to enable connection multiplexing, and then click Open.
3. In the Configure HTTP Profiles dialog box, select the Connection Multiplexing check box. Note that this check box is enabled by default.
4. Click OK.

To enable Persistent ETag by using the command line interface

At the command prompt, type:

set ns httpProfile <name> -persistentETag enabled

To enable Persistent ETag by using the configuration utility

1. Navigate to System > Profiles.
2. In the details pane, on the HTTP Profiles tab, select the HTTP profile for which you want to enable Persistent Etag, and then click Open.
3. In the Configure HTTP Profiles dialog box, select the Persistent ETag option. By default, this option is disabled.

Parameter Descriptions (of commands listed in the CLI procedure)

set ns httpProfile

maxReusePool

Maximum connections in reusepool. If set to zero, limit will not be applied. Maximum value: 360000

conMultiplex

Connection multiplexing Possible values: ENABLED, DISABLED Default value: ENABLED

persistentETag

Generate the persistent NetScaler specific ETag for the HTTP response with ETag header. Possible values: ENABLED, DISABLED Default value: DISABLED

View description(s) in command reference Top

Compression

The Citrix NetScaler appliance compression feature compresses the size of HTTP responses sent from servers to compression-aware browsers and thereby improves the performance of Web sites by reducing the download time of Web content. Bandwidth is also saved in the process. Another indirect benefit of HTTP compression is that the data passed between the Web server and the browser is encrypted by virtue of the compression algorithm, adding more security to the data.

After you enable the compression feature and compression is set at the service level, global compression policies are enabled, and the NetScaler can compress data for traffic that matches these policies. You can augment the built-in compression policies by creating new compression actions and policies and binding the policies globally or to particular virtual servers.

When you bind a policy globally, you specify a bind point, which corresponds to a step in the sequence in which traffic is processed. Policies bound to a virtual server have their own place in the sequence. Therefore, binding the policies affects the order in which they are evaluated. Alternatively, you can associate policies with policy labels that are not associated with a bind point. Such policies can be invoked only by other policies.

You can view statistics for compressed data that the NetScaler transmits.

Note: The compression feature uses both classic and default syntax policies. This content is best understood if you are familiar with configuration principles for basic policies, virtual servers, and services. For more information about policies, see "Policies and Expressions." For more information about virtual servers and services, see "Creating a Virtual Server" and "Configuring Services."

The NetScaler can compress HTML and other content that is generated statically or dynamically, including MIME types such as text/html, text/plain, text/xml, text/css, text/rtf, application/msword, application/vnd.ms-excel, and application/vnd.ms-powerpoint.

After you enable the compression feature on the NetScaler and set compression ON for HTTP and SSL services, built-in compression policies are applied to the HTTP and SSL services. You can disable compression on a particular service, and you can create custom compression policies and bind both the built-in and custom compression policies to a load balancing virtual server.

Enabling or Disabling Compression

If you want the NetScaler appliance to compress data, enable the compression feature and set compression ON for the configured service. After enabling compression, the built-in compression policies are in effect, and compression is automatically enabled for any services that you create.

If you want to use compression in a load balancing environment, you also enable the load balancing feature. To compress traffic that is sent over SSL, you also enable the SSL feature.

To enable or disable compression, load balancing, and SSL by using the command line interface

At the command prompt, type one of the following commands:

- enable ns feature cmp lb ssl
- disable ns feature cmp lb ssl

To enable or disable compression, load balancing, and SSL by using the configuration utility

1. Navigate to System > Settings.
2. In the details pane, under the Modes and Features group, click Configure basic features.
3. In the Configure Basic Features dialog box, select the Compression check box to enable it; clear the check box to disable it. If appropriate, also select the Load Balancing and SSL Offloading check boxes.
4. Click OK, and click Yes in the Enable/Disable Feature(s)? message box.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Enabling and Disabling Compression for a Service

By default, if the compression feature is disabled, any new service that you create is disabled for compression and uses the built-in compression policies. If you create any services prior to enabling compression, you must manually enable compression for the service.

You can disable or enable compression for HTTP and SSL services.

Compression is in effect for a compression-enabled service once you bind the service to a virtual server. You can bind HTTP services to an HTTP load balancing vserver, and bind SSL services to an SSL load balancing virtual server. The protocol types must match.

To create a compression-enabled service by using the command line interface

At the command prompt, type:

- add service <name> <IPAddress> HTTP <portNumber>
- set service <name> -CMP YES

Example

```
> add service Service-HTTP-1 10.102.29.51 HTTP 80
> set service Service-HTTP-1 -CMP YES
```

To enable or disable service-level compression by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, on the Services tab, select the service for which you want to enable or disable compression, and then click Open.
3. In the Configure Service dialog box, on the Advanced tab, under Settings, select Override Global, and then select or clear the Compression check box.
4. Click OK, and then click Close.

Parameter Descriptions (of commands listed in the CLI procedure)

add service

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

set service

CMP

The state of the HTTP Compression feature for this service. Possible values: YES, NO

View description(s) in command reference Top

Configuring Compression Actions

You associate actions with compression policies. If an HTTP request matches the policy rule, the action is applied to the response. For example, you can configure a compression policy that identifies requests that are sent to a particular server, and associate the policy with an action that compresses data that is sent with the response.

There are four built-in compression actions:

- **COMPRESS:** Uses the GZIP algorithm to compress data for browsers that support either GZIP or both GZIP and DEFLATE. The NetScaler appliance uses the DEFLATE algorithm to compress data for browsers that support the DEFLATE algorithm. If the browser does not support either algorithm, and the action has been set to COMPRESS, the NetScaler appliance does not compress data.
- **NOCOMPRESS:** Does not compress data.
- **GZIP:** Uses the GZIP algorithm to compress data for browsers that support GZIP compression. If the browser does not support the GZIP algorithm the NetScaler appliance does not compress data.
- **DEFLATE:** Uses the DEFLATE algorithm to compress data for browsers that support the DEFLATE algorithm. If the browser does not support the DEFLATE algorithm, and the action has been set to DEFLATE, the NetScaler appliance does not compress data.

Compression actions determine whether and what type of compression the NetScaler appliance applies to a response. After creating an action, you associate the action with one or more compression policies.

To create a compression action by using the command line interface

At the command prompt, type:

add cmp action <name> -cmpType (compress|gzip|deflate|nocompress)

To create a compression action by using the configuration utility

1. In the navigation pane, expand HTTP Compression, and then click Actions.
2. In the details pane, click Add.
3. In the Create Compression Action dialog box, in the Name text box, type the name of the action (for example, Action-CMP-1).
4. Under Compression Type, choose the compression type (for example, GZIP).
5. Click Create, and then click Close.

If you try to delete a built-in action, or any action that is associated with a policy, an error message appears. Only custom actions that have no associated policy can be deleted.

Parameter Descriptions (of commands listed in the CLI procedure)

add cmp action

name

The name of the compression action.

cmpType

The type of compression action. Possible values: compress, gzip, deflate, nocompress

View description(s) in command reference Top

Configuring Compression Policies

A compression policy contains a rule, which is a logical expression that enables the NetScaler appliance to identify the traffic that should be compressed.

When the Citrix NetScaler appliance receives an HTTP response from a server, it evaluates a built-in or custom compression policy to determine whether to compress the response and the type of compression to apply.

There are five built-in classic and advanced and default syntaxcompression policies. These policies are activated globally when you enable compression.

The following table describes the built-in compression policies.

Table 1. Built-in Classic and Advanced and Default Syntax Policies for Compression

Built-in Classic and Advanced Compression Policies	Description
ns_nocmp_mozilla_47 ns_adv_nocmp_mozilla_47	Does not compress CSS files when a request is sent from a Mozilla 4.7 Web browser.
ns_cmp_mscss ns_adv_cmp_mscss	Compresses CSS files when the request is sent from a Microsoft Internet Explorer Web browser.
ns_cmp_msapp ns_adv_cmp_msapp	Compresses files that are generated by the following applications: · Microsoft Office Word · Microsoft Office Excel · Microsoft Office PowerPoint
ns_cmp_content_type ns_adv_cmp_content_type	Compresses data when the response contains the header 'Content-Type' and contains text.
ns_nocmp_xml_ie ns_adv_nocmp_xml_ie	Does not compress when a request is sent from a Microsoft Internet Explorer browser with the response header 'Content-Type' and contains text or xml.

To view built-in compression policies by using the configuration utility

1. In the navigation pane, expand HTTP Compression, and then click Policies.
2. In the details pane, view the built-in compression policies.

You can create a compression policy by using the built-in compression actions and named expressions, or you can use custom actions and expressions.

To create a compression policy by using the command line interface

At the command prompt, type:

add cmp policy <name> -resAction (compress|gzip|deflate|nocompress) -rule <build_in_rule_name>|“<user_defined_rule>”

Example

> add cmp policy Policy-CMP-2 -resAction gzip -rule HTTP.REQ.HEADER(“User-Agent”).CONTAINS(“Mozilla/4.

To create a compression policy by using the configuration utility

1. In the navigation pane, expand HTTP Compression, and then click Policies.
2. In the details pane, click Add.
3. In the Create Compression Policy dialog box, in the Policy Name text box, type the name of the policy.
4. In Response Action, do one of the following:
   - To use a built-in or existing compression action, choose a compression action in the drop-down list.
   - To create a new compression action, click New. In the Create Compression Action dialog box, enter a compression action name and type, and then click Create.
5. In the Expression box, either type the default syntax expression or do one of the following:
   - Click Prefix, and then select the expression prefix you want. Then, select the flow type (REQ or RES), and then enter a period (.) to display a list of functions that can be used with the flow type. Type a period after each function until you have entered the expression you want. Click the Operators button to insert an operator (for example, a Boolean or relational operator).
   - Click Add, and then select a named expression.
6. If you want to evaluate your expression, click Evaluate.
7. If you want to clear the Expression box, click Clear.
8. Click Create, and then click Close.

You can modify the actions and expressions that are associated with a user-defined policy. However, you cannot make any modifications to the built-in compression policies.

You can remove a compression policy if the policy is not bound globally or to a vserver. If the compression policy is bound, you must first unbind it. You cannot remove a built-in compression policy.

Parameter Descriptions (of commands listed in the CLI procedure)

add cmp policy

name

The name of the HTTP compression policy to be created.

resAction

The compression action that needs to be performed when the rule matches. The string value can be either be a created compression action (user-defined) or one of the following built-in compression actions: NOCOMPRESS action - can be used to define a policy that disables compression for the matching policy.COMPRESS action - can be used to enable compression for a specific policy. This action will do GZIP or DEFLATE, based on the browser. GZIP action - can be used to enable GZIP compression for a specific policy. With this action, GZIP compression will be performed if the browser supports GZIP, other wise compression is disabled. DEFLATE action - can be used to enable DEFLATE compression for a specific policy. With this action, DEFLATE compression will be performed if the browser supports DEFLATE, otherwise compression is disabled.

rule

The rule associated with the HTTP compression policy.

View description(s) in command reference Top

Bind Points and Order of Evaluation for Default Syntax Compression Policies

For a default syntax policy to take effect, you must ensure that the policy is invoked at some point during the Citrix NetScaler appliance's processing of traffic. To specify the invocation time, you associate the policy with a bind point. The following are the built-in bind points, listed in order of evaluation:

- **Request-time override.** If a request matches a request-time override policy, by default request-time policy evaluation ends and the NetScaler appliance stores the action that is associated with the matching policy.
- **Request-time load balancing virtual server.** If policy evaluation cannot be completed after all the request-time override policies are evaluated, the NetScaler appliance processes request-time policies that are bound to load balancing virtual servers. If the request matches one of these policies, evaluation ends and the NetScaler appliance stores the action that is associated with the matching policy.
- **Request-time content switching virtual server.** Policies that are bound to this bind point are evaluated after request-time policies that are bound to load balancing virtual servers.
- **Request-time default.** If policy evaluation cannot be completed after all request-time, virtual server-specific policies are evaluated, the NetScaler appliance processes request-time default policies. If the request matches a request-time default policy, by default request-time policy evaluation ends and the NetScaler appliance stores the action that is associated with the matching policy.
- **Response-time override.** Similar to request-time override policy evaluation.
- **Response-time load balancing virtual server.** Similar to request-time virtual server policy evaluation.
- **Response-time content switching virtual server.** Similar to request-time virtual server policy evaluation.
- **Response-time default.** Similar to request-time default policy evaluation.

You can associate multiple policies with each bind point. To control the order of evaluation of the policies associated with the bind point you configure a priority level. In the absence of any other flow control information, policies are evaluated according to priority level, starting with the lowest numeric priority value.

You can also bind a given default syntax compression policy to more than one bind point. However, the bind point at which the policy is evaluated first is determined by the order specified in the preceding list. Assigned priority values must be unique within the collection of policies bound to a specific bind point. Additionally, for a given policy, only one binding is allowed per bind point at any given time. You should bind a policy with an INVAL action to a request-time override or a response-time override bind point. To delete a policy, you must first unbind it.

Table 1. Entries to Control Evaluation Flow in a Policy Label

Attribute	Specifies
Name	The name of the policy that you bound to the virtual server.
Bound To	The name of the virtual server to which the policy is bound.
Priority	The priority level used to determine when the policy is evaluated relative to other policies that are bound to this virtual server. Specify an integer. The lower the integer, the higher the priority.
Goto Expression	Determines the next policy to evaluate in this label. Goto can proceed only forward in a policy label. Omitting the Goto expression is the same as specifying END. You can provide one of the following values: · **NEXT:** Go to the policy with the next higher priority. · **END:** Stop evaluation. · **USE_INVOCATION_RESULT:** Applicable if this entry invokes another policy label. If the final Goto in the invoked bank has a value of END, evaluation stops. If the final Goto is anything other than END, the current policy label performs a NEXT. · **Positive number:** Priority number of the next policy to be evaluated. · **Numeric expression:** Expression that produces the priority number of the next policy to be evaluated.
Flow Type	You must specify a flow type to determine whether this policy is evaluated at request time or response time.
Invoke Label Type	Designates a policy label type. The value can be one of the following: · **Request Vserver:** Invokes request-time policies that are associated with a virtual server. · **Response Vserver:** Invokes response-time policies that are associated with a virtual server. · **Policy label:** Invokes another policy label, as identified by the policy label for the bank.
Invoke Label Name	The name of a virtual server or a policy label, depending on the value that you specified for the invocation type.

Finally, you can also bind compression policies to custom bind points—bind points that you create. The bind points that you create are called *policy labels*. For more information about policy labels, see "Creating Policy Labels."

Bind Points and Order of Evaluation for Classic Compression Policies

You can bind a classic compression policy either at the global level or at the virtual server (content switching or load balancing virtual server) level. You can also bind a given compression policy to more than one bind point. The priority values that are assigned to a policy that is bound to various bind points need not have the same value. For example, if you bind a policy called *mycompressionpolicy* both globally and to a load balancing virtual server, you can assign the policy a priority of 10 at the global bind point and a priority of 100 at the virtual server bind point. If you do not assign a policy a priority value, the NetScaler appliance assigns the classic compression policy a default priority value of 0 (zero).

Therefore, the priorities assigned to the classic compression policies that are bound to various bind points at any given time might be an assortment of custom priority values and default values. During classic policy evaluation, priority values are considered first. The NetScaler appliance begins with the policy that has the lowest priority value (the default value of 0, if any, or the next higher custom priority value if none of the policies have a priority value of 0) regardless of the bind point to which the policy is bound. Then, the appliance evaluates policies in ascending order of priority values while moving from one bind point to the other if necessary.

When the NetScaler appliance is evaluating policies based on their priority values, if multiple policies bound to different bind points happen to have the same priority value, the bind points of those policies are considered, with the order of evaluation progressing from the most specific bind point to the least specific bind point. For example, if classic policies are bound globally, to a content switching virtual server, and to a load balancing virtual server, the policies bound to the load balancing virtual server are evaluated first because, in this configuration, the load balancing virtual server represents the most specific bind point. The NetScaler appliance then evaluates the policies that are bound to the content switching virtual server. Finally, the appliance evaluates the policies that are bound at the global level (which is the least specific bind point in this configuration).

Finally, at a given bind point, if two or more policies have the same priority value, the chronological order in which the policies were configured is considered. Among the policies that are bound to the same bind point, with the same priority value, the policy that was configured first is evaluated first, followed by the policy that was configured second, and so on. In this way, the NetScaler appliance evaluates classic policies based first on assigned priorities, then on bind points, and finally on the chronological order in which the policies were configured.

Creating Policy Labels

You can create compression policy labels and configure banks of policies for these new labels.

Policy labels can be considered as abstract bind points that you create. You can create policy labels only for advanced policies. The policies that are bound to a policy label can be evaluated by invoking the policy label from a policy that is bound to one of the following bind points:

- Request-time override
- Request-time default
- Response-time override
- Response-time default
- A virtual server

You can invoke a policy label any number of times, unlike a policy which can only be invoked once.

To create a policy label for compression by using the command line interface

At the command prompt, type:

add cmp policylabel <labelName> -type (REQ | RES)

To create a policy label for compression by using the configuration utility

1. In the navigation pane, expand HTTP Compression, and then click Policy Labels.
2. In the details pane, click Add.
3. In the Create Compression Policy Label dialog box, in Name, specify a name for the policy label.
4. In the Evaluates drop-down list, select whether the policy label will be evaluated at request time (REQ) or response time (RES).
5. Click Insert Policy, and then select the policy, or click New Policy to create a new policy.

   Note: To ensure that the NetScaler appliance processes the policy label at the right time, you can configure an invocation of this label from the policy labels that are associated with the built-in bind points. Select the appropriate policy label of request vserver from the Invoke column field.
6. Click Create, and then click Close.

   Note: You can use the NOPOLICY “dummy” policy to invoke any policy label from another policy label. The NOPOLICY entry is a placeholder that does not process a rule.

Parameter Descriptions (of commands listed in the CLI procedure)

add cmp policylabel

labelName

The name of the HTTP compression policy label to be created.

type

Specifies when policies bound to this policy label will be evaluated. Possible values: REQ, RES

View description(s) in command reference Top

Binding Compression Policies Globally

A global compression policy applies to all services that support compression. When binding the policy, you assign it a priority. The policy is enabled by default upon creation.

To globally bind a compression policy by using the command line interface

At the command prompt, type:

bind cmp global <policyName> -priority <positiveInteger> -state (enabled|disabled)

To unbind a globally bound compression policy by using the command line interface

At the command prompt, type:

unbind cmp global <policyName>

To globally bind a compression policy by using the configuration utility

1. In the navigation pane, expand HTTP Compression, and then click Policies.
2. From the Action drop down list, select Policy Manager.
3. In the Compression Policy Manager dialog box, do one of the following:
   - To bind compression policies by using classic expressions, perform the following:
     - Click Switch to Classic Syntax on the top right corner of the page.
     - Click Global.
     - Click Insert Policy, and then click the policy name that you want to bind.
     - Double-click the Priority field for the policy and set the priority. A lower value causes the policy to be evaluated before policies with a higher priority value.
     - Click Apply Changes.

     Optionally, to configure an expression as described in "Binding Compression Policies Globally", double-click the field in the Expression column, and specify a valid expression.
   - To bind compression policies by using advanced expressions, perform the following:
     - Click Switch to Default Syntax on the top right corner of the page.
     - Select a Request or Response bind point, and then select a second level of binding of either Override Global or Default Global.

       A list of policies appears. These are policies that are bound to this bind point.
     - Click Insert Policy, and then click the policy name that you want to bind.
     - Double-click the Priority field for the policy and set the priority.

       A lower value causes the policy to be evaluated before policies with a higher priority value.
     - Specify other optional values, such as a Goto expression or invocation of an external policy label.

       To configure a Goto expression, double-click the field in the Goto Expression column, and enter valid priority level, the keywords NEXT or END, or an advanced expression.
4. Click Apply Changes, and then click Close.

Parameter Descriptions (of commands listed in the CLI procedure)

bind cmp global

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

unbind cmp global

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Binding Compression Policies to Virtual Servers

When you configure virtual server-based compression, you bind services and compression policies to a virtual server. This causes traffic that flows through a virtual server (to and from the bound services) to be subject to compression policies that you bind to the vserver.

If you bind a policy to a vserver, the policy is evaluated only by compression-enabled services that are bound to this vserver. When binding a policy, you set a priority value. Policies with a lower priority value are evaluated before policies with a higher value. After unbinding a policy from a vserver, the policy ceases to act on the services associated with that vserver.

To bind a compression policy to a load balancing vserver by using the command line interface

At the command prompt, type:

bind lb vserver <vserverName> -policyName <policyName> -priority <positiveInt>

To bind a compression policy to a load balancing vserver by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click the name of the virtual server, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, on the Policies tab, click Compression.
4. Click either Classic Expression or Advanced Expression. Click Insert Policy and select the policy that you want to bind. Optionally, you can double-click the Priority field and type a new priority level. To invoke another policy label or to configure a policy for a request vserver, from the Invoke drop-down list, make an appropriate selection. If you select a request vserver, you can bind a compression policy for the selected vserver by double-clicking the Invoke field. The Configure Compression Policies dialog box appears.
5. Click OK, and then click Close.

Parameter Descriptions (of commands listed in the CLI procedure)

bind lb vserver

policyName

The SureConnect/priority queuing/Compression/AppSecure/Transform/Filter/Authorization/Rewrite/Responder/Cache/Syslog/Nslog/TMTraffic policy that needs to be bound to the specified load balancing virtual server for SureConnect or priority queuing to be activated on a load balancing virtual server.

View description(s) in command reference Top

Setting Global Compression Parameters

You can customize the way the NetScaler appliance compresses data.

To set global compression parameters by using the command line interface

At the command prompt, type:

set cmp parameter [-cmpLevel <compressionLevel>] [-quantumSize <integer>] [-serverCmp (ON | OFF)] [-minResSize <positiveInteger>] [-cmpBypassPct <positiveInteger>] [-cmpOnPush (ENABLED | DISABLED)] [-policyType (CLASSIC | ADVANCED)]

To set global compression parameters by using the configuration utility

1. In the navigation pane, click HTTP Compression.
2. In the details pane, click Change compression settings.
3. In the Configure Compression Parameters dialog box, configure the settings (for example, set the Quantum size and Compression level), and then click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set cmp parameter

cmpLevel

Compression level. Possible values: optimal, bestspeed, bestcompression Default value: NSCMPLVL_OPTIMAL

quantumSize

Minimum amount of data to compress as one unit. Default value: 57344 Minimum value: 8 Maximum value: 63488

serverCmp

Compression at back-end server. Possible values: ON, OFF Default value: ON

minResSize

Size of the smallest HTTP response that will be compressed.

cmpBypassPct

CPU usage (%) at which NetScaler should start progressively bypassing compression on HTTP requests. Default value: 100 Maximum value: 100

cmpOnPush

Enable/disable compression on PUSH packet Possible values: ENABLED, DISABLED Default value: DISABLED

policyType

The type of the HTTP compression global policy bindings to be used for virtual servers that have no HTTP compression policies bound. Possible values: CLASSIC, ADVANCED Default value: NS_EXPR_TYPE_CLASSIC

View description(s) in command reference Top

Configuring Compression for a Load Balancing Virtual Server

When you configure virtual server-based compression, you bind services and compression policies to a virtual server. This causes traffic that flows through a virtual server to and from the bound services to be subject to compression policies that you bind to the vserver.

When a client request flows through a vserver, compression policies identify whether the client can accept compressed data. The Citrix NetScaler appliance forwards the request to the destination server, as identified by a service that is bound to the load balancing vserver. After the NetScaler appliance receives the response from the server, it determines whether the response is compressible based on the compression policies that are bound to the virtual server. If the content is compressible, it is compressed and forwarded to the client.

Task overview: configuring compression for a load balancing vserver.

1. Enable compression and load balancing, as described in "Enabling and Disabling Compression."
2. Add a vserver, as explained in Creating a Virtual Server" and Configuring an SSL-Based Virtual Server".
3. Add one or more HTTP or SSL services and bind the services to a vserver, as explained in "Creating a Service" and "Binding Services to the Virtual Server."
4. Create compression policies, as described in "Configuring Compression Policies."
5. Bind the compression policies to the vserver, as described in "Binding Compression Policies to Virtual Servers."

Viewing Compression Statistics by Using the Dashboard

The Dashboard utility displays summary and detailed compression statistics in tabular and graphic format.

Note: For more information about the statistics and charts, see the Dashboard help on the Citrix NetScaler appliance.

To view compression statistics by using the Dashboard

1. In the Dashboard utility, in the Select Group list, choose Compression, and then do one or more of the following:
   - To view of summary of compression statistics, click the Summary tab.
   - To view compression statistics by protocol type, click the Details tab.
   - To view the rate of requests processed by the compression feature, click the Chart tab.

Viewing Compression Statistics by Using SNMP

You can collect compression statistics in an SNMP monitor. You can view the following compression statistics by using the SNMP network management application.

Note: For more information about SNMP, see "SNMP."

- Number of compression requests (OID: 1.3.6.1.4.1.5951.4.1.1.50.1)
- Number of compressed bytes transmitted (OID: 1.3.6.1.4.1.5951.4.1.1.50.2)
- Number of compressible bytes received (OID: 1.3.6.1.4.1.5951.4.1.1.50.3)
- Number of compressible packets transmitted (OID: 1.3.6.1.4.1.5951.4.1.1.50.4)
- Number of compressible packets received (OID: 1.3.6.1.4.1.5951.4.1.1.50.5)
- Ratio of compressible data received and compressed data transmitted (OID: 1.3.6.1.4.1.5951.4.1.1.50.6)
- Ratio of total data received to total data transmitted (OID: 1.3.6.1.4.1.5951.4.1.1.50.7)

Viewing Additional Compression Statistics

When the NetScaler appliance compresses a response based on a policy, the policy hit counter is incremented. You can view statistics for a compression policy, including the number of hits.

Note: The stat cmp policy command displays statistics only for advanced compression policies.

To view details and hits to a compression policy by using the command line interface

At the command prompt, type:

show cmp policy <name>

To view a summary of compression statistics by using the command line interface

At the command prompt, type:

stat cmp

To view detailed compression statistics by using the command line interface

At the command prompt, type:

stat cmp -detail

To view compression statistics by using the configuration utility

1. In the navigation pane, click HTTP Compression.
2. In the details pane, click the Statistics link.

   Note: To view statistics for an individual policy, expand HTTP Compression, and then click Policies. In the details pane, click the policy for which you want to view statistics.

To view statistics of a compression policy by using the command line interface

At the command prompt, type:

stat cmp policy<name>

Note: Statistics is displayed only for advanced policies.

The output includes the number of hits, rate of hits per second, the number of undefined hits, and the rate of undefined hits on the policy.

To view statistics of a compression policy by using the configuration utility

1. In the navigation pane, expand HTTP Compression, and then click Policies.
2. In the details pane, click Statistics.
3. On the Compression Policy Statistics page, view the statistics of the listed advanced compression policies, or select an advanced policy and click Statistics to display detailed statistics for that policy.

To view statistics of a compression policy label by using the command line interface

At the command prompt, type:

stat cmp policylabel <labelName>

The output of the stat cmp policylabel command includes the number of hits and the rate of hits on the policy label, and the statistics of the policies bound to the policy label.

To view statistics of a compression policy label by using the configuration utility

1. In the navigation pane, expand HTTP Compression, and then click Policy Labels.
2. In the details pane, click Statistics.
3. On the Compression Policy label Statistics page, view the statistics of the listed compression policy labels, or select a policy label and click Statistics to display detailed statistics for that policy label.

Parameter Descriptions (of commands listed in the CLI procedure)

show cmp policy

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

stat cmp

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

stat cmp policy

name

The name of the compress policy for which statistics will be displayed. If not given statistics are shown for all compress policies.

View description(s) in command reference Top

stat cmp policylabel

labelName

The name of the compress policy label for which statistics will be displayed. If not given statistics are shown for all compress policylabels.

View description(s) in command reference Top

Integrated Caching

The integrated cache provides in-memory storage on the Citrix NetScaler appliance and serves Web content to users without requiring a round trip to an origin server. For static content, the integrated cache requires little initial setup. After you enable the integrated cache feature and perform basic setup (for example, determining the amount of NetScaler appliance memory the cache is permitted to use), the integrated cache uses built-in policies to store and serve specific types of static content, including simple Web pages and image files. You can also configure the integrated cache to store and serve dynamic content that is usually marked as non-cacheable by Web and application servers (for example, database records and stock quotes).

When a request or response matches the rule (logical expression) specified in a built-in policy or a policy that you have created, the NetScaler appliance performs the action associated with the policy. By default, all policies store cached objects in and retrieve them from the Default content group, but you can create your own content groups for different types of content.

To enable the NetScaler appliance to find cached objects in a content group, you can configure selectors, which match cached objects against expressions, or you can specify parameters for finding objects in the content group. If you use selectors (which Citrix recommends), configure them first, so that you can specify selectors when you configure content groups. Next, set up any content groups that you want to add, so that they are available when you configure the policies. To complete the initial configuration, create policy banks by binding each policy to a global bind point or a virtual server, or to a label that can be called from other policy banks.

You can tune the performance of the integrated cache, using methods such as pre-loading cached objects before they are scheduled to expire. To manage the handling of cached data once it leaves the NetScaler appliance, you can configure caching-related headers that are inserted into responses. The integrated cache can also act as a forward proxy for other cache servers.

Note: Integrated caching requires some familiarity with HTTP requests and responses. For information about the structure of HTTP data, see *Live HTTP Headers* at "http://livehttpheaders.mozdev.org/."

How the Integrated Cache Works

The integrated cache monitors HTTP and SQL requests that flow through the Citrix NetScaler appliance and compares the requests with stored policies. Depending on the outcome, the integrated cache feature either searches the cache for the response or forwards the request to the origin server. For HTTP requests, the integrated cache feature can also serve partial content from the cache in response to single byte-range and multi-part byte-range requests.

Cached data can be compressed if the client accepts compressed content. You can configure expiration times for a content group, and you can selectively expire entries in a content group.

Data that is served from the integrated cache is a cache hit, and data served from the origin is a cache miss, as described in the following table.

Table 1. Cache Hits and Misses

Transaction Type	Specifies

Cache Hit	Responses that the NetScaler appliance serves from the cache, including: · Static objects, for example, image files and static Web pages · 200 OK pages · 203 Non-Authoritative Response pages · 300 Multiple Choices pages · 301 Moved Permanently pages · 302 Found pages · 304 Not Modified pages These responses are known as positive responses. The NetScaler appliance also caches the following negative responses: · 307 Temporary Redirect pages · 403 Forbidden pages · 404 Not Found pages · 410 Gone pages To further improve performance, you can configure the NetScaler appliance to cache additional types of content.
Storable Cache Miss	For a storable cache miss, the NetScaler appliance fetches the response from the origin server, and stores the response in the cache before serving it to the client.
Non-Storable Cache Miss	A non-storable cache miss is inappropriate for caching. By default, any response that contains the following status codes is a non-storable cache miss: · 201, 202, 204, 205, 206 status codes · All 4xx codes, except 403, 404 and 410 · 5xx status codes

Note: To integrate dynamic caching with your application infrastructure, use the XML API to issue cache commands remotely. For example, you can configure triggers that expire cached responses when a database table is updated.

To ensure the synchronization of cached responses with the data on the origin server, you configure expiration methods. When the NetScaler appliance receives a request that matches an expired response, it refreshes the response from the origin server.

Example of Dynamic Caching

Dynamic caching evaluates HTTP requests and responses based on parameter-value pairs, strings, string patterns, or other data. For example, suppose that a user searches for Bug 31231 in a bug reporting application. The browser sends the following request on the user's behalf:

```
GET /mybugreportingsystem/mybugreport.dll?IssuePage&RecordId=31231&Template=view&TableId=1000
Host: mycompany.net
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9) Gecko/2008052906 Firefox/3.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
. . .
```

In this example, GET requests for this bug reporting application always contain the following parameters:

- IssuePage
- RecordID
- Template
- TableId

GET requests do not update or alter the data, so you can configure these parameters in caching policies and selectors, as follows:

- You configure a caching policy that looks for the string mybugreportingsystem and the GET method in HTTP requests. This policy directs matching requests to a content group for bugs.
- In the content group for bugs, you configure a hit selector that matches various parameter-value pairs, including IssuePage, RecordID, and so on.

Note that a browser can send multiple GET requests based on one user action. The following is a series of three separate GET requests that a browser issues when a user searches for a bug based on a bug ID. **Bold** has been added for emphasis:

```
GET /mybugreportingsystem/mybugreport.dll?IssuePage&RecordId=31231&Template=view&TableId=1000
GET /mybugreportingsystem/mybugreport.dll?IssuePage&Template=viewbtns&RecordId=31231&TableId=1000
GET /mybugreportingsystem/mybugreport.dll?IssuePage&Template=viewbody&RecordId=31231&tableid=1000
```

To fulfill these requests, multiple responses are sent to the user's browser, and the Web page that the user sees is an assembly of the responses.

If a user updates a bug report, the corresponding responses in the cache should be refreshed with data from the origin server. The bug reporting application issues HTTP POST requests when a user updates a bug report. In this example, you configure the following to ensure that POST requests trigger invalidation in the cache:

- A request-time invalidation policy that looks for the string mybugreportingsystem and the POST HTTP request method, and directs matching requests to the content group for bug reports.
- An invalidation selector for the content group for bug reports that expires cached content based on the RecordID parameter. This parameter appears in all of the responses, so the invalidation selector can expire all relevant items in the cache.

The following excerpt shows a POST request that updates the sample bug report. **Bold** has been added for emphasis:

POST /mybugreportingsystem/mybugreport.dll?TransitionForm HTTP/1.1\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0) Opera 7.23 [en]\r\n
Host: mybugreportingsystem\r\n
Cookie:ttSearch.134=%23options%3Afalse%23active%23owner%3Afalse%23unowned%3Afalse%23submitter%3Afa
Cookie2: $Version=1\r\n
. . .
\r\n
ProjectId=2&RecordId=31231&TableId=1000&TransitionId=1&Action=Update&CopyProjectId=0&ReloadForm=0

When the Citrix NetScaler appliance receives this request, it does the following:

- Matches the request with an invalidation policy.
- Finds the content group that is named in the policy.
- Applies the invalidation selector for this content group and expires all responses that match RecordID=31231.

When a user issues a new request for this bug report, the NetScaler appliance goes to the origin server for updated copies of all the responses that are associated with the report instance, stores the responses in the content group, and serves them to the user's browser, which reassembles the report and displays it.

Setting Up the Integrated Cache

To use the integrated cache, you must install the license and enable the feature. After you enable the integrated cache, the Citrix® NetScaler® appliance automatically caches static objects as specified by built-in policies and generates statistics on cache behavior. (Built-in policies have an underscore in the initial position of the policy name.)

Even if the built-in policies are adequate for your situation, you might want to modify the global attributes. For example, you might want to modify the amount of NetScaler appliance memory allocated to the integrated cache.

If you would like to observe cache operation before changing settings, see "Displaying Cached Objects and Cache Statistics."

Note: The NetScaler cache is an in-memory store that is purged when you restart the appliance.

Installing the Integrated Cache License

An integrated cache license is required. For information about licenses, see information about obtaining NetScaler licenses at "http://support.citrix.com/article/ctx121062."

To install the license for the Integrated Caching feature

1. Obtain a license code from Citrix, go to the command line interface, and log in.
2. At the command line interface, copy the license file to the /nsconfig/license folder.
3. Reboot the NetScaler appliance by using the following command:

   reboot

Parameter Descriptions (of commands listed in the CLI procedure)

reboot

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Enabling or Disabling Integrated Cache

When you enable integrated caching, the NetScaler appliance begins caching server responses. If you have not configured any policies or content groups, the built in policies store cached objects in the Default content group.

To enable or disable integrated caching by using the command line interface

At the command prompt, type one of the following commands to enable or disable integrated caching:

- enable ns feature `IC`
- disable ns feature `IC`

To enable or disable integrated caching by using the configuration utility

1. Navigate to System > Settings.
2. In the details pane, under the Modes and Features group, click Configure basic features.
3. In the Configure Basic Features dialog box, select the Integrated Caching check box to enable integrated caching, or clear the check box to disable it.
4. In the confirmation message box, click OK, and then click Yes.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Global Attributes for Caching

Global attributes apply to all cached data. You can specify the amount of NetScaler memory allocated to the integrated cache, Via header insertion, a criterion for verifying that a cached object should be served, the maximum length of a POST body permitted in the cache, whether to bypass policy evaluation for HTTP GET requests, and an action to take when a policy cannot be evaluated.

The cache memory capacity is limited only by the memory of the hardware appliance. Also, any packet engine (the central distribution hub of all incoming TCP requests) in the nCore NetScaler appliance is aware of objects cached by other packet engines in the nCore NetScaler appliance.

Note that the default global memory limit is 0. Therefore, even if Integrated Caching is enabled, the NetScaler appliance does not cache any objects. You must explicitly set the global memory limit when integrated caching is enabled.

You can modify the global memory limit configured for caching objects. However, when you update the global memory limit to a value lower than the existing value (for example, from 10 GB to 4 GB), if a higher amount of memory (greater than 4 GB) is already being used to cache objects, the NetScaler continues using that amount of memory.

This means that even though the integrated caching limit is configured to some value, the actual limit used can be higher. This excessive memory is however released when the objects are removed from cache.

The output of the show cache parameter command indicates the configured value (Memory Usage limit) and the actual value being used (Memory usage limit (active value)).

To configure global settings for caching by using the command line interface

At the command prompt, type:

set cache parameter [-memLimit <MBytes>] [-via <string>] [-verifyUsing <criterion>] [-maxPostLen <positiveInteger>] [-prefetchMaxPending <positiveInteger>] [-enableBypass (YES|NO)] [-undefAction (NOCACHE|RESET)]

To configure global settings for caching by using the configuration utility

1. In the navigation pane, click Integrated Caching.
2. In the details pane, click Change cache settings.
3. In the Cache Global Settings dialog box, configure the global settings for caching. For a description of a parameter, hover the mouse cursor over the corresponding field.
4. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set cache parameter

memLimit

The memory limit for Integrated Cache.

via

The string to be inserted in the "Via" header. A Via header is inserted in all responses served from a content group if its insertVia flag is set.

verifyUsing

The criteria for deciding whether a cached object can be served for an incoming HTTP request. a. If the value of this attribute is set to HOSTNAME, then URL , host name and host port values in the incoming HTTP request header must match before a cached object can be served. The IP address and the TCP port of the destination host are not matched. For certain deployments the HOSTNAME setting can be a security risk. A rogue client can access a rogue server via the Integrated Cache using the following HTTP request : GET / HTTP/1.1 Host: sensitive.foo.com Integrated Cache will store the rogue page served by the rogue server. Any subsequent client trying to access the root page from sensitive.foo.com will be served the rogue page. The HOSTNAME setting should only be set if it is certain that no rogue client can access a rogue server via the Integrated Cache. The YES setting can lead to more hits if DNS-based load balancing is in use and the same content can be served by multiple backend servers. b. If the attribute is set to HOSTNAME_AND_IP, then the following items must match: URL, host name, host port in the incoming HTTP request header, and the IP address and TCP port of the destination server. c. If the attribute is set to DNS, then the following items should match: URL, host name and host port in the incoming HTTP request, and the TCP port. The hostname is used to do a DNS lookup of the destination server's IP address, and is compared with the set of addresses returned by the DNS lookup. The default value of this attribute is DNS. Possible values: HOSTNAME, HOSTNAME_AND_IP, DNS

maxPostLen

maximum number of POST body bytes to consider when evaluating parameters for a content group for which you have configured hitParams and invalParams. Default value: 4096 Maximum value: 131072

prefetchMaxPending

The maximum number of outstanding prefetches in the IC.

enableBypass

The bypass parameter. When this value is set to NO, an incoming request will serve a hit if a matching object is found in cache storage, regardless of the cacheability policy configuration. If set to YES, the bound request cacheability policies are evaluated before attempting any hit selection in the cache storage. If the request matches a policy with a NOCACHE action, the request will bypass all cache processing. This flag does not affect processing of requests that match any invalidation policy. Possible values: YES, NO

undefAction

Set the default cache undef action. If an UNDEF event is triggered during policy evaluation and if the current policy's undefAction is not specified, then this global undefAction value is used. Can be NOCACHE or RESET. NOCACHE is the default value of default cache undef action. Possible values: NOCACHE, RESET

View description(s) in command reference Top

Built-in Content Group, Pattern Set, and Policies for the Integrated Cache

The Citrix NetScaler appliance includes a built-in integrated caching configuration that you can use for caching content. The configuration consists of a content group called `ctx_cg_poc`, a pattern set called `ctx_file_extensions`, and a set of integrated cache policies. In the content group `ctx_cg_poc`, only objects that are 500 KB or smaller are cached. The content is cached for 86000 seconds, and the memory limit for the content group is 512 MB. The pattern set is an indexed array of common file extensions for file-type matching.

The following table lists the built-in integrated caching policies. By default, the policies are not bound to any bind point. You must bind them to a bind point if you want the NetScaler appliance to evaluate traffic against the policies. The policies cache objects in the `ctx_cg_poc` content group.

Table 1. Built-in Integrated Caching Policies

me	Policy rule
	`HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS_INDEX(\"ctx_file_extensions\").BETWEEN(101,150)`
	`HTTP.REQ.URL.ENDSWITH(\".css\")`
	`HTTP.REQ.URL.ENDSWITH(\".pdf\")`
	`HTTP.REQ.URL.ENDSWITH(\".js\")`
s	`HTTP.RES.HEADER(\"Content-Type\").CONTAINS(\"application/x-javascript\")`
	`TRUE`

Configuring Selectors and Basic Content Groups

You can configure selectors and apply them to content groups. When you add a selector to one or more content groups, you specify whether the selector is to be used for identifying cache hits or identifying cached objects to be invalidated (expired). Selectors are optional. Alternatively, you can configure content groups to use hit parameters and invalidation parameters. However, Citrix recommends that you configure selectors.

After configuring selectors, or deciding to use parameters instead, you are ready to set up a basic content group. After creating the basic content group, you need to decide how objects should be expired from the cache, and configure cache expiration. You can further modify the cache as described in "Improving Cache Performance" and "Configuring Cookies, Headers, and Polling", but you might first want to configure caching policies.

Note: Content group parameters and selectors are used only at request time, and you typically associate them with policies that use MAY_CACHE or MAY_NOCACHE actions.

Advantages of Selectors

A selector is a filter that locates particular objects in a content group. If you do not configure a selector, the Citrix® NetScaler® appliance looks for an exact match in the content group. This can lead to multiple copies of the same object residing in a content group. For example, a content group that does not have a selector may need to store URLs for host1.domain.com\mypage.htm, host2.domain.com\mypage.htm, and host3.domain.com\mypage.htm. In contrast, a selector can match just the URL (mypage.html, using the expression http.req.url) and the domain (.com, using the expression http.req.hostname.domain), allowing the requests to be satisfied by the same URL.

Selector expressions can perform simple matching of parameters (for example, to find objects that match a few query string parameters and their values). A selector expression can use Boolean logic, arithmetic operations, and combinations of attributes to identify objects (for example, segments of a URL stem, a query string, a string in a POST request body, a string in an HTTP header, a cookie). Selectors can also perform programmatic functions to analyze information in a request. For example, a selector can extract text in a POST body, convert the text into a list, and extract a specific item from the list.

For more information about expressions and what you can specify in an expression, see "Policies and Expressions."

Using Parameters Instead of Selectors

Although Citrix recommends the use of selectors with a content group, you can instead configure hit parameters and invalidation parameters. For example, suppose that you configure three hit parameters in a content group for bug reports: BugID, Issuer, and Assignee. If a request contains BugID=456, with Issuer=RohitV and Assignee=Robert, the NetScaler appliance can serve responses that match these parameter-value pairs.

Invalidation parameters in a content group expire cached entries. For example, suppose that BugID is ab invalidation parameter and a user issues a POST request to update a bug report. An invalidation policy directs the request to this content group, and the invalidation parameter for the content group expires all cached responses that match the BugID value. (The next time a user issues a GET request for this report, a caching policy can enable the NetScaler appliance to refresh the cached entry for the report from the origin server.)

Note that the same parameter can be used as a hit parameter or an invalidation parameter.

Content groups extract request parameters in the following order:

- URL query
- POST body
- Cookie header

After the first occurrence of a parameter, regardless of where it occurred in the request, all its subsequent occurrences are ignored. For example, if a parameter exists both in the URL query and in the POST body, only the one in the URL query is considered.

If you decide to use hit and invalidation parameters for a content group, configure the parameters when you configure the content group.

Note: Citrix recommends that you use selectors rather than parameterized content groups, because selectors are more flexible and can be adapted to more types of data.

Configuring a Selector

A content group can use a hit selector to retrieve cache hits or use an invalidation selector to expired cached objects and fetch new ones from the origin server.

A selector contains a name and a logical expression, called an *advanced expression*.

For more information about advanced expressions, see "Policies and Expressions."

To configure a selector, you assign it a name and enter one or more expressions. As a best practice, a selector expression should include the URL stem and host, unless there is a strong reason to omit them.

To configure a selector by using the command line interface

At the command prompt, type:

add cache selector <selectorName> (<rule> ...)

For information about configuring the expression or expressions, see "To configure a selector expression by using the command line interface."

Examples

```
>add cache selector product_selector "http.req.url.query.value(\"ProductId\")" "http.req.url.query.value(\"Ba
> add cache selector batch_selector "http.req.url.query.value(\"ProductId\")" "http.req.url.query.value(\"Bat
> add cache selector product_id_selector "http.req.url.query.value(\"ProductId\")"
> add cache selector batchnum_selector "http.req.url.query.value(\"BatchNum\")" "http.req.url.query.value(
> add cache selector batchid_selector "http.req.url.query.value(\"depotLocation\")" "http.req.url.query.value
```

To configure a selector by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Cache Selectors.
2. In the details pane, click Add.
3. In the Create Cache Selector dialog box, in the Name text box, type the name of the selector (for example, myDatabase_hitSelector).
4. In the Expressions box, enter the expression that you want to use for matching items in the cache (as described in “To configure a policy or selector expression by using the configuration utility”).
5. Click Create, and then click Close.

Parameter Descriptions (of commands listed in the CLI procedure)

add cache selector

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

About Content Groups

A content group is a container for cached objects that can be served in a response. When you first enable the integrated cache, cacheable objects are stored in a content group named Default. You can create new content groups that have unique properties. For example, you can define separate content groups for image data, bug reports, and stock quotes, and you can configure the stock quote content group to be refreshed more often than the other groups.

You can configure expiration of an entire content group or selected entries in a content group.

The data in a content group can be static or dynamic, as follows:

- **Static content groups**. Finds an exact match between the URL stem and host name on the request and the URL stem and host name of the response.
- **Dynamic content groups**. Looks for objects that contains particular parameter-value pairs, arbitrary strings, or string patterns. Dynamic content groups are useful when caching data that is updated frequently (for example, a bug report or a stock quote).

Process overview: Serving a hit from a content group

1. A user enters search criteria for an item, such as a bug report, and clicks the Find button in an HTML form.
2. The browser issues one or more HTTP GET requests. These requests contain parameters (for example, the bug owner, bug ID, and so on).
3. When the NetScaler appliance receives the requests, it searches for a matching policy, and if it finds a caching policy that matches these requests, it directs the requests to a content group.
4. The content group looks for appropriate objects in the content group, usually based on criteria that you configure in a selector.

   For example, the content group can retrieve responses that match NameField=username and BugID=ID.
5. If it finds matching objects, the NetScaler appliance can serve them to the user's browser, where they are assembled into a complete response (for example, a bug report).

Example: Invalidating an object in a content group

1. A user modifies data (for example, the user modifies the bug report and clicks the Submit button).

2. The browser sends this data in the form of one or more HTTP requests. For example, it can send a bug report in the form of several HTTP POST requests that contain information about the bug owner and bug ID.

3. The NetScaler appliance matches the requests against invalidation policies. Typically, these policies are configured to detect the HTTP POST method.

4. If the request matches an invalidation policy, the NetScaler appliance searches the content group that is associated with this policy, and expires responses that match the configured criteria for invalidation.

   For example, an invalidation selector can find responses that match NameField=username and BugID=ID.

5. The next time the NetScaler appliance receives a GET request for these responses, it fetches refreshed versions from the origin server, caches the refreshed responses, and serves these responses to the user's browser, where they are assembled into a complete bug report.

Setting Up a Basic Content Group

By default, all cached data is stored in the default content group. You can configure additional content groups and specify these content groups in one or more policies.

You can configure content groups for static content, and you must configure content groups for dynamic content. You can modify the configuration of any content group, including the default group.

To set up a basic content group by using the command line interface

At the command prompt, type:

add cache contentgroup <name> (-hitSelector <hitSelectorName> -invalSelector <invalidationSelectorName> | -hitParams <hitParamName> -invalParams <invalidationParamName>) -type <type> [-relExpiry <sec> | -relExpiryMilliSec <msec>] [-heurExpiryParam <positiveInteger>]

Examples

> add cache contentgroup Products_Details –hitSelector product_selector –invalSelector id_selector
> add cache contentgroup bugrep -hitParams IssuePage RecordID Template TableId -invalParams RecordID -r

To set up a basic content group by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Content Groups.
2. In the details pane, do one of the following:
   - To create a new content group, click Add.
   - To modify an existing content group, select the content group, and then click Open.
3. In the Create Cache Content Group or the Configure Cache Content Group dialog box, set the relevant parameters in Expiry Method and Parameterization tabs.
4. Click Create or OK.

Parameter Descriptions (of commands listed in the CLI procedure)

add cache contentgroup

name

The name of the content group to be created

hitSelector

The selector used for hit selection.

invalSelector

The selector used for invalidation.

hitParams

Use these parameters for parameterized hit evaluation of an object. Up to 128 parameters can be configured.

invalParams

Use these parameters for parameterized invalidation of an object. Up to 8 parameters can be configured.

relExpiry

The relative expiry time in seconds Default value: VAL_NOT_SET Maximum value: 31536000

relExpiryMilliSec

The relative expiry time in milliseconds. Default value: VAL_NOT_SET Maximum value: 86400000

heurExpiryParam

The heuristic expiry time, in percent of the duration since the object was last modified Default value: VAL_NOT_SET Maximum value: 100

View description(s) in command reference Top

Expiring or Flushing Cached Objects

If a response does not have an Expires header or a Cache-Control header with an expiration time (Max-Age or Smax-Age), you must expire objects in a content group by using one of the following methods:

- Configure content group expiration settings to determine whether and how long to keep the object.
- Configure an invalidation policy and action for the content group. For more information, see "Configuring Policies for Caching and Invalidation."
- Expire the content group or objects within it manually.

After a cached response expires, the NetScaler appliance refreshes it the next time the client issues a request for the response. By default, when the cache is full, the NetScaler appliance replaces the least recently used response first.

The following list describes methods for expiring cached responses using settings for a content group. Typically, these methods are specified as a percent or in seconds:

- **Manual**. Manually invalidate all responses in a content group or all responses in the cache.
- **Response-based**. Specific expiration intervals for positive and negative responses. Response-based expiry is considered only if the Last-Modified header is missing in the response.
- **Heuristic expiry**. For responses that have a Last-Modified header, heuristic expiry is a percentage of the time since the response was modified (calculated as current time minus the Last-Modified time, multiplied by the heuristic expiry value). For example, if a Last-Modified header indicates that a response was updated 2 hours ago, and the heuristic expiry setting is 10%, cached objects expire after 0.2 hours. This method assumes that frequently updated responses need to be expired more often.
- **Absolute or relative**. Specify an exact (absolute) time when the response expires every day, in HH:MM format, local time or GMT. Local time may not work in all time zones.

  Relative expiration specifies a number of seconds or milliseconds from the time a cache miss causes a trip to the origin server to the expiration of the response. If you specify relative expiration in milliseconds, enter a multiple of 10. This form of expiration works for all positive responses. Last-Modified, Expires, and Cache-Control headers in the response are ignored.

  Absolute and relative expiration override any expiration information in the response itself.
- **On download**. The option Expire After Complete Response Received expires a response as soon as it is downloaded. This is useful for frequently updated responses, for example, stock quotes. By default, this option is disabled.

Enabling both Flash Cache and Expire After Complete Response Received accelerates the performance of dynamic applications. When you enable both options, the NetScaler appliance fetches only one response for a block of simultaneous requests.

For more information, see "Queuing Requests to the Cache."

- **Pinned**. By default, when the cache is full the NetScaler appliance replaces the least recently used response first. The NetScaler appliance does not apply this behavior to content groups that are marked as pinned.

If you do not configure expiration settings for a content group, the following are additional options for expiring objects in the group:

- Configure a policy with an INVAL action that applies to the content group.
- Enter the names of content groups when configuring a policy that uses an INVAL action.

How Expiration Methods Are Applied

Expiration works differently for positive and negative responses. Positive and negative responses are described in the table, *Expiration of Positive and Negative Responses* mentioned below.

The following are rules of thumb for understanding the expiration method that is applied to a content group:

- You can control whether the NetScaler appliance evaluates response headers when deciding whether to expire an object.
- Absolute and relative expiration cause the NetScaler appliance to ignore the response headers (they override any expiration information in the response).
- Heuristic expiration settings and “Weak Positive” and “Weak Negative” expiration (labeled as **Default** values in the configuration utility) cause the NetScaler appliance to examine the response headers. These settings work together as follows:
  - The value in an Expires or Cache-Control header overrides these content group settings.
  - For positive responses that lack an Expires or Cache-Control header but have a Last-Modified header, the NetScaler appliance compares heuristic expiration settings with the header value.
  - For positive responses that lack an Expires, Cache-Control, or Last-Modified header, NetScaler appliance uses the “weak positive” value.
  - For negative responses that lack an Expires or Cache-Control header, NetScaler appliance uses the “weak negative” value.

For a list of expiration parameters see, "Configuring Periodic Expiration of a Content Group." The following table describes how these methods are applied.

Table 1. Expiration of Positive and Negative Responses

Response Type	Expiration Header Type	Content Group Setting	Period the Object Remains in the Cache
Positive	any header	Expire Content After (relExpiry) with no other settings	Use the value of the Expire Content After setting.
Positive	any header	Expire Content At (absExpiry) with no other settings	Subtract current date from the value of the Expire Content At setting.
Positive	any header	Expire Content After (relExpiry) and Expire content at (absExpiry)	Use the smaller of the two values for the content group settings. See the previous rows in this table.
Positive	Last-Modified (with any other headers)	Heuristic (heurExpiry Param) with any other setting	Subtract the Last-Modified date from the current date, multiply the result by the value of the heuristic expiry setting, and then divide by 100.
Positive	Last-Modified (with any other headers)	Default (positive) (weakPosRel Expiry) and no other setting	Use the value of the Default (positive) expiry setting.
Positive	Expires or Cache-Control: Max-Age header is present Last-Modified header is absent	Heuristic (heurExpiry Param), Default (positive) (weakPosRel Expiry), or both	Subtract the current date from the Expires or the Cache-Control:Max-Age date.
Positive	no caching headers	Default (positive) (weakPosRel Expiry) and any other expiration setting.	Use the value of the Default (positive) setting.

Positive	no caching headers	Heuristic (heurExpiry Param) is present Default (positive) (weakPosRel Expiry) setting is absent	If the Last-Modified header is absent, the response is not cached or it is cached with an Already Expired status. If the Last-Modified header is present, use the heuristic expiry value.
Negative	Expires or Cache-Control:Max-Age	Expire Content After (relExpiry), Expire Content At (absExpiry), or both settings	Subtract the current date from the value of the Expires header, or use the value of the Cache-Control:Max-Age header.
Negative	Expires or Cache-Control headers are absent	Expire Content After (relExpiry), Expire Content At (absExpiry), or both settings	Response is not cached, or is cached with an Already Expired status.
Negative	Expires or Cache-Control:Max-Age	Any setting	Subtract the current date from the Expires or Cache-Control:Max-Age date.
Negative	Expires and Cache-Control:Max-Age headers are absent	Default (negative) (weakNegRel Expiry)	Use the value of the Default (negative) setting.
Negative	Expires and Cache-Control:Max-Age headers are absent	Any setting other than Default (negative) (weakNegRel Expiry)	Object is not cached or is cached with an Already Expired status.

Expiring a Content Group Manually

You can manually expire all of the entries in a content group.

To manually expire all responses in a content group by using the command line interface

At the command prompt, type:

expire cache contentGroup <name>

To manually expire all responses in a content group by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Content Groups.
2. In the details pane, click the content group that you want to invalidate, and click Invalidate.
3. In the Invalidate Selected Cache Content Group dialog box, click Expire, and then click OK.

To manually expire all responses in the cache by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Content Groups.
2. In the details pane, click Invalidate All.
3. In the Invalidate All Content Groups dialog box, click Expire All, and then click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

expire cache contentGroup

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Periodic Expiration of a Content Group

You can configure a content group so that it performs selective or full expiration of its entries. The expiration interval can be fixed or relative.

To configure content group expiration by using the command line interface

At the command prompt, type:

set cache contentgroup <name> (-relExpiry|-relExpiryMilliSec|-absExpiry|-absExpiryGMT|-heurExpiryParam|-weakPosRelExpiry|-weakNegRelExpiry| -expireAtLastBye) <expirationValue>

To configure content group expiration by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Content Groups.
2. In the details pane, click the content group for which you want to set the heuristic expiry parameter, and then click Open.
3. In the Configure Cache Content Group dialog box, on the Expiry Method tab, specify values for the relevant parameters. For a description of a parameter, hover the mouse cursor over the corresponding field.
4. Click Create.

Expiring Individual Responses

Expiring a response forces the NetScaler appliance to fetch a refreshed copy from the origin server. Responses that do not have validators, for example, ETag or Last-Modified headers, cannot be revalidated. As a result, flushing these responses has the same effect as expiring them.

To expire a cached response in a content group for static data, you can specify a URL that must match the stored URL. If the cached response is part of a parameterized content group, you must specify the group name as well as the exact URL stem. The host name and the port number must be the same as in the host HTTP request header of the cached response. If the port is not specified, port 80 is assumed.

To expire individual responses in a content group by using the command line interface

At the command prompt, type:

expire cache object -url <URL> -host <hostName> [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET|POST]

To expire individual responses in a content group by using the command line interface (selector-based)

At the command prompt, type the following command:

expire cache object -locator <positiveInteger>

To expire a cached response by using the configuration utility

1. View the cached response. For more information, see "Displaying Cached Objects and Cache Statistics."
2. Click the response you want to expire.
3. Click Expire.

To expire a response by using the Lookup tool (selector-based)

1. Find the response that you want to expire. For more information, see "Finding Particular Cached Responses."
2. Click Expire.

Flushing Responses in a Content Group

You can remove, or flush, all responses in a content group, some responses in a group, or all responses in the cache. Flushing a cached response frees up memory for new cached responses.

Note: To flush responses for more than one object at a time, use the configuration utility method. The command line interface does not offer this option.

To flush responses from a content group by using the command line interface

At the command prompt, type:

flush cache contentGroup <name> [-query <queryString> | [-selectorValue <selectorExpressionIDList> -host <hostName>]]

To flush responses from a content group by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Content Groups.
2. In details pane, flush the responses as follows:
   - To flush all responses in all content groups, click Invalidate All. In the Invalidate All Content Groups, click Flush All.
   - To flush responses in a particular content group, select the content group that you want to invalidate, and then click Invalidate. In the Invalidate Selected Cache Content Group dialog box, click Flush.
3. Click OK, and then click Close.

Note: If this content group uses a selector, you can selectively flush responses by entering a string in the Selector value text box, entering a host name in the Host text box. Then click Flush and OK. The Selector value can be a query string of up to 2319 characters that is used for parameterized invalidation.

If the content group uses an invalidation parameter, you can selectively flush responses by entering a string in the Query field.

If the content group uses an invalidation parameter and Invalidate objects belonging to target host is configured, enter strings in the Query and Host fields.

To flush a cached response by using the command line interface

At the command prompt, type:

flush cache object -locator <positiveInteger> | -url <URL> -host <hostName> [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET|POST]

To flush a cached response by using the configuration utility

1. Find the cached response. For more information, see "Configuring Global Attributes for Caching."
2. Select the response that you want to expire.
3. Click Flush.

Deleting a Content Group

You can remove a content group if it is not used by any policy that stores responses in the cache. If the content group is bound to a policy, you must first remove the policy. Removing the content group removes all responses stored in that group.

You cannot remove the Default, BASEFILE, or Deltajs group. The Default group stores cached responses that do not belong in any other content group.

To delete a content group by using the command line interface

At the command prompt, type:

rm cache contentgroup<name>

To delete a content group by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and click Content Groups.
2. In the details pane, click the content group name that you want to remove, and click Remove.
3. In the Remove message box, click Yes.

Parameter Descriptions (of commands listed in the CLI procedure)

set cache contentgroup

name

The name of the content group whose attibutes will be changed.

relExpiry

The relative expiry time in seconds. Default value: VAL_NOT_SET Maximum value: 31536000

relExpiryMilliSec

The relative expiry time in milliseconds. Default value: VAL_NOT_SET Maximum value: 86400000

absExpiry

Expiry time for all objects in the content group(up to 4 times a day [local time]).

absExpiryGMT

Expiry time for all objects in the content group(up to 4 times a day [GMT]).

weakPosRelExpiry

Responses with response codes between 200 and 399. (Similar to -relExpiry, but has lesser precedence.) Maximum value: 31536000

weakNegRelExpiry

All negative responses. This value is used only if the expiry time cannot be determined from any other source. Maximum value: 31536000

View description(s) in command reference Top

expire cache object

url

The URL of the object to be expired.

host

The host of the object to be expired.

port

The host port of the object to be expired. Default value: 80 Minimum value: 1

groupName

The name of the content group to be in which the cell is present.

httpMethod

The HTTP request method that caused the object to be stored. Possible values: GET, POST Default value: NS_HTTP_METHOD_GET

locator

The id of the cached object.

View description(s) in command reference Top

flush cache contentGroup

name

The name of the content group whose objects are to be flushed.

query

If a query string is specified, then the selected objects in this group will be flushed using parameterized invalidation. Otherwise, all objects in the group will be flushed.

selectorValue

The value of the selector to be used for flushing objects in the contentgroup.

host

To be set only if parameterized invalidation is being done. Objects belonging only to the specified host will be flushed. The host argument can be provided if and only if -invalRestrictedToHost is set to YES for the given group.

View description(s) in command reference Top

flush cache object

locator

The ID of the cached object.

url

The URL of the object to be flushed.

host

The host of the object to be flushed.

port

The host port of the object to be flushed. Default value: 80 Minimum value: 1

groupName

The name of the content group to be in which the cell is present.

httpMethod

The HTTP request method that caused the object to be stored. Possible values: GET, POST Default value: NS_HTTP_METHOD_GET

View description(s) in command reference Top

rm cache contentgroup

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Policies for Caching and Invalidation

Policies enable the integrated cache to determine whether to try to serve a response from the cache or the origin. The Citrix NetScaler appliance provides built-in policies for integrated caching, and you can configure additional policies. When you configure a policy, you associate it with an action. An action either caches the objects to which the policy applies or invalidates (expires) the objects. Typically, you based caching policies on information in GET and POST requests. You typically base invalidation policies on the presence of the POST method in requests, along with other information. You can use any information in a GET or POST request in a caching or an invalidation policy.

You can view some of the built-in policies in the integrated cache's Policies node in the configuration utility. The built-in policy names begin with an underscore (_).

Actions determine what the NetScaler appliance does when traffic matches a policy. The following actions are available:

- **Caching actions**. Policies that you associate with the CACHE action store responses in the cache and serve them from the cache.
- **Invalidation actions**. Policies that you associate with the INVAL action immediately expire cached responses and refresh them from the origin server. Note that for Web-based applications, invalidation policies often evaluate POST requests.
- **"Do not cache" actions**. Policies that you associate with a NOCACHE action never store objects in the cache.
- **"Provisionally cache" actions**. Policies that you associate with a MAYCACHE or MAYNOCACHE action depend on the outcome of additional policy evaluations.

Although the integrated cache does not store objects specified by the LOCK method, you can invalidate cached objects upon receipt of a LOCK request. For invalidation policies only, you can specify LOCK as a method by using the expression `http.req.method.eq("lock")`. Unlike policies for GET and POST requests, you must enclose the LOCK method in quotes because the NetScaler appliance recognizes this method name as a string only.

After you create a policy, you bind it to a particular point in the overall processing of requests and responses. Although you create a policy before binding it, you should understand how the bind points affect the order of processing before you create your policies.

The policies bound to a particular bind point constitute a policy bank. You can use goto expressions to modify the order of execution in a policy bank. You can also invoke policies in other policy banks. In addition, you can create labels and bind policies to them. Such a label is not associated with a processing point, but the policies bound to it can be invoked from other policy banks.

Actions to Associate with Integrated Caching Policies

The following table describes actions for integrated caching policies.

Table 1. Actions That You Can Associate with an Integrated Caching Policy

Action	Specifies
CACHE	Serves a response from the cache if the response has not expired. If the response must be fetched from the origin server, the NetScaler appliance caches the response before serving it. Even data that is updated and accessed frequently can be cached. For example, stock quotes are updated frequently, but they can be cached so that they can be served quickly to multiple users. If necessary, cached data can be refreshed immediately after it is downloaded. A CACHE action can be overridden by built-in policies.
NOCACHE	Always fetches the response from the origin server and marks the response as non-storable. You typically configure NOCACHE policies for data that is sensitive or personalized.
MAY_CACHE	Used in a request-time policy, this setting provisionally enables a response to be stored in a content group, pending evaluation of response-time policies. The following are possible: · If a matching response-time policy has a CACHE action but does not specify a content group, the response is stored in the Default group unless built-in policies override this policy. · If a matching response-time policy has a CACHE action and specifies the same content group as the one in the request-time policy, the response is stored in the named content group unless built-in policies override this policy. · If a matching response-time policy has a CACHE action but specifies a different content group from the one in the request-time policy, a NOCACHE action is applied. · If a matching response-time policy has a NOCACHE action, perform a NOCACHE action. · If there is no matching response-time policy, a CACHE action is applied, unless a built-in policy overrides this policy.

MAY_NOCACHE	For a request-time policy, this setting provisionally prevents caching the response. At response time, one of following actions is taken: · If no response-time policy matches the request, the final action is NOCACHE. · If a matching response-time policy contains a CACHE action, the final action is CACHE, unless built-in policies override this policy. · If a matching response-time policy contains a NOCACHE action, the final action is NOCACHE. · If a matching response-time policy has a CACHE action but does not specify a content group, the final action is to CACHE the response in the Default content group, unless built-in policies override this policy.
INVAL	Expires cached responses. Depending on how the policy and the content group are configured, all responses in one or more content groups are expired, or selected objects in the content group are expired. **Note:** You can specify INVAL actions in request-time policies only.

Bind Points for a Policy

You can bind the policy to one of the following bind points:

- **A global policy bank**. These are the request-time default, request-time override, response-time default, and response-time override policy banks, as described in "Order of Policy Evaluation."
- **A virtual server**. Policies that you bind to a virtual server are processed after the global override policies and before the global default policies, as described in "Order of Policy Evaluation." Note that when binding a policy to a virtual server, you bind it to either request-time or response-time processing.
- **An ad-hoc policy label**. A policy label is a name assigned to a policy bank. In addition to the global labels, the integrated cache has two built-in custom policy labels:
  - **_reqBuiltinDefaults**. This policy label, by default, is invoked from the request-time default policy bank.
  - **_resBuiltinDefaults**. This policy label, by default, is invoked from the response-time default policy bank.

  You can also define new policy labels. Policies bound to a user-defined policy label must be invoked from within a policy bank for one of the built-in bind points. For more information about creating a policy label, see "Configuring a Policy Label in the Integrated Cache." For more information about policy label invocation, see "Configuring a Policy Bank for Caching."

Important: You should bind a policy with an INVAL action to a request-time override or a response-time override bind point. To delete a policy, you must first unbind it.

Order of Policy Evaluation

For an advanced policy to take effect, you must ensure that the policy is invoked at some point during the NetScaler appliance's processing of traffic. To specify the invocation time, you associate the policy with a bind point. The following are the bind points, listed in order of evaluation:

- **Request-time override**. If a request matches a request-time override policy, by default request-time policy evaluation ends and the NetScaler appliance stores the action that is associated with the matching policy.
- **Request-time load balancing virtual server**. If policy evaluation cannot be completed after all the request-time override policies are evaluated, the NetScaler appliance processes request-time policies that are bound to load balancing virtual servers. If the request matches one of these policies, evaluation ends and the NetScaler appliance stores the action that is associated with the matching policy.
- **Request-time content switching virtual server**. Policies that are bound to this bind point are evaluated after request-time policies that are bound to load balancing virtual servers.

- **Request-time default**. If policy evaluation cannot be completed after all request-time, virtual server-specific policies are evaluated, the NetScaler appliance processes request-time default policies. If the request matches a request-time default policy, by default request-time policy evaluation ends and the NetScaler appliance stores the action that is associated with the matching policy.

- **Response-time override**. Similar to request-time override policy evaluation.

- **Response-time load balancing virtual server**. Similar to request-time virtual server policy evaluation.

- **Response-time content switching virtual server**. Similar to request-time virtual server policy evaluation.

- **Response-time default**. Similar to request-time default policy evaluation.

You can associate multiple policies with each bind point. To control the order of evaluation of the policies associated with the bind point you configure a priority level. In the absence of any other flow control information, policies are evaluated according to priority level, starting with the lowest numeric priority value.

After all integrated caching policies have been evaluated, if there are conflicting actions specified in request-time and response-time policies, the NetScaler appliance determines the final action as specified in the table, "Actions That You Can Associate with an Integrated Caching Policy."

Note: Request-time policies for POST data or cookie headers must be invoked during request-time override evaluation, because the built-in request-time policies in the integrated cache return a NOCACHE action for POST requests and a MAY_NOCACHE action for requests with cookies. Note that you would associate MAY_CACHE or MAY_NOCACHE actions with a request-time policy that points to a parameterized content group. The response time policy determines whether the transaction is stored in the cache.

Configuring a Policy in the Integrated Cache

You configure new policies to handle data that the built-in policies cannot process. You configure separate policies for caching, preventing caching from occurring, and for invalidating cached data. Following are the main components of a policy for integrated caching:

- Rule: A logical expression that evaluates an HTTP request or response.
- Action: You associate a policy with an action to determine what to do with a request or response that matches the policy rule.
- Content groups: You associate the policy with one or more content groups to identify where the action is to be performed.

To configure a policy for caching by using the command line interface

At the command prompt, type:

add cache policy <policyName> -rule <expression> -action CACHE|MAY_CACHE|NOCACHE|MAY_NOCACHE [-storeInGroup <contentGroupName>] [-undefAction NOCACHE|RESET]

Examples

> add cache policy image_cache -rule "http.req.url.contains(\"jpg\") || http.req.url.contains(\"jpeg\")" -actio
> add cache policy bugReportPolicy -rule "http.req.url.query.contains(\"IssuePage\")" -action CACHE -storeIn
> add cache policy my_form_policy -rule "http.req.header(\"Host\")contains(\"my.company.com\") && http.re
> add cache policy viewproducts_policy –rule "http.req.url.contains(\"viewproducts.aspx\")" –action CACHE -s

To configure a policy for invalidation by using the command line interface

At the command prompt, type:

add cache policy <policyName> -rule <expression> -action INVAL [-invalObjects "<contentGroupName1>[,<selectorName1>"]. . .]] | [-invalGroup <contentGroupName1>[, <contentGroupName2>. . .]] [-undefAction NOCACHE|RESET]

Examples

```
> add cache policy invalidation_events_policy -rule "http.req.header(\"Host\")contains(\"my.company.com\")
> add cache policy inval_all -rule "http.req.method.eq(\"POST\") && http.req.url.contains(\"jpeg\")" -action I
> add cache policy bugReportInvalidationPolicy -rule "http.req.url.query.contains(\"TransitionForm\")" -actio
> add cache policy editproducts_policy –rule "http.req.url.contains(\"editproducts.aspx\")" –action INVAL -inv
```

To configure a policy for caching or invalidation by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Policies.
2. In the details pane, do one of the following:
   - To create a new policy for caching or invalidation, click Add.
   - To modify an existing policy for caching or invalidation, select the policy, and then click Open.
3. In the Create Cache Policy or Configure Cache Policy dialog box, specify values for the following parameters. For a description of a parameter, hover the mouse cursor over the corresponding field.
   - Name
   - Action
   - Store in Group
   - Undefined-Result Action
   - Expression
   - Invalidate all objects in the following groups
   - Invalidate selected objects in the following parameterized groups
4. Click Create, and then click Close.

Parameter Descriptions (of commands listed in the CLI procedure)

add cache policy

policyName

The name of the new Integrated Cache policy.

rule

The request/response rule that will trigger the given action. The only actions you can specify with a request rule are: MAY_CACHE, MAY_NOCACHE, and INVAL. You specify a rule using a single expression or a logical combination of expressions (called a compound

expression). You can combine xpressions using the && and || operators. For more information on creating expressions, refer to the add expression CLI command. Note: If a compound expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes. The following are examples of valid expressions: ns_ext_cgi||ns_ext_asp "ns_non_get && (ns_header_cookie||ns_header_pragma)"

action

The integrated cache action to be applied when the system finds content that matches the rules. Possible values: CACHE, NOCACHE, MAY_CACHE, MAY_NOCACHE, INVAL

storeInGroup

The content group where the object will be stored when the action directive is CACHE

undefAction

A CACHE action, which is used by the policy when the rule evaluation is undefined. The undef action can be NOCACHE or RESET. Possible values: NOCACHE, RESET

invalObjects

The content group(s) where the objects will be invalidated when the action directive is INVAL

View description(s) in command reference Top

Globally Binding an Integrated Caching Policy

When you globally bind a policy, it is available to all virtual servers on the NetScaler appliance.

To bind an integrated caching policy globally by using the command line interface

At the command prompt, type:

bind cache global <policy> -priority <positiveInteger> [-type REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT] [-gotoPriorityExpression <expression>] [-invoke <labelType> <labelName>]

Example

> bind cache global myCachePolicy -priority 100 -type req_default

Note that the type argument is optional for globally bound policies, to maintain backward compatibility with policies that you defined using earlier versions of the NetScaler appliance. If you omit the type, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. If the rule contains both request time and response time parameters, it is bound to RES_DEFAULT. Following is an example of a binding that omits the type.

> bind cache global myCache Policy 200

To bind an integrated caching policy globally by using the configuration utility

1. In the navigation pane, click Integrated Caching.
2. In the details pane, click Cache policy manager.
3. In the Cache Policy Manager dialog box, select a Request or Response bind point, and then select a second level of binding of either Override Global or Default Global. A list of policies appears. These are policies that are bound to this bind point.
4. Click Insert Policy and do one of the following:
   - To configure a new policy, click New Policy and configure the new policy as described in "Configuring a Policy in the Integrated Cache."
   - To bind an existing policy, click the name of the policy.
5. Drag and drop the policy to the position in the policy bank where you want it to be evaluated, or manually enter a priority level, as a positive integer, for this entry in the Priority field.
6. Optionally, to configure a Goto expression as described in the "Policies and expressions", double-click the field in the Goto Expression column, and enter valid priority level, the keywords NEXT or END, or an advanced expression. See "Entries to Control Evaluation Flow in a Policy Bank" for details.
7. Optionally, to invoke an external policy bank, click the field in the Invoke Type column, and select the type of policy bank that you are adding (a global label or a virtual server bank). In the Invoke Name field, enter the label or virtual server name. See "Entries to Control Evaluation Flow in a Policy Bank" for details.
8. Click Apply Changes.

Parameter Descriptions (of commands listed in the CLI procedure)

bind cache global

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Binding an Integrated Caching Policy to a Virtual Server

When you bind a policy to a virtual server, it is available only to requests and responses that match the policy and that flow through the relevant virtual server.

When using the configuration utility, you can bind the policy using the configuration dialog box for the virtual server. This enables you to view all of the policies from all NetScaler modules that are bound to this virtual server. You can also use the Policy Manager configuration dialog for the integrated cache. This enables you to view only the integrated caching policies that are bound to the virtual server.

To bind an integrated caching policy to a virtual server by using the command line interface

At the command prompt, type:

- bind lb vserver <name>@ -policyName <policyName> -priority <positiveInteger> -type (REQUEST|RESPONSE)
- bind cs vserver <name>@ -policyName <policyName> -priority <positiveInteger> -type (REQUEST|RESPONSE)

To bind an integrated caching policy to a virtual server by using the configuration utility (virtual server method)

1. In the navigation pane, expand the module where you want to bind the caching policy, and then click Virtual Servers. This must be a module in which you can configure virtual servers. The choices are Load Balancing or Content Switching.

2. In the details pane, double-click the name of the virtual server with which you want to associate a policy for Integrated Caching, and then click Open.

3. In the Configure Virtual Server dialog box, click the Policies tab. In the list of policies in this dialog box, Integrated Caching policies can be identified in the Type column by the label Cache. Click the Active check box for the Integrated Caching policy that you want to bind to this bind point.

4. To configure a priority for the policy, double-click the value in the Priority field and enter a new positive integer value. The lower the value, the earlier the policy is evaluated.

5. In the Flow Type field for this entry, select Request or Response.

6. Click OK.

To bind an integrated caching policy to a virtual server by using the configuration utility (Policy Manager method)

1. In the navigation pane, click Integrated Caching.
2. In the details pane, click Cache policy manager.
3. In the Cache Policy Manager dialog box, select a Request or Response bind point, select a second level of binding of either LB Virtual Server or CS Virtual Server, and then select the name of a virtual server. A list of policies appears. These are integrated caching policies that are bound to this virtual server.
4. Click Insert Policy and do one of the following:
   - To configure a new policy, click New Policy and configure the new policy as described in "Configuring a Policy in the Integrated Cache."
   - To bind an existing policy, click the name of the policy.
5. Drag and drop the policy to the position in the policy bank where you want it to be evaluated, or manually enter a priority level, as a positive integer, for this entry in the Priority field.
6. Optionally, configure a Goto expression as described in "Configuring a Policy Bank for Caching."
7. Optionally, to invoke an external policy bank, click the field in the Invoke Type column, and select the type of policy bank that you are adding (a global label or a virtual server bank). In the Invoke Name field, enter the label or virtual server name. See "Entries to Control Evaluation Flow in a Policy Bank."
8. Click Apply Changes.

Parameter Descriptions (of commands listed in the CLI procedure)

bind lb vserver

policyName

The SureConnect/priority queuing/Compression/AppSecure/Transform/Filter/Authorization/Rewrite/Responder/Cache/Syslog/Nslog/TMTraffic policy that needs to be bound to the specified load balancing virtual server for SureConnect or priority queuing to be activated on a load balancing virtual server.

View description(s) in command reference Top

bind cs vserver

policyName

The content switch policy name (created with the add cs policy command).

View description(s) in command reference Top

Example: Caching Compressed and Uncompressed Versions of a File

By default, a client that can handle compression can be served uncompressed responses or compressed responses in gzip, deflate, compress, and pack200-gzip format. If the client handles compression, an Accept-Encoding:compression format header is sent in the request. The compression type accepted by the client must match the compression type of the cached object. For example, a cached .gzip file cannot be served in response to a request with an Accept-Encoding:deflate header.

A client that cannot handle compression is served a cache miss if the cached response is compressed.

For dynamic caching, you need to configure two content groups, one for compressed data and one for uncompressed versions of the same data. The following is an example of configuring the selectors, content groups, and policies for serving uncompressed files from the cache to clients that cannot handle compression, and serving compressed versions of the same files to client that can handle compression.

```
add cache selector uncompressed_response_selector http.req.url "http.req.header(\"Host\")"
add cache contentGroup uncompressed_group -hitSelector uncompressed_responst_selector -invalSelector u
add cache policy cache_uncompressed -rule "HTTP.REQ.URL.CONTAINS(\"xyz\") && !HTTP.REQ.HEADER(\"Acc
bind cache global cache_uncompressed -priority 100 -gotoPriorityExpression END -type REQ_OVERRIDE
add cache selector compressed_response_selector HTTP.REQ.URL "HTTP.REQ.HEADER(\"Host\")" "HTTP.REQ.H
add cache contentGroup compressed_group -hitSelector compressed_response_selector
add cache policy cache_compressed -rule "HTTP.REQ.URL.CONTAINS(\"xyz\") && HTTP.REQ.HEADER(\"Accept
bind cache global cache_compressed -priority 200 -gotoPriorityExpression END -type REQ_OVERRIDE
```

Configuring a Policy Bank for Caching

All of the policies that are associated with a particular bind point are collectively known as a policy bank. In addition to configuring priority levels for policies in a bank, you can modify the order of evaluation order in a bank by configuring Goto expressions. You can further modify the evaluation order by invoking an external policy bank from within the current policy bank. You can also configure new policy banks, to which you assign your own labels. Because such policy banks are not bound to any point in the processing cycle, they can be invoked only from within other policy banks. For convenience, policy banks whose labels do not correspond to a built-in bind point are called policy labels.

In addition to controlling order of policy evaluation by binding the policy and assigning a priority level, as described in "Binding Policies That Use the Default Syntax", you can establish the flow within a bank of policies by configuring a Goto expression. A Goto expression overrides the flow that is determined by the priority levels. You can also control the evaluation flow by invoking an external policy bank after evaluating an entry in the current bank. Evaluation always returns to the current bank after evaluation has completed for the external bank.

The following table summarizes the entries to control evaluation in a policy bank.

Table 1. Entries to Control Evaluation Flow in a Policy Bank

Attribute	Specifies
Name	The name of a policy, or, to invoke another policy bank without evaluating the policy, the keyword NOPOLICY. You can specify NOPOLICY more than once in a policy bank, but you can specify a named policy only once.
Priority	An integer. The lower the integer, the higher the priority.

Goto Expression	Determines the next policy or policy bank to evaluate. You can provide one of the following values: · **NEXT**: Go to the policy with the next higher priority. · **END**: Stop evaluation. · **USE_INVOCATION_RESULT**: Applicable if this entry invokes another policy bank. If the final Goto in the invoked bank has a value of END, evaluation stops. If the final Goto is anything other than END, the current policy bank performs a NEXT. · **Positive number**: Priority number of the next policy to be evaluated. · **Numeric expression**: Expression that produces the priority number of the next policy to be evaluated. The Goto can only proceed forward in a policy bank. Omitting the Goto expression is the same as specifying END.
Invocation Type	Designates a policy bank type. The value can be one of the following: · **Request Vserver**: Invokes request-time policies that are associated with a virtual server. · **Response Vserver**: Invokes response-time policies that are associated with a virtual server. · **Policy label**: Invokes another policy bank, as identified by the policy label for the bank.
Invocation Name	Name of a virtual server or a policy label, depending on the value that you specified for the Invocation Type.

The integrated cache has two built-in policy labels, and you can configure additional policy labels:

- **_reqBuiltInDefaults**: This policy label is invoked from the request-time default bind point.
- **_resBuiltInDefaults**: This policy label is invoked from the response-time default bind point.

Note: For information about creating policy labels, see " Configuring a Policy Label in the Integrated Cache."

To invoke a policy label in a caching policy bank by using the command line interface

At the command prompt, type:

bind cache policylabel <labelName> -policname<policyName> -priority<priority> [-gotoPriorityExpression <gotopriorityExpression>] [-invoke <labelType> <labelName>]

To invoke a policy label in a caching policy bank by using the configuration utility

1. In the navigation pane, click Integrated Caching.
2. In the details pane, click Cache policy manager.
3. In the Cache Policy Manager dialog box, select a Request or Response bind point, and then select a second level of binding of either Override Global or Default Global. A list of policies appears. These are policies that are bound to this bind point.
4. If you want to invoke a policy label without evaluating a policy, select Insert Policy and select the keyword NOPOLICY.

   If you want to invoke a policy label after processing a policy, skip this step.
5. To invoke an external policy bank, click the field in the Invoke Type column, and select the type of policy bank that you want to invoke at this point in the policy bank. This can be a global label or a virtual server bank. In the Invoke Name field, enter the label or virtual server name. See "Entries to Control Evaluation Flow in a Policy Bank" for details.
6. Click Apply Changes.

To invoke a caching policy label in a virtual server policy bank by using the command line interface

At the command prompt, type:

- bind lb vserver <name>@ -policyName <policyName>|<NOPOLICY-CACHE> -priority <positiveInteger> -gotoPriorityExpression <expression> -type REQUEST|RESPONSE -invoke <labelType> <labelName>
- bind cs vserver <name> -policyName <policyName>|<NOPOLICY-CACHE> -priority <positiveInteger> -gotoPriorityExpression <expression> -type REQUEST|RESPONSE -invoke <labelType> <labelName>

For more information, see "Entries to Control Evaluation Flow in a Policy Bank."

To invoke a caching policy label in a virtual server policy bank by using the configuration utility

1. In the navigation pane, click Load Balancing or Content Switching, as appropriate, and then click Virtual Servers.

2. Double-click the virtual server where you want to configure the policy bank, and in the Configure Virtual Server dialog box, click the Policies tab.

3. If you are configuring an existing entry in this bank, skip this step. If you are adding a new policy to this policy bank, or you want to use the “dummy” NOPOLICY entry, click Add Policy, and do one of the following:

   - To configure a new policy, click Cache and configure the new policy as described in "Configuring a Policy in the Integrated Cache."

   - To invoke a policy bank without processing a policy a rule, select the NOPOLICY-CACHE option.

   After configuring the new entry, it appears at the bottom of the list of entries with the name of the policy in the Policy Name field.

4. To bind the entry to this policy label, ensure the Active check box is selected.

5. Enter a priority level for this entry in the Priority field. The priority is a positive integer.

6. Optionally, to configure a Goto Expression, double-click the field in the Goto Expression column, and enter valid priority number, the keyword NEXT or END, or an advanced expression. For more information, see "Entries to Control Evaluation Flow in a Policy Bank."

7. To invoke another policy bank, click the field in the Invoke Type column, and select the type of policy bank that you are adding (a global label or a virtual server bank). In the Invoke Name field enter the label or virtual server name. When you are done, click OK. For more information, see "Entries to Control Evaluation Flow in a Policy Bank."

Parameter Descriptions (of commands listed in the CLI procedure)

bind cache policylabel

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind lb vserver

policyName

The SureConnect/priority queuing/Compression/AppSecure/Transform/Filter/Authorization/Rewrite/Responder/Cache/Syslog/Nslog/TMTraffic policy that needs to be bound to

the specified load balancing virtual server for SureConnect or priority queuing to be activated on a load balancing virtual server.

View description(s) in command reference Top

bind cs vserver

policyName

The content switch policy name (created with the add cs policy command).

View description(s) in command reference Top

Configuring a Policy Label in the Integrated Cache

In addition to configuring policies in a policy bank for one of the built-in bind points or a virtual server, you can create caching policy labels and configure banks of policies for these new labels.

A policy label for the integrated cache can be invoked only from one of the bind points that you can view in the Policy Manager in the **Integrated Caching** details pane (request override, request default, response override, or response default) or the built-in policy labels _reqBuiltinDefaults and _resBuiltinDefaults. You can invoke a policy label any number of times unlike a policy, which can only be invoked once.

The configuration utility provides an option to rename a policy label. Renaming a policy label does not affect the process of evaluation of the policies bound to the label.

Note: You can use the NOPOLICY “dummy” policy to invoke any policy label from another policy bank. The NOPOLICY entry is a placeholder that does not process a rule.

To configure a policy label for caching by using the command line interface

At the command prompt, type the following command to create a policy label and verify the configuration:

- add cache policylabel <labelName> -evaluates (REQ|RES)
- show cache policylabel <labelName>

Invoke this policy label from a policy bank. For more information, see "Configuring a Policy Bank for Caching."

To configure a policy label for caching by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Policy Labels.
2. If you are configuring a new policy label, click Add. Then, in the Create Cache Policy Label dialog box, enter a name. To specify whether the policy label is invoked at request time or response time, in the Evaluates drop-down menu, select either REQ or RES, respectively.

   If you are configuring an existing label, from the Policy Labels page, double-click the label.
3. To add a policy to this policy label, click Insert Policy.
4. Optionally, you can invoke other policy labels from this policy label, as described in "Configuring a Policy Bank for Caching."
5. To ensure that the NetScaler appliance processes the policy label at the right time, you configure an invocation of this label in one of the banks that are associated with the built-in bind points, as described in "Configuring a Policy Bank for Caching."

To rename a policy label by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Policy Labels.
2. In the details pane, select the policy label that you want to rename, and then click **Rename**.
3. In the **Rename Cache Policy Label** dialog box, in **Name**, replace the existing name with the name you want.
4. Click **OK**.

Parameter Descriptions (of commands listed in the CLI procedure)

add cache policylabel

evaluates

Gives when policies bound to this label get executed. Possible values: REQ, RES, MSSQL_REQ, MSSQL_RES, MYSQL_REQ, MYSQL_RES

View description(s) in command reference Top

show cache policylabel

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Unbinding and Deleting an Integrated Caching Policy and Policy Label

You can unbind a policy from a policy bank, and you can delete it. To delete the policy, you must first unbind it. You can also remove a policy label invocation and delete a policy label. To delete the policy label, you must first remove any invocations that you have configured for the label.

You cannot unbind or delete the labels for the built-in bind points (request default, request override, response default, and response override).

To unbind a global caching policy by using the command line interface

At the command prompt, type:

unbind cache global <policy>

To unbind a virtual server-specific caching policy by using the command line interface

At the command prompt, type:

(unbind lb vserver|unbind cs vserver) <vserverName> -policyName <policyName> -type (REQUEST|RESPONSE)

To delete a caching policy by using the command line interface

At the command prompt, type:

rm cache policy <policyName>

To unbind a caching policy by using the configuration utility

1. In the navigation pane, click Integrated Caching.
2. In the details pane, click Cache policy manager.
3. In the Cache Policy Manager dialog box, select a Request or Response bind point, select a second level of binding of either LB Virtual Server or CS Virtual Server, and then select the name of a virtual server. A list of policies appears. These are integrated caching policies that are bound to this virtual server.
4. Select the caching policy you want to unbind, and then click Unbind Policy.
5. Click Close.

To delete a policy label invocation by using the configuration utility

1. In the navigation pane, click Integrated Caching.
2. In the details pane, click Cache policy manager.
3. In the Cache Policy Manager dialog box, select a Request or Response bind point, select a second level of binding of either LB Virtual Server or CS Virtual Server, and then select the name of a virtual server. A list of policies appears. These are integrated caching policies that are bound to this virtual server.
4. In the Invoke column for the policy label you want to invoke, click the drop-down list and clear the entry.
5. Click Close.

Parameter Descriptions (of commands listed in the CLI procedure)

unbind cache global

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

rm cache policy

policyName

The name of the cache policy to be removed.

View description(s) in command reference Top

Caching Support for Database Protocols

The integrated cache monitors database requests that flow through the Citrix® NetScaler® appliance and caches them as determined by the cache policies. Users have to configure the cache polices for MYSQL and MSSQL protocols, because the NetScaler does not provide any default policies for these protocols. When configuring the protocols, remember that request based policies currently support CACHE and INVAL actions, while response based policies currently support only NOCACHE action. After configuring the policies, bind them to virtual servers. MYSQL and MSSQL policies, both request and response, can be bound only to virtual servers

Before creating a cache policy, create a cache content group of type MYSQL or MSSQL. When you create a MYSQL or MSSQL cache content group, associate at least one hit selector with it. See "Setting Up a Basic Content Group" for setting up cache content groups.

The following example illustrates the procedure for configuring and verifying cache support for SQL protocols.

```
> enable feature IC
> set cache parameter -memlimit 100
> add cache selector sel1 mssql.req.query.text

> add cache contentgroup cg1  -type "MSSQL" -hitselector "sel1" -invalselector "inval_sel" -relExpiry "500" -ma
 "100"
> add cache policy cp1  -rule "mssql.req.query.command.contains(\"select\")" -action "CACHE" -storeInGroup
> add cache policy cp2  -invalObjects "cg1" -rule "mssql.req.query.text.contains(\"insert\")" -action "INVAL"
> add db user user1  -password "Pass1"
> add service svc_sql_1 10.102.147.70 mssql 64834 -healthMonitor "NO" -downstateflush "ENABLED"
> add lb vserver lb_mssql1 mssql 10.102.147.77 1433  -lbmethod "roundrobin"
> bind lb vserver lb_mssql1 svc_sql_1
> bind lb vserver lb_mssql1 -policyName cp1  -type "REQUEST" -priority "2"
> bind lb vserver lb_mssql1 -policyName cp2  -type "REQUEST" -priority "1"

> show cache selector sel1
    Name:sel1
                Expressions:
                1)mssql.req.query.text
> show cache policy cp1
                Name:cp1
    Rule:mssql.req.query.command.contains("select")
                CacheAction:CACHE
                Stored in group: cg1
                UndefAction:Use Global
              Hits:2
                Undef Hits:0
                Policy is bound to following entities
                1) Bound to:
                        REQ VSERVER lb_mssql1
                        Priority:2
                        GotoPriorityExpression: END
```

Note: The methods for reducing flash crowds, as explained in "Reducing Flash Crowds", are not supported for MYSQL and MSSQL protocols.

Configuring Expressions for Caching Policies and Selectors

A request-time expression examines data in request-time transaction, and a response-time expression examines data in a response-time transaction. In a policy for caching, if an expression matches data in a request or response, the Citrix NetScaler appliance takes the action associated with the policy. In a selector, request-time expressions are used to find matching responses that are stored in a content group.

Before configuring policies and selectors for the integrated cache, you need to know, at minimum, the host names, paths, and IP addresses that appear in HTTP request and response URLs. And you probably need to know the format of entire HTTP requests and responses. Programs such as Live HTTP Headers (http://livehttpheaders.mozdev.org/) or HTTPFox (https://addons.mozilla.org/en-US/firefox/addon/6647) can help you investigate the structure of the HTTP data that your organization works with.

Following is an example of an HTTP GET request for a stock quote program:

```
GET /quote.dll?page=dynamic&mode=data&mode=stock&symbol=CTXS&page=multi&selected=CTXS&random
Host: quotes.mystockquotes.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9) Gecko/2008052906 Firefox/3.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate,compress,pack200-gzip
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://quotes.mystockquotes.com/quote.dll?mode=stock&symbol=CTXS&page=multi&selected=CTX
Cookie: __qca=1210021679-72161677-10297606
```

When configuring an expression, note the following limitations:

Table 1. Restrictions on Request-Time and Response-Time Expressions

Expression Type	Restrictions
Request	Do not configure request-time expressions in a policy with a CACHE or NOCACHE action. Use MAY_CACHE or MAY_NOCACHE instead.

Response	Configure response-time expressions in caching policies only. · Selectors can use only request-time expressions. · Do not configure response-time expressions in a policy with an INVAL action. Do not configure response-time expressions in a policy with a CACHE action and a parameterized content group. Use the MAY_CACHE action.

Note: For a comprehensive discussion of advanced expressions, see "Policies and Expression."

Expression Syntax

Following are basic components of the syntax:

- Separate keywords with periods (.), as follows:

  ```
  http.req.url
  ```

- Enclose string values in parentheses and quotes, as follows:

  ```
  http.req.url.query.contains("this")
  ```

- When configuring an expression from the command line, you must escape internal quote marks (the quotes that delimit values in the expression, as opposed to the quotes that delimit the expression). One method is to use a slash, as followings:

  ```
  \"abc\"
  ```

Selector expressions are evaluated in order of appearance, and multiple expressions in a selector definition are joined by a logical AND. Unlike selector expressions, you can specify Boolean operators and modify the precedence in an advanced expression for a policy rule.

Configuring an Expression in a Caching Policy or a Selector

Note that on the command line, the syntax for a policy expression is somewhat different from a selector expression. For a comprehensive discussion of advanced expressions, see "Policies and Expressions."

To configure a policy expression by using the command line interface

1. Start the policy definition as described in "Globally Binding an Integrated Caching Policy."

2. To configure the policy rule, delimit the entire rule in quotes, and delimit string values within the rule in escaped quotes.

   The following is an example:

   "http.req.url.contains(\"jpg\")"

3. To add Boolean values, insert &&, ||, or ! operators.

   The following are examples:

   "http.req.url.contains(\"jpg\") || http.req.url.contains(\"jpeg\")"
   "http.req.url.query.contains(\"IssuePage\")"
   "http.req.header(\"Host\")contains(\"my.company.com\") && http.req.method.eq(\"GET\") && http.req.u

4. To configure an order of evaluation for the constituent parts of a compound

   "http.req.url.contains(\"jpg\") || (http.req.url.contains(\"jpeg\") && http.req.method.eq(\"GET\"))"

To configure a selector expression by using the command line interface

1. Start the selector definition as described in "About Content Groups."

2. To configure the selector expression, delimit the entire rule in quotes, and delimit string values within the rule in escaped quotes.

   The following is an example:

   "http.req.url.contains(\"jpg\")"

3. You cannot add Boolean values, insert &&, ||, or ! operators. Enter each expression element delimited in quotes. Multiple expressions in the definition are treated as a compound expression joined by logical ANDs.

   The following are examples:

   "http.req.url.query.value(\"ProductId\")" "http.req.url.query.value(\"BatchNum\")" "http.req.url.query.val

To configure a policy or selector expression by using the configuration utility

1. Start the policy or selector definition as described in "To configure a policy for caching or invalidation by using the configuration utility" or "To configure a selector by using the configuration utility."

2. Click in the Expression field.

3. Click the Prefix icon (the house) and select the first expression prefix from the drop-down list. The options are HTTP, SYS, CLIENT, and SERVER. The next set of applicable options appears in a drop-down list.

4. Double-click the next option to select it, and then type a period (.). Again, a set of applicable options appear in another drop-down list.

5. Continue selecting options until an entry field (indicated by parentheses) appears. When you see an entry field, enter an appropriate value in the parentheses. For example, if you select GT(int) (greater-than, integer format), you specify an integer in the parentheses. Text strings are delimited by quote marks. The following is an example:

   ```
   HTTP.REQ.BODY(1000).BETWEEN("this","that")
   ```

6. To insert an operator between two parts of a compound expression, click the Operators icon (the sigma), and select the operator type. The following is an example of a configured expression with a Boolean OR (signaled by double vertical bars, ||):

   ```
   HTTP.REQ.URL.EQ("www.mycompany.com")||HTTP.REQ.BODY(1000).BETWEEN("this","that")
   ```

7. To insert a named expression, click the down arrow next to the Add icon (the plus sign) and select a named expression. For more information about named expressions, see "Policies and Expressions."

8. To configure an expression using drop-down menus, and to insert built-in expressions, click the Add icon (the plus sign). The Add Expression dialog box works in a similar way to the main dialog box, but it provides drop-down lists for selecting options, and it provides text fields for data entry instead of parentheses. This dialog box also provides a Frequently Used Expressions drop-down list that inserts commonly used expressions. When you are done adding the expression using this dialog box, click OK.

9. To test the expression, click the Evaluate icon (the check mark). In the Advanced Expression Evaluator dialog box, select the Flow Type that matches the expression. In the data field, paste the HTTP request or response that you hope to parse using the expression, and click Evaluate. Click OK to save your expression and close this dialog box.

10. When you are done, click Create and then click Close.

Displaying Cached Objects and Cache Statistics

You can view particular cached objects, and you can view summary statistics on cache hits, misses, and memory usage. The statistics provide insight on the amount of data that is being served from the cache, what items are responsible for the largest performance benefit, and what you can tune to improve cache performance.

Viewing Cached Objects

After enabling caching, you can view details for cached objects. For example, you can view the following items:

- Response sizes and header sizes
- Status codes
- Content groups
- ETag, Last-Modified, and Cache-Control headers
- Request URLs
- Hit parameters
- Destination IP addresses
- Request and response times

To view a list of cached objects by using the command line interface

At the command prompt, type:

show cache object

Table 1. Properties of Cached Objects

Properties	Specifies
Response size (bytes)	The size of the response header and body.
Response header size (bytes)	The size of the header portion of the response.
Response status code	The status code sent with the response.
ETag	The ETag header inserted in the response. Typically, this header indicates whether the response has changed recently.
Last-Modified	The Last-Modified header inserted in the response. This header indicates the date that the response was last changed.
Cache-Control	The Cache-Control header inserted in the response.
Date	The Date header that indicates when the response was sent.

Contentgroup	The content group where the response is stored.
Complex match	If this object was cached on the basis of parameterized values, this field value is YES.
Host	The host specified in the URL that requested this response.
Host port	The listen port for the host specified in the URL that requested this response.
URL	The URL issued for the stored response.
Destination IP	The IP address of the server from which this response was fetched.
Destination port	The listen port for the destination server.
Hit parameters	If the content group that stores the response uses hit parameters, they are listed in this field.
Hit selector	If this content group uses a hit selector, it is listed in this field.
Inval selector	If this content group uses an invalidation selector, it is listed in this field.
Selector Expressions	If this content group uses a selector, this field displays the expression that defines the selection rule.
Request time	The time in milliseconds since the request was issued.
Response time	The time in milliseconds since the cache started to receive the response.
Age	Amount of time the object has been in the cache.
Expiry	Amount of time after which the object is marked as expired.
Flushed	Whether the response has been flushed after expiry.
Prefetch	If Prefetch has been configured for this content group, the amount of time before expiry during which the object is fetched from the origin. Prefetch does not apply to negative objects (for example, 404 "object not found" responses).

Current readers	Approximately the current number of hits being served. When a response with a Content-Length header object is being downloaded, the current misses and the current readers values are each typically 1. When a chunked response object is being downloaded, the current misses value is typically 1, but the current readers value is typically 0, because the chunked response that is served to the client does not come from the integrated caching buffers.
Current misses	The current number of requests that resulted in a cache miss and fetching from the origin server. This value is typically 0 or 1. If Poll Every Time is enabled for a content group, the count can be greater than 1.
Hits	The number of cache hits for this object.
Misses	The number of cache misses for this object.
Compression format	The type of compression applied to this object. Compression formats include gzip, deflate, compress, and pack200-gzip.
HTTP version in response	The version of HTTP that was used to send the response.
Weak etag present in response	Strong etag headers change if the bits of an entity change. Strong headers are based on the octet values of an object. Weak etag headers change if the meaning of an entity changes. Weak etag values are based on semantic identity. Weak etags values start with a "W."
Negative marker cell	A marker object is cacheable, but it does not yet meet all the criteria for being cached. For example, the object may exceed the maximum response size for the content group. A marker cell is created for objects of this type. The next time a user sends a request for this object, a cache miss is served.
Reason marker created	The reason a marker cell was created (for example, “Waiting for minhit,” “Content-length response data is not in group size limit”).
Auto poll every time	If the integrated cache receives an already expired 200 OK response with validators (either the Last-Modified or the ETag response headers) it stores the response and marks it as Auto-PET (automatically poll every time).

NetScaler Etag inserted in response	A variation of the ETag header generated by the NetScaler appliance. A value of YES appears if the NetScaler inserts an Etag in the response.
Full response present in cache	Indicates whether this is a complete response.
Destination IP verified by DNS	Indicates whether DNS resolution was performed when storing the object.
Object stored through a cache forward proxy	Indicates whether this response was stored due to a forward proxy that is configured in the integrated cache.
Object is a Delta basefile	A response that is delta-compressed.
Waiting for minhits	Indicates whether this content group requires a minimum number of origin server hits before caching a response.
Minhit count	If this content group requires a minimum number of origin server hits before caching an object, this field displays a count of the number of hits received so far.
HTTP Request Method	The method, GET or POST, used in the request that obtained this object.
Stored by policy	The name of the caching policy that caused this object to be stored. A value of NOT AVAILABLE indicates that the policy has been deactivated or deleted. A value of NONE indicates that the object did not match a visible policy, but was stored according to internal criteria for caching.
Application firewall metadata exists	This parameter is used when the application firewall and the integrated cache are both enabled. The application firewall analyzes the contents of a response page, stores its metadata (for example, URLs and forms contained in page), and exports the metadata with the response to the cache. The cache stores the page and the metadata, and when the cache serves the page, it sends the metadata back to the request's session.
HTTP callout object, name, type, response	These cells indicate whether this data was stored as a result of an HTTP Callout expression, and provide information about various aspects of the callout and the corresponding response. For more information about HTTP callouts, see "HTTP Callouts".

To view cached objects by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Cache Objects.

   By default, all cached responses are displayed. If you have not yet configured any content groups, all of the responses are in the Default group.

2. To filter the cached responses by content group, click the Content Group Name drop-down menu, and then select the name of a content group.

3. To filter the cached responses by HTTP status code, enter the HTTP status code in the HTTP Status Code dialog box.

4. To filter out marker objects and not-ready objects, click the check box for Ignore Marker Objects and leave the check box for Include Not Ready Objects blank.

   These settings represent objects that can be served from the cache, pending additional information. Marker objects are responses that have not yet reached a minimum number of hits before being cached. Not-ready objects have not yet received response headers.

5. Click Go.

   To view details for a cached object, click it, and then click Details.

6. To save a locator number for later use, right-click the row that contains the object and its locator number, select Copy, and then paste the information into a document.

Parameter Descriptions (of commands listed in the CLI procedure)

show cache object

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Finding Particular Cached Responses

You can find individual items in the cache based on search criteria. There are different methods for finding cached items, depending on whether the content group that contains the data uses hit and invalidation selectors, as follows:

- If the content group uses selectors, you can only conduct the search using the Locator ID for the cached item.
- If the content group does not use selectors, you conduct the search using criteria such as URL, host, content group name, and so on.

When searching for a cached response, you can locate some items by URL and host. If the response is in a content group that uses a selector, you can find it only by using a Locator number (for example, 0x00000000ad7af00000050). To save a Locator number for later use, right-click the entry and select **Copy**. For more information about selectors, see "Configuring Selectors and Basic Content Groups."

To display cached responses in content groups that do not have a selector by using the command line interface

At the command prompt, type:

show cache object [-locator <positiveInteger>] | [(-url <URL> (-host <hostName> [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET | POST])) | [-httpStatus<positive integer>] | -group <contentGroupName> | -ignoreMarkerObjects (ON | OFF) | -includeNotReadyObjects (ON | OFF)]

To display cached responses in content groups that have a selector by using the command line interface

At the command prompt, type:

show cache object -locator <locatorString> MarkerObjects (ON | OFF) | -includeNotReadyObjects (ON | OFF) | [-httpStatus<positive integer>]

To display cached responses in content groups that do not have a selector by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Cache Objects.

   If you have not yet configured any content groups, all of the objects are in the Default group.

2. At the top of the details pane, click Find.

3. Enter search criteria, as follows:

   - In the Search In drop-down list, select a search filter, for example, URL. Note that if you are searching for items in a content group that uses a selector, select the Locator option.

   - In the Criterion drop-down list, select the search method, for example, Contains.

   - In Look for, enter the text that is to be matched, for example, **www.myurl.com**.

   - Optionally, restrict the search according to a particular content group, and exclude not ready and marker objects.

4. Click Find Now.

To display cached responses in content groups that have a selector by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Cache Objects.

2. In the details pane, click Look Up.

3. In the Look Up Cache Object dialog box, do one of the following:

   - To find an object that resides in a content group that does not use a selector, click Only static and parameterized groups and enter selection criteria.

     The URL and host IP address are required. For example, you could enter /manual/images/sub.gif as the URL and 10.102.91.160 as the host. The content group name is also required if the content group contains parameterized objects.

   - To find an object that resides in a content group that uses a selector, click All groups including selector-based and, in Locator, enter the locator of the object that you want to view.

4. Click View Details.

5. In the Details dialog box, click any parameter to display its value in the Value box.

Parameter Descriptions (of commands listed in the CLI procedure)

show cache object

locator

The id of the cached object.

url

The URL of the object.

host

The hostname of the object.

port

The host port of the object. Default value: 80 Minimum value: 1

groupName

The name of the content group to be in which the cell is present

httpMethod

The HTTP request method that caused the object to be stored. Possible values: GET, POST Default value: NS_HTTP_METHOD_GET

httpStatus

HTTP status of the object.

group

The name of the content group whose objects should be listed.

ignoreMarkerObjects

Ignore marker objects Possible values: ON, OFF

includeNotReadyObjects

Include objects not-ready for a cache hit Possible values: ON, OFF

View description(s) in command reference Top

Viewing Cache Statistics

The following table summarizes the detailed cache statistics that you can view.

Table 1. Integrated Cache Statistics

Counter	Specifies
Hits	Responses that are found in and served from the integrated cache. Includes static objects such as image files, pages with status codes 200, 203, 300, 301, 302, 304, 307, 403, 404, 410, and responses that match a user-defined policy with a CACHE action..
Misses	Intercepted HTTP requests where the response was ultimately fetched from origin server.
Requests	Total cache hits plus total cache misses.
Non-304 hits	If the user requests an item more than once, and the item in the cache is unchanged since the last time the NetScaler appliance served it, the NetScaler appliance serves a 304 response instead of the cached object. This statistic indicates how many items the NetScaler appliance served from the cache, excluding 304 responses.
304 hits	Number of 304 (object not modified) responses the NetScaler appliance served from the cache.
304 hit ratio (%)	Percentage of 304 responses that the NetScaler appliance served, relative to other responses.
Hit ratio (%)	Percentage of responses that the NetScaler appliance served from the cache (cache hits) relative to responses that could not be served from the cache.
Origin bandwidth saved (%)	An estimate of the processing capacity that the NetScaler appliance saved on the origin server due to serving responses from the cache.
Bytes served by the NetScaler	Total number of bytes that the NetScaler appliance served from the origin server and the cache.

Bytes served by cache	Total number of bytes that the NetScaler appliance served from the cache.
Byte hit ratio(%)	Percentage of data that the NetScaler appliance served from the cache, relative to all of the data in all served responses.
Compressed bytes from cache	Amount of data, in bytes, that the NetScaler appliance served in compressed form.
Storable misses	If the NetScaler appliance does not find a requested object in the cache, it fetches the object from the origin server. This is known as a cache miss. A storable cache miss can be stored in the cache.
Non-storable misses	A non-storable cache miss cannot be stored in the cache.
Misses	All cache misses.
Revalidations	Max-Age setting in a Cache-Control header determines, in number of seconds, when an intervening cache must revalidate the content with the integrated cache before serving it to the user. For more information, see "Inserting a Cache-Control Header."
Successful revalidations	Number of re-validations that have been performed. For more information, see "Inserting a Cache-Control Header."
Conversions to conditional req	A user-agent request for a cached PET object is always converted to a conditional request and sent to the origin server. For more information, see "Polling the Origin Server Every Time a Request Is Received."
Storable miss ratio (%)	Storable cache misses as a percentage of non-storable cache misses.
Successful reval ratio (%)	Successful revalidations as a percentage of all revalidation attempts. For more information, see "Inserting a Cache-Control Header."

Expire at last byte	Number of times that the cache expired content immediately after receiving the last body byte. Only applicable to positive responses, as described in the table "Cache Hits and Misses." For more information, see "Example of Performance Optimization."
Flashcache misses	If you enable Flash Cache, the cache allows only one request to reach the server, eliminating flash crowds. This statistic indicates the number of Flash Cache requests that were cache misses. For more information, "Queuing Requests to the Cache."
Flashcache hits	Number of Flash Cache requests that were cache hits. For more information, see "Queuing Requests to the Cache."
Parameterized inval requests	Requests that match a policy with an invalidation (INVAL) action and a content group that uses an invalidation selector or parameters to selectively expire cached objects in the group.
Full inval requests	Requests that match an invalidation policy where the invalGroups parameter is configured and expires one or more content groups.
Inval requests	Requests that match an invalidation policy and result in expiration of specific cached responses or entire content groups.
Parameterized requests	Number of cache requests that were processed using a policy with a parameterized content group.
Parameterized non-304 hits	Number of cache requests that were processed using a policy with a parameterized content group, where full cached response was found, and the response was not a 304 (object not updated) response.
Parameterized 304 hits	Number of cache requests that were processed using a policy with a parameterized content group, where the cached object was found, and the object was a 304 (object not updated) response.
Total parameterized hits	Number of cache requests that were processed using a policy with a parameterized content group, where the cached object was found.

Parameterized 304 hit ratio (%)	Percentage of 304 (object not updated) responses that were found using a parameterized policy, relative to all cache hits.
Poll every time requests	If Poll Every Time is enabled, the NetScaler appliance always consults the origin server before serving a stored object. For more information, see "Polling the Origin Server Every Time a Request Is Received."
Poll every time hits	Number of times a cache hit was found using the Poll Every Time method. For more information, see "Polling the Origin Server Every Time a Request Is Received."
Poll every time hit ratio (%)	Percentage of cache hits using the Poll Every Time method, relative to all searches for cached objects using Poll Every Time. For more information, see "Polling the Origin Server Every Time a Request Is Received."
Maximum memory (KB)	Maximum amount of memory in the NetScaler appliance that is allocated to the cache. For more information, see "Configuring Global Attributes for Caching."
Maximum memory active value (KB)	Maximum amount of memory (active value) that will be set after the memory is actually allocated to the cache. For more information, see "How to Configure the Integrated Caching Feature of a NetScaler Appliance for various Scenarios."
Utilized memory (KB)	Amount of memory that is actually being used.
Memory allocation failures	Number of failed attempts to utilize memory for the purpose of storing a response in the cache.
Largest response so far	Largest response in bytes found in either the cache or the origin server and sent to the client.
Cached objects	Number of objects in the cache, including responses that have not yet been fully downloaded and responses that have been expired but not yet flushed.

Marker objects	Marker objects are created when a response exceeds the maximum or minimum response size for the content group, or has not yet received the minimum number of hits for the content group.
Hits being served	Number of hits that have been served from the cache.
Misses being handled	Responses that were fetched from the origin server, stored in the cache, and then served. Should approximate the number for storable misses. Does not include non-storable misses.

To view summary cache statistics by using the command line interface

At the command prompt, type:

stat cache

To view specific cache statistics by using the command line interface

At the command prompt, type:

stat cache -detail [-fullValues] [-ntimes <positiveInteger>] [-logFile <inputFilename>]

To view summary cache statistics by using the configuration utility

1. Click the Dashboard tab at the top of the page.
2. Scroll down to the Integrated Caching section of the window.
3. To see detailed statistics, click the More... link at the bottom of the table.

To view specific cache statistics by using the configuration utility

1. Click the Reporting tab at the top of the page.
2. Under Built-In Reports, expand Integrated Cache, and then click the report with the statistics you want to view.
3. To save the report as a template, click Save As and name the report. The saved report appears under Custom Reports.

Parameter Descriptions (of commands listed in the CLI procedure)

stat cache

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Improving Cache Performance

You can improve the performance of integrated cache, including handling simultaneous requests for the same cached data, avoiding delays that are associated with refreshing cached responses from the origin server, and ensuring that a response is requested often enough to be worth caching.

Reducing Flash Crowds

Flash crowds occur when many users simultaneously request the same data. All of the requests in a flash crowd can become cache misses if you configured the cache to serve hits only after the entire object is downloaded.

The following techniques can reduce or eliminate flash crowds:

- **PREFETCH**: Refreshes a positive response before it expires to ensure that it never becomes stale or inactive.

  For more information, see "Refreshing a Response Prior to Expiration."

- **Cache buffering**: Starts serving a response to multiple clients as soon as it receives the response header from the origin server, rather than waiting for the entire response to be downloaded.

  The only limit on the number of clients that can download a response simultaneously is the available system resources.

  The Citrix NetScaler appliance downloads and serves responses even if the client that initiated the download halts before the download is complete. If the size of the response exceeds the cache size or if the response is chunked, the cache stops storing the response, but service to the clients is not disrupted.

- **Flash Cache**: Flash Cache queues requests to the cache, and allows only one request to reach the server at a time.

  For more information, see "Queuing Requests to the Cache."

Refreshing a Response Prior to Expiration

To ensure that a cached response is fresh whenever it is needed, the PREFETCH option refreshes a response before its calculated expiration time. The prefetch interval is calculated after receiving the first client request. From that point onward, the NetScaler appliance refreshes the cached response at a time interval that you configure in the PREFETCH parameter.

This setting is useful for data that is updated frequently between requests. It does not apply to negative responses (for example, 404 messages).

To configure prefetch for a content group by using the command line interface

At the command prompt, type:

set cache contentgroup <name> -prefetch YES [-prefetchPeriod <seconds> | -prefetchPeriodMilliSec <milliseconds>] [-prefetchMaxPending <positiveInteger>]

To configure prefetch for a content group by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Content Groups.
2. In the details pane, click the content group for which you want to set prefetch, and then click Open.
3. In the Configure Cache Content Group dialog box, on the Others tab, under Flash Crowd and Prefetch, select the Prefetch check box.
4. In the Interval text box, enter a value to define an interval that a prefetch can be attempted. This should be shorter than the content group's calculated expiration time. Or, accept the default (heuristic prefetch interval). Note that the value can be in seconds or, if relative expiry is specified in milliseconds on the Expiry Method tab, you can select a value in milliseconds.
5. In the Maximum number of pending prefetches text box, enter a value for the maximum number of prefetches that can be queued for the content group. The minimum value is 0, and the maximum value is 4294967295.
6. Click OK.

Queuing Requests to the Cache

The Flash Cache option queues requests that arrive simultaneously (a flash crowd), retrieves the response, and distributes it to all the clients whose requests are in the queue. If, during this process, the response becomes non-cacheable, the NetScaler appliance stops serving the response from the cache and instead serves the origin server's response to the queued clients. If the response is not available, the clients receive an error message.

Flash Cache is disabled by default. You cannot enable Poll Every Time (PET) and Flash Cache on the same content group.

One disadvantage of Flash Cache is if the server replies with an error (for example, a 404 that is quickly remedied), the error is fanned out to the waiting clients.

Note: If Flash Cache is enabled, in some situations the NetScaler appliance is unable to correctly match the Accept-Encoding header in the client request with the Content-Encoding header in the response. The NetScaler appliance can assume that these headers match and mistakenly serve a hit. As a work-around, you can configure Integrated Caching policies to disallow serving hits to clients that do not have an appropriate Accept-Encoding header.

To enable Flash Cache by using the command line interface

At the command prompt, type:

set cache contentgroup <contentGroupName> -flashcache yes

To enable Flash Cache by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Content Groups.
2. In the details pane, click the content group for which you want to set the flash cache option, and then click Open.
3. In the Configure Cache Content Group dialog box, on the Others tab, under Flash Crowd and Prefetch, select the Flash Cache check box, and then click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set cache contentgroup

prefetch

The option to refresh an object immediately before it goes stale. Possible values: YES, NO Default value: YES

prefetchPeriod

The duration in seconds of the period during which prefetch should be attempted, immediately before the object's calculated expiry time. Default value: VAL_NOT_SET Maximum value: 4294967294

prefetchPeriodMilliSec

The duration in milliseconds of the period during which prefetch should be attempted, immediately before the calculated expiry time. Default value: VAL_NOT_SET Maximum value: 4294967290

prefetchMaxPending

The maximum number of outstanding prefetches on the contentgroup.

flashcache

The option to do flash cache on Integrated caching. Possible values: YES, NO Default value: NO

View description(s) in command reference Top

Caching a Response after a Client Halts a Download

You can set the Quick Abort parameter to continue caching a response, even if the client halts a request before the response is in the cache.

If the downloaded response size is less than or equal to the Quick Abort size, the NetScaler appliance stops downloading the response. If you set the Quick Abort parameter to 0, all downloads are halted.

To configure quick abort size by using the command line interface

At the command prompt, type:

set cache contentgroup <name> -quickAbortSize <integerInKBytes>

To configure quick abort size by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Content Groups.
2. In the details pane, click the content group for which you want to set the quick abort size, and then click Add.
3. In the Configure Cache Content Group dialog box, on the Memory tab, in the Quick Abort: Continue caching if more than text box, type an integer value, calculated in kilobytes (KB), and then click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set cache contentgroup

quickAbortSize

The quick abort size. If the client aborts when the downloaded response size is less than or equal to the quick-abort-size, then the Integrated Cache will stop downloading the response. Maximum value: 4194303

View description(s) in command reference Top

Setting a Minimum Number of Server Hits Prior to Caching

You can configure the minimum number of times that a response must be found on the origin server before it can be cached. You should consider increasing the minimum hits if the cache memory fills up quickly and has a lower-than-expected hit ratio.

The default value for the minimum number of hits is 0. This value caches the response after the first request.

To configure the minimum number of hits that are required before caching by using the command line interface

At the command prompt, type:

set cache contentgroup <name> -minhits <positiveInteger>

To configure the minimum number of hits that are required before caching by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Content Groups.
2. In the details pane, click the content group for which you want to set the minimum hit count, and then click Open.
3. On the Memory tab, in the Do not cache, if hits are less than text box, type the value you want to set, and then click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set cache contentgroup

minhits

The minimum number of accesses for an object to be stored in Cache.

View description(s) in command reference Top

Example of Performance Optimization

In this example, a client accesses a stock quote. Stock quotes are highly dynamic. You configure the integrated cache to serve the same stock quote to concurrent clients without sending multiple requests to the origin server. The stock quote expires after it is downloaded to all of the clients, and the next request for a quote for the same stock is fetched from the origin server. This ensures that the quote is always up to date.

The following task overview describes the steps to configure the cache for the stock quote application.

Task overview: Configuring caching for a stock quote application

1. Create a content group for stock quotes.

   For more information, see "About Content Groups."

   Configure the following for this content group:

   - On the Expiry Method tab, select the Expire after complete response received check box.

   - On the Others tab, select the Flash Cache check box, and click Create.
2. Add a cache policy to cache the stock quotes.

   For more information, see "Configuring a Policy in the Integrated Cache."

   Configure the following for the policy:

   - In the Action and Store in Group lists, select CACHE and select the group that you defined in the previous step.

   - Click Add, and in the Add Expression dialog box configure an expression that identifies stock quote requests, for example:

     ```
     http.req.url.contains("cgi-bin/stock-quote.pl")
     ```
3. Activate the policy.

   For more information, see "Globally Binding an Integrated Caching Policy." In this example, you bind this policy to request-time override processing and set the priority to a low value.

Configuring Cookies, Headers, and Polling

This section describes the procedures to configure how the cache manages cookies, HTTP headers, and origin server polling, including modifying default behavior that causes the cache to diverge from documented standards, overriding HTTP headers that might cause cacheable content to not be stored in the cache, and configuring the cache to always poll the origin for updated content under specialized circumstances.

Divergence of Cache Behavior from the Standards

By default, the integrated cache conforms to the following standards:

- RFC 2616, “Hypertext Transfer Protocol HTTP/1.1”
- The caching behaviors described in RFC 2617, “HTTP Authentication: Basic and Digest Access Authentication”
- The caching behavior described in RFC 2965, “HTTP State Management Mechanism”

The built-in policies and the Default content group attributes ensure conformance with most of these standards.

The default integrated cache behavior diverges from the specifications as follows:

- There is limited support for the Vary header.

  By default, any response containing a Vary header is considered to be non-cacheable unless it is compressed. A compressed response contains `Content-Encoding: gzip`, `Content-Encoding: deflate`, or `Content-Encoding: pack200-gzip` and is cacheable even if it contains the `Vary: Accept-Encoding` header.

- The integrated cache ignores the values of the headers `Cache-Control: no-cache` and `Cache-Control: private`.

  For example, a response that contains `Cache-Control: no-cache=”Set-Cookie”` is treated as if the response contained `Cache-Control: no-cache`. By default, the response is not cached.

- An image (Content-Type = image/*) is always considered cacheable even if an image response contains Set-Cookie or Set-Cookie2 headers, or if an image request contains a Cookie header.

  The integrated cache removes Set-Cookie and Set-Cookie2 headers from a response before caching it. This diverges from RFC 2965. You can configure RFC-compliant behavior as follows:

  ```
  add cache policy rfc_compliant_images_policy -rule "http.res.header.set-cookie2.exists || http.res.heac
  bind cache global rfc_compliant_images_policy -priority 100 -type REQ_OVERRIDE
  ```

- The following Cache-Control headers in a request force an RFC-compliant cache to reload a cached response from the origin server:

  ```
  Cache-control: max-age=0
  ```

Cache-control: no-cache

To guard against Denial of Service attacks, this behavior is not the default. For more information, see "Inserting a Cache-Control Header."

- By default, the caching module considers a response to be cacheable unless a response header states otherwise.

  To make this behavior RFC 2616 compliant, set -weakPosRelExpiry and -weakNegResExpiry to 0 for all content groups.

Removing Cookies from a Response

Cookies are often personalized for a user, and typically should not be cached. The Remove Response Cookies parameter removes Set-Cookie and Set-Cookie2 headers before caching a response. By default, the Remove Response Cookies option for a content group prevents caching of responses with Set-Cookie or Set-Cookie2 headers.

Note that when images are cached, the built-in behavior is to remove the Set-Cookie and Set-Cookie2 headers before caching, no matter how the content group is configured.

Note: Citrix recommends that you accept the default Remove Response Cookies for every content group that stores embedded responses, for example, images.

To configure Remove Response Cookies for a content group by using the command line interface

At the command prompt, type:

set cache contentgroup <name> -removeCookies YES

To configure Remove Response Cookies for a content group by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Content Groups.
2. In the details pane, click the content group for which you want to enable or disable the remove response cookies option, and then click Open.
3. In the Configure Cache Content Group, on the Others tab, under Settings, select or clear the Remove response cookies check box, and then click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set cache contentgroup

removeCookies

The option to remove cookies from response. Possible values: YES, NO Default value: YES

View description(s) in command reference Top

Inserting HTTP Headers at Response Time

The integrated cache can insert HTTP headers in responses that result from cache hits. The Citrix® NetScaler® appliance does not alter headers in responses that result from cache misses.

The following table describes headers that you can insert in a response.

Table 1. Different HTTP Headers You Can Insert in a Response That Is Served from the Cache

Header	Specifies
Age	Provides the age of the response in seconds, calculated from the time the response was generated at the origin server. By default, the cache inserts an Age header for every response that is served from the cache.
Via	Lists protocols and recipients between the start and end points for a request or a response. The NetScaler appliance inserts a Via header in every response that it serves from the cache. The default value of the inserted header is “NS-CACHE-9.2:last octet of the NetScaler IP address.” For more information, see "Configuring Global Attributes for Caching."
ETag	The cache supports response validation using Last-Modified and ETag headers to determine if a response is stale. The cache inserts an ETag in a response only if it caches the response and the origin server has not inserted its own ETag header. The ETag value is an arbitrary unique number. The ETag value for a response changes if it is refreshed from the origin server, but it stays the same if the server sends a 304 (object not updated) response. Origin servers typically do not generate validators for dynamic content because dynamic content is considered non-cacheable. You can override this behavior. With ETag header insertion, the cache is permitted to not serve full responses. Instead, the user agent is required to cache the dynamic response sent by the integrated cache the first time. To force a user agent to cache a response, you configure the integrated cache to insert an ETag header and replace the origin-provided Cache-Control header.

Cache-Control	The NetScaler appliance typically does not modify cacheability headers in responses that is serves from the origin server. If the origin server sends a response that is labeled as non-cacheable, the client treats the response as non-cacheable even if the NetScaler appliance caches the response. To cache dynamic responses in a user agent, you can replace Cache-Control headers from the origin server. This applies only to user agents and other intervening caches. They do not affect the integrated cache. For more information, see "Inserting a Cache-Control Header."

Inserting an Age, Via, or ETag Header

The following procedures describe how to insert Age, Via, and ETag headers.

To insert an Age, Via, or Etag header by using the command line interface

At the command prompt, type:

set cache contentgroup <name> -insertVia YES -insertAge YES -insertETag YES

To insert an Age, Via, or Etag header by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Content Groups.
2. In the details pane, click the content group for which you want to insert Age, Via, or Etag headers, and then click Open.
3. In the Configure Cache Content Group dialog box, on the Others tab, under HTTP Header Insertions, select or clear the Via, Age, or ETag check boxes, as needed. The values for the other header types are calculated automatically. Note that you configure the Via value in the main settings for the cache.
4. Click OK.

Inserting a Cache-Control Header

When the integrated cache replaces a Cache-Control header that the origin server inserted, it also replaces the Expires header. The new Expires header contains an expiration time in the past. This ensures that HTTP/1.0 clients and caches (that do not understand the Cache-Control header) do not cache the content.

To insert a Cache-Control header by using the command line interface

At the command prompt, type:

set cache contentgroup <name> -cacheControl <value>

To insert a Cache-Control header by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Content Groups.
2. In the details pane, click the content group for which you want to configure cache-control, and then click Open.
3. In the Configure Cache Content Group dialog box, on the Expiry Method tab, clear the heuristic and default expiry settings if any are set, and in the Expire content after text box, type a value in seconds. For example, a value of 3600 expires cached responses after 3600 seconds (one hour).
4. On the Others tab, under HTTP Header Insertions, in the Cache-Control text box, type the header you want to insert, for example, **private**, **max-age=0**, or click Configure and set the Cache-Control directives that you want to insert in responses that are sent to user agents and intervening caches.

Parameter Descriptions (of commands listed in the CLI procedure)

set cache contentgroup

name

The name of the content group whose attibutes will be changed.

insertVia

The option to insert a Via header. Possible values: YES, NO Default value: YES

insertAge

The option to insert an Age header. Possible values: YES, NO Default value: YES

insertETag

The option to insert an ETag header. Possible values: YES, NO Default value: YES

cacheControl

The option to insert a Cache-Control header.

View description(s) in command reference Top

Ignoring Cache-Control and Pragma Headers in Requests

By default, the caching module processes Cache-Control and Pragma headers. The following tokens in Cache-Control headers are processed as described in RFC 2616.

- max-age
- max-stale
- only-if-cached
- no-cache

A Pragma: no-cache header in a request is treated in the same way as a Cache-Control: no-cache header.

If you configure the caching module to ignore Cache-Control and Pragma headers, a request that contains a Cache-Control: No-Cache header causes the NetScaler appliance to retrieve the response from the origin server, but the cached response is not updated. If the caching module processes Cache-Control and Pragma headers, the cached response is refreshed.

The following table summarizes the implications of various settings for these headers and the Ignore Browser's Reload Request setting.

Table 1. Outcome of Settings for Ignoring Reload Requests, Cache-Control, and Pragma Headers

Setting for Ignore Cache-Control and Pragma Headers	Setting for Ignore Browser's Reload Request	Outcome
Yes	Yes or No	Ignore the Cache-Control and Pragma headers from the client, including the Cache-Control: no-cache directive.
No	Yes	The Cache-Control: no-cache header produces a cache miss, but a response that is already in the cache is not refreshed.
No	No	A request that contains a Cache-Control: no-cache header causes a cache miss and the stored response is refreshed.

To ignore Cache-Control and Pragma headers in a request by using the command line interface

At the command prompt, type:

set cache contentgroup <name> -ignoreReqCachingHdrs YES

To ignore browser reload requests by using the command line interface

At the command prompt, type:

set cache contentgroup <name> -ignoreReloadReq NO

Note that by default, the -ignoreReloadReq parameter is set to YES.

To ignore Cache-Control and Pragma headers in a request by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Content Groups.
2. In the details pane, click the content group for which you want to ignore cache-control and pragma headers, and then click Open.
3. In the Configure Cache Content Group dialog box, on the Others tab, under Settings, select the Ignore Cache-control and Pragma Headers in Requests check box, and then click OK.

Example of a Policy to Ignore Cache-Control Headers

In the following example, you configure a request-time override policy to cache responses that contain Content-type: image/* regardless of the Cache-Control header in the response.

To configure a request-time override policy to cache all responses with image/*

1. Flush the cache using the Invalidate All option.

   For more information, see "Flushing Responses in a Content Group."

2. Configure a new cache policy, and direct the policy to a particular content group. For more information, see "Configuring a Policy in the Integrated Cache."

3. Ensure the content group that the policy uses is configured to ignore Cache-Control headers, as described in "Ignoring Cache-Control and Pragma Headers in Requests."

4. Bind the policy to the request-time override policy bank.

   For more information, see "Globally Binding an Integrated Caching Policy."

Parameter Descriptions (of commands listed in the CLI procedure)

set cache contentgroup

name

The name of the content group whose attibutes will be changed.

ignoreReqCachingHdrs

The option to ignore the Cache-control and Pragma headers in the incoming request. Possible values: YES, NO Default value: YES

ignoreReloadReq

For a request, the option to force the system to reload a cached object from the origin. To guard against Denial of Service attacks, you should set this flag to YES. To get RFC-compliant behavior, you should set it to NO. Possible values: YES, NO Default value: YES

View description(s) in command reference Top

Polling the Origin Server Every Time a Request Is Received

You can configure the NetScaler appliance to always consult the origin server before serving a stored response. This is known as Poll Every Time (PET). When the NetScaler appliance consults the origin server and the PET response has not expired, a full response from the origin server does not overwrite cached content. This property is useful when serving client-specific content.

After a PET response expires, the NetScaler appliance refreshes it when the first full response arrives from the origin server.

The Poll Every Time (PET) function works as follows:

- For a cached response that has validators in the form of an ETag or a Last-Modified header, if the response expires it is automatically marked PET and cached.
- You can configure PET for a content group.

  If you configure a content group as PET, every response in the content group is marked PET. The PET content group can store responses that do not have validators. Responses that are automatically marked PET are always expired. Responses that belong to a PET content group can expire after a delay, based on how you configure the content group.

Two types of requests are affected by polling:

- **Conditional Requests**: A client issues a conditional request to ensure that the response that it has is the most recent copy.

  A user-agent request for a cached PET response is always converted to a conditional request and sent to the origin server. A conditional request has validators in If-Modified-Since or If-None-Match headers. The If-Modified-Since header contains the time from the Last-Modified header. An If-None-Match header contains the response's ETag header value.

  If the client's copy of the response is fresh, the origin server replies with 304 Not Modified. If the copy is stale, a conditional response generates a 200 OK that contains the entire response.
- **Non-Conditional Requests**: A non-conditional request can only generate a 200 OK that contains the entire response.

The following table summarizes response types based on the origin server's response

Table 1. How Responses Are Affected by Poll Every Time

Origin Server Response	Action

Send the full response	The origin server sends the response as-is to the client. If the cached response has expired, it is refreshed.
304 Not Modified	The following header values in the 304 response are merged with the cached response and the cached response is served to the client: · Date · Expires · Age · Cache-Control header Max-Age and S-Maxage tokens
401 Unauthorized 400 Bad Request 405 Method Not Allowed 406 Not Acceptable 407 Proxy Authentication Required	The origin's response is served as-is to the client. The cached response is not changed.
Any other error response, for example, 404 Not Found	The origin's response is served as-is to the client. The cached response is removed.

Note: The Poll Every Time parameter treats the affected responses as non-storable.

To configure poll every time by using the command line interface

At the command prompt, type:

add cache contentgroup <contentGroupName> -pollEveryTime YES

To configure poll every time by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Content Groups.
2. In the details pane, click a cache content group, and then click Open.
3. On the Others tab, click Poll every time (validate cached content with origin for every request).

PET and Client-Specific Content

The PET function can ensure that content is customized for a client. For example, a Web site that serves content in multiple languages examines the Accept-Language request header to select the language for the content that it is serving. For a multi-language Web site where English is the predominant language, all English language content can be cached in a PET content group. This ensures that every request goes to the origin server to determine the language for the response. If the response is English, and the content has not changed, the origin server can serve a 304 Not Modified to the cache.

The following example shows commands to cache English responses in a PET content group, configure a named expression that identifies English responses in the cache, and configure a policy that uses this content group and named expression. Bold is used for emphasis:

```
add cache contentgroup EnglishLanguageGroup -pollEveryTime YES
add expression containsENExpression –rule "http.res.header(\"Content-Language\").contains(\"en\")"
add cache policy englishPolicy -rule containsENExpression -action CACHE -storeInGroup englishLanguageGrou
bind cache policy englishPolicy -priority 100 -precedeDefRules NO
```

PET and Authentication, Authorization, and Auditing

Outlook Web Access (OWA) is a good example of dynamically generated content that benefits from PET. All mail responses (*.EML objects) have an ETag validator that enables them to be stored as PET responses.

Every request for a mail response travels to the origin server, even if the response is cached. The origin server determines whether the requestor is authenticated and authorized. It also verifies that the response exists in the origin server. If all results are positive, the origin server sends a 304 Not Modified response.

Parameter Descriptions (of commands listed in the CLI procedure)

add cache contentgroup

pollEveryTime

Use this parameter to specify whether to poll every time for the objects in this content group Possible values: YES, NO Default value: NO

View description(s) in command reference Top

Configuring the Integrated Cache as a Forward Proxy

The integrated cache can service as a forward proxy device that passes requests to other NetScaler appliances or to other types of cache servers. You configure the integrated cache as a forward proxy by identifying the IP addresses of the cache server or servers. After configuring the forward proxy, the NetScaler appliance sends requests that contain the configured IP address on to the cache server instead of involving the integrated cache.

To configure the NetScaler as a forward cache proxy by using the command line interface

At the command prompt, type:

add cache forwardProxy <IPAddress> <port>

To configure the NetScaler as a forward cache proxy by using the configuration utility

1. In the navigation pane, expand Integrated Caching, and then click Forward Proxy.
2. In the details pane, click Add.
3. Enter the IP address and port of the cache server, and then click Create.
4. Enter a second IP address and port, or click Close.

Parameter Descriptions (of commands listed in the CLI procedure)

add cache forwardProxy

IPAddress

The IP address of the forward proxy.

port

The port of the forward proxy. Minimum value: 1

View description(s) in command reference Top

Example of an Integrated Caching Configuration

The following task overview provides one method of setting up and testing an end-to-end configuration for integrated caching.

Task overview: an Integrated Caching configuration

1. Configure the load balancing virtual servers for your environment, and bind services to them.
2. Enable the integrated cache.
3. Check the expiration settings of the Default content group and ensure there is enough time for objects to remain in the cache.
4. Check the memory settings and ensure there is enough room to store cached objects.
5. Configure a caching policy that stores responses in the cache. The policy can be very general for ease of testing. For example, the following rule produces a hit for any GET request:

   ```
   http.req.method.eq(GET)
   ```

6. Open a browser and enter `http://your_load_balancing_virtual_ip_address/known_content_on_the_destination server`. For example, if you have a Web server that contains a top-level file named myfile.txt and a virtual server that services the Web server with an IP address of 22.222.22.22, you could enter the following URL:

   ```
   http://22.222.22.22/myfile.txt
   ```

7. In the configuration utility click Cache Objects, or at the command line enter `show cache object`. If the expected object does not appear in the cache, check for conflicting caching policies. You can also ping the named destination server where the object of interest resides to see whether the IP address is the same as the one that you configured as a service on your virtual server. Finally, you can look in the configuration utility under Integrated Caching, on the landing page for Policies, in the Hits column for the policy, to see if the Citrix® NetScaler® appliance did use the intended policy to evaluate the request for the cached object.

The following is an example of a test configuration. The service IP address corresponds to a valid destination on the internet, and the load balancing virtual server IP address corresponds to a valid IP address in your network. You would send a browser request to the IP address for the virtual server:

```
enable ns feature lb ic
add service myTestService 11.111.11.11 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO
```

```
add lb vserver myTestLBVserver HTTP 10.100.10.10 80 -persistenceType NONE -cltTimeout 180
bind lb vserver myTestLBVserver myTestService
add cache policy myCachePolicy -rule "http.req.method.eq(\"GET\")" -action cache
bind cache global myCachePolicy -priority 1 -type req_override
```

Parameter Descriptions (of commands listed in the CLI procedure)

show cache object

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Default Settings for the Integrated Cache

The Citrix NetScaler integrated cache feature provides built-in policies with default settings as well as initial settings for the Default content group. The information in this section defines the parameters for the built-in policies and Default content group.

Default Caching Policies

The integrated cache has built-in policies. The NetScaler appliance evaluates the policies in a particular order, as discussed in the following sections.

You can override these built-in policies with a user-defined policy that is bound to a request-time override or response-time override policy bank.

Note that if you configured policies prior to release 9.0 and specified the -precedeDefRules parameter when binding the policies, they are automatically assigned to override-time bind points during migration.

Viewing the Default Policies

The built-in policy names start with an underscore (_). You can view the built-in policies from the command line and the administrative console using the show cache policy command.

Default Request Policies

You can override the following built-in request time policies by configuring new policies and binding them to the request-time override processing point. In the following policies, note that the MAY_NOCACHE action stipulates that the transaction is cached only when there is a user-configured or built-in CACHE directive at response time.

The following policies are bound to the _reqBuiltinDefaults policy label. They are listed in priority order.

1. Do not cache a response for a request that uses any method other than GET.

   The policy name is **_nonGetReq**. The following is the policy rule:

   ```
   !HTTP.REQ.METHOD.eq(GET)
   ```

2. Set a NOCACHE action for a request with header value that contains If-Match or If-Unmodified-Since.

   The policy name is **_advancedConditionalReq**. The following is the policy rule:

   ```
   HTTP.REQ.HEADER("If-Match").EXISTS ||
   HTTP.REQ.HEADER("If-Unmodified-Since").EXISTS
   ```

3. Set a MAY_NOCACHE action for a request with the following header values: Cookie, Authorization, Proxy-authorization or a request which contains the NTLM or Negotiate header.

   The policy name is **_personalizedReq**. The following is the policy rule:

```
HTTP.REQ.HEADER("Cookie").EXISTS ||
HTTP.REQ.HEADER("Authorization").EXISTS ||
HTTP.REQ.HEADER("Proxy-Authorization").EXISTS ||
HTTP.REQ.IS_NTLM_OR_NEGOTIATE
```

Default Response Policies

You can override the following default response-time policies by configuring new policies and binding them to the response-time override processing point.

The following policies are bound to the **_resBuiltinDefaults** policy label and are evaluated in the order in which they are listed:

1. Do not cache HTTP responses unless they are of type 200, 304, 307, 203 or if the types are between 400 and 499 or between 300 and 302.

   The policy name is **_uncacheableStatusRes**. The following is the policy rule:

   ```
   !((HTTP.RES.STATUS.EQ(200)) || (HTTP.RES.STATUS.EQ(304)) ||
   (HTTP.RES.STATUS.BETWEEN(400,499)) ||
   (HTTP.RES.STATUS.BETWEEN(300, 302)) || (HTTP.RES.STATUS.EQ(307))||
   (HTTP.RES.STATUS.EQ(203)))
   ```

2. Do not cache an HTTP response if it has a Vary header with a value of anything other than Accept-Encoding.

   The compression module inserts the Vary: Accept_Encoding header. The name of this expression is **_uncacheableVaryRes**. The following is the policy rule:

   ```
   ((HTTP.RES.HEADER("Vary").EXISTS) &&
   ((HTTP.RES.HEADER("Vary").INSTANCE(1).LENGTH > 0) || (!HTTP.RES.HE
   ADER("Vary").STRIP_END_WS.SET_TEXT_MODE(IGNORECASE).eq("Accept-Enc
   oding"))))
   ```

3. Do not cache a response if its Cache-Control header value is No-Cache, No-Store, or Private, or if the Cache-Control header is not valid.

   The policy name is **_uncacheableCacheControlRes**. The following is the policy rule:

   ```
   ((HTTP.RES.CACHE_CONTROL.IS_PRIVATE) ||
   (HTTP.RES.CACHE_CONTROL.IS_NO_CACHE) ||
   (HTTP.RES.CACHE_CONTROL.IS_NO_STORE) ||
   (HTTP.RES.CACHE_CONTROL.IS_INVALID))
   ```

4. Cache responses if the Cache-Control header has one of the following values: Public, Must-Revalidate, Proxy-Revalidate, Max-Age, S-Maxage.

   The policy name is **_cacheableCacheControlRes**. The following is the policy rule:

   ```
   ((HTTP.RES.CACHE_CONTROL.IS_PUBLIC) ||
   (HTTP.RES.CACHE_CONTROL.IS_MAX_AGE) ||
   (HTTP.RES.CACHE_CONTROL.IS_MUST_REVALIDATE) ||
   (HTTP.RES.CACHE_CONTROL.IS_PROXY_REVALIDATE) ||
   (HTTP.RES.CACHE_CONTROL.IS_S_MAXAGE))
   ```

5. Do not cache responses that contain a Pragma header.

   The name of the policy is **_uncacheablePragmaRes**. The following is the policy rule:

   ```
   HTTP.RES.HEADER("Pragma").EXISTS
   ```

6. Cache responses that contain an Expires header.

   The name of the policy is **_cacheableExpiryRes**. The following is the policy rule:

   ```
   HTTP.RES.HEADER("Expires").EXISTS
   ```

7. If the response contains a Content-Type header with a value of Image, remove any cookies in the header and cache it.

   The name of the policy is **_imageRes**. The following is the policy rule:

   ```
   HTTP.RES.HEADER("Content-Type").SET_TEXT_MODE(IGNORECASE).STARTSWI
   TH("image/")
   ```

   You could configure the following content group to work with this policy:

   ```
   add cache contentgroup nocookie_group -removeCookies YES
   ```

8. Do not cache a response that contains a Set-Cookie header.

   The name of the policy is **_ personalizedRes**. The following is the policy rule:

   ```
   HTTP.RES.HEADER("Set-Cookie").EXISTS ||
   HTTP.RES.HEADER("Set-Cookie2").EXISTS
   ```

Restrictions on Default Policies

You cannot override the following built-in request time policies with user-defined policies.

These policies are listed in priority order.

1. Do not cache any responses if the corresponding HTTP request lacks a GET or POST method.

2. Do not cache any responses for a request if the HTTP request URL length plus host name exceeds 1744 byes.

3. Do not cache a response for a request that contains an If-Match header.

4. Do not cache a request that contains an If-Unmodified-Since header.

   Note that this is different from the If-Modified-Since header.

5. Do not cache a response if the server does not set an expiry header.

You cannot override the following built-in response time policies. These policies are evaluated in the order in which they are listed:

1. Do not cache responses that have an HTTP response status code of 201, 202, 204, 205, or 206.

2. Do not cache responses that have an HTTP response status code of 4xx, with the exceptions of status codes 403, 404, and 410.

3. Do not cache responses if the response type is FIN terminated, or the response does not have one of the following attributes: Content-Length, or Transfer-Encoding: Chunked.

4. Do not cache the response if the caching module cannot parse its Cache-Control header.

Initial Settings for the Default Content Group

When you first enable integrated caching, the NetScaler appliance provides one predefined content group named the Default content group. The following table shows the settings for this group.

Table 1. Predefined Settings for the Default Content Group

Parameter	Description	Default Value
Hit parameters	The hit parameters contain the parameter names that are significant for generating a response. In parameterized hit selection, NetScaler appliance matches the URL stem byte-for-byte, matches normalized values of the hit parameters, and matches the target service information.	none
Invalidation Parameters	These parameters mark a cached object as obsolete during parameterized selection. Specific objects, or all objects in a content group, are selected if the values of the invalidation parameters in the object and in the request are same after normalization. The invalidation parameters are a subset of the hit parameters.	none
Poll Every Time	Poll every time for the objects in this content group.	NO

Ignore reload request	Specifies whether a request can force the system to reload a cached object from the origin. To guard against Denial of Service attacks, you must set this flag to YES. To get RFC-compliant behavior you should set it to NO.	YES
Remove Response Cookies	If this option is disabled for a content group, and if the response contains cookies, the cookies are stored and served with every cache hit. By default, the remove cookies option is enabled for a content group, to prevent the integrated cache from storing any responses with Set-Cookie or Set-Cookie2 headers unless the response is an image.	YES
Prefetch	The Prefetch option refreshes an object when it is about to expire. This ensures that the object remains stale or inactive (and therefore it cannot be served) for a shorter duration of time.	YES
Prefetch period	This duration in seconds during which prefetch should be attempted, immediately before the object's calculated expiry time.	heuristic
Maximum outstanding prefetches	The number of items that can be subjected to a prefetch at a time.	4294967295
Flashcache	Determines whether to enable queuing of client requests and simultaneous distribution of responses to all clients in the queue.	NO
Expire at last byte	Determines whether to expire a cached response immediately after serving it.	NO

Insert Via header	Defines a string to be inserted in a Via header. By default, a Via header is inserted in all responses served from a content group. The Via header is not inserted for responses that are served by the origin server.	YES
Insert Age header	The Age header contains information about the age of the object in seconds as calculated by the integrated cache.	YES
Insert ETag header	With ETag header insertion, the integrated cache does not serve full responses on repeat requests. This is done by forcing the user agent to cache the dynamic response sent by the cache the first time.	YES
Cache-control header	You can enable caching of dynamic objects in the user agent by replacing the Cache-Control headers that are inserted by the origin server. You must configure the new Cache-Control header to be inserted in the content group.	NONE
Quick abort size	If the size of an object that is being downloaded is less than or equal to the quick abort value, and a client aborts during the download, the cache stops downloading the response. If the object is larger than the quick abort size, the cache continues to download the response.	4194303 KBytes (maximum)
Minimum Response Size	You can control memory use by setting a minimum response size. Cached objects must be larger than the minimum response size.	0 KBytes

Maximum Response Size	You can control memory use by setting a maximum response size. Cached objects must be smaller than the maximum response size.	80 KBytes
Memory usage limit	Sets the maximum amount of memory that the cache can use. The effective limit is based on the available memory of the NetScaler appliance. The minimum value is 0 and the maximum value is unlimited.	UNLIMITED
Ignore caching headers in request	Disregards Cache-Control and Pragma headers in HTTP requests.	YES
MinHits configured	Number of hits that are required to qualify a response for storage in this content group.	0
Always evaluate policies		NO
Pinned	By default, when the cache is full the NetScaler appliance replaces the least recently used response first. The NetScaler appliance does not apply this behavior to content groups that are marked as pinned.	NO
Lazy DNS resolution	If set to YES, DNS resolution is performed for responses only if the destination IP address in the request does not match the destination IP address of the cached response.	YES

TCP Buffering

The TCP buffering feature improves the performance of a transaction management environment by adding a speed-matching mechanism between a fast server network and a slow client network and buffering a server's response before delivering it to the client at the client's speed. The server can quickly offload the requested data and then devote its resources to other tasks. Any required retransmission of packets from a server to a client is also done by the Citrix® NetScaler® appliance.

TCP buffering is bypassed for some NetScaler features, including SSL, compression, and caching, because these features perform their own type of buffering. However, TCP buffering is performed for non-compressible and non-cacheable responses from the server, even when compression and caching are enabled. TCP buffering is also skipped for small responses that can fit in a single packet.

You enable or disable the TCP buffering feature globally and on a per-service basis. You can also set the size and memory limit of the buffer.

Note: This content is best understood if you are familiar with creating services and binding them to vservers. For more information, see "Creating a Service" and "Binding Services to a Virtual Server."

Enabling or Disabling TCP Buffering Globally

TCP buffering is disabled on the appliance by default. When you enable TCP buffering globally, all new services are enabled for TCP buffering by default.

To enable or disable the TCP buffering mode globally by using the command line interface

At the command prompt, type one of the following commands:

- enable ns mode TCPB
- disable ns mode TCPB

To enable or disable the TCP buffering mode globally by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under the Modes and Features group, click Configure modes.
3. In the Configure Modes dialog box, select or clear the TCP Buffering check box.
4. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns mode

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable ns mode

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Enabling or Disabling TCP Buffering for a Service

You can enable or disable TCP buffering at the service level.

Note: Service level settings take precedence over the global settings.

To enable or disable the TCP buffering mode for a service by using the command line interface

At the command prompt, type:

set service <name>@ -TCPB (YES | NO)

To enable or disable the TCP buffering mode for a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click the service for which you want to enable or disable TCP buffering, and then click Open.
3. In the Configure Service dialog box, on the Advanced tab, under Settings, select or clear the TCP Buffering check box.
4. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set service

TCPB

The state of the TCP Buffering feature for this service. Possible values: YES, NO

View description(s) in command reference Top

Setting TCP Buffering Parameters

You can configure two TCP buffering parameters: buffer size and memory usage limit. For best performance, set the connection buffer size so that most responses can fit in the TCP buffer. If integrated caching is not enabled, to provide maximum buffering capacity, increase the memory usage limit to up to half the total system memory.

To set TCP buffering parameters by using the command line interface

At the command prompt, type:

set ns tcpbufParam -size <positiveInteger> -memLimit <positiveInteger>

To set TCP buffering parameters by using the configuration utility

1. Navigate to System > Settings.
2. In the details pane, under Settings, click Change TCP parameters.
3. In the Configure TCP Parameters dialog box, under TCP Buffering, in the Buffer Size (KBytes) text box, type the size of the TCP buffer you want to set, for example, 128.
4. In the Memory Usage Limit (MBytes) text box, type the maximum memory size that you want to use for buffering, for example, 128.
5. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set ns tcpbufParam

size

The size (in KBytes) of the TCP buffer per connection. Default value: 64 Minimum value: 4 Maximum value: 20480

memLimit

The maximum memory that can be used for buffering, in megabytes. Default value: 64

View description(s) in command reference Top

TCP Keep-Alive

The TCP keep-alive feature monitors TCP connection to verify if the peers are up. It sends keep-alive probes at regular intervals to each peer. A peer that acknowledges the probes, is considered to be UP. A peer that does not respond after a specified number of attempts, is considered to be DOWN. By default, the NetScaler appliance does not send keep-alive probes for TCP connections. You can enable the appliance to send TCP keep-alive probes to the peer connections by using the command-line interface or configuration utility.

Note: TCP keep-alive is configured through the set ns tcpProfile command and is not the same as the Client keep-alive. Client keep-alive applies to HTTP and HTTPS applications, and needs no additional configuration. TCP keep-alive is configurable and can be applied to any service using TCP transport, including HTTP and HTTPS.

Configuring Keep-Alive in TCP Profiles

A TCP profile is a collection of configuration settings used to control TCP requests to and responses from virtual servers on a NetScaler appliance. You can use the TCP profile to enable the NetScaler appliance to send TCP keep-alives to the client and server connections. By default, NetScaler does not send keep-alives for TCP connections. You can enable NetScaler appliance to send TCP keep-alive probes to the peer connections by using the command-line interface or configuration utility.

When TCP keep-alive feature is enabled, with the default settings, the appliance probes any TCP connection that has been idle for 15 minutes. If the appliance does not receive a response from the peer within 75 seconds, it sends a second probe. If no response to that probe is received within 75 seconds, the appliance sends a third, final probe. If no response to the final probe is received within 75 seconds, the appliance resets the connection.

By default, this feature is disabled. In addition to enabling the keep-alive feature, you can change the default values for connection idle time, number of probes to send to the peer, and the interval at which to send probes.

In the CLI, use the following command to change the default settings:

set ns tcpProfile <name> [-KA ENABLED] [-KAconnIdleTime <positive_integer>] [-KAmaxProbes <positive_integer>] [-KAprobeInterval <positive_integer>].

In the configuration utility, you can change the settings in the System > Profiles > TCP Profiles >Add TCP Profile or Configure TCP Profile dialog box.

For more information about TCP Profiles, see "Configuring TCP Profiles."

When you configure the TCP profile on a virtual server or service, if the idle time-out of the virtual server or service is less than the keep-alive connection idle time, then the connection might be closed at the idle time-out of the virtual server, even before a keep-alive probe can be sent. Make sure that the idle time-out is not lower than keep-alive connection idle time.

By default, Netscaler will does not close a connection that is responding to keep-alive probes. That can be a security concern. If you would like to close a connection after some time, irrespective of keep-alive status, you can perform the following configuration:

1. Set the idle time-out of the virtual server or service to the maximum time that you want the connection to be open.

2. Set the KAprobeUpdateLastActivity parameter to DISABLED by using the set ns tcpProfile command.

This will ignore keep-alive activity on the connection, and close the connection at time-out value, as if it were idle.

Parameter Descriptions (of commands listed in the CLI procedure)

set ns tcpProfile

name

Name of the TCP profile

KA

Send periodic TCP keep-alive probes to check if peer is still up Possible values: ENABLED, DISABLED Default value: DISABLED

KAconnIdleTime

How long the connection should be idle, in seconds, before sending a keep-alive probe Default value: NSTCP_KA_DEFAULT_CONN_IDLETIME Minimum value: 1 Maximum value: 4095

KAmaxProbes

How many keep-alive probes to send, when not acknowledged, before assuming peer to be down Default value: NSTCP_KA_DEFAULT_PROBE_COUNT Minimum value: 1 Maximum value: 255

KAprobeInterval

Time interval (seconds) before the next probe, if peer does not respond Default value: NSTCP_KA_DEFAULT_INTERVAL Minimum value: 1 Maximum value: 4095

View description(s) in command reference Top

System

2015-05-17 05:02:26 UTC

Contents

System

The following topics provide information of the NetScaler system.

Administration	Manages and monitors the NetScaler appliance by using built-in features such as authentication and authorization, SNMP management, audit logging, web server logging, NTP management, and Reporting tool.
AppFlow	Provides information about the reporting capabilities of AppFlow feature of the NetScaler.
AutoScale	Describes how users of Citrix® CloudPlatform can use the AutoScale feature on the NetScaler appliance to enable automatic scaling of their applications.
CloudBridge	Provides help in reducing the cost of moving your applications to the cloud, reduce the risk of application failure, and increase network efficiency in your cloud environment.
Clustering	A setup of multiple nCore NetScaler appliances that ensure high availability, high throughput, and scalability of a deployment of NetScaler appliances.
EdgeSight Monitoring for NetScaler	Monitors the end-user experience with web applications that are served in a NetScaler environment.
Flex Tenancy	A methodology that allows you to tune a group of NetScaler VPX instances to the unique characteristics and needs of individual applications in a complex Web 2.0 setup.
High Availability	A setup of two NetScaler appliances that ensure the high availability of NetScaler appliances.
Networking	Provides information for configuring the various networking components on the NetScaler appliance.
Web Interface	Provides access to Citrix® XenApp™ and Citrix® XenDesktop® applications.

Administration

The following topics provide a conceptual reference and instructions for managing and monitoring the Citrix NetScaler appliance by using built-in features, such as command policies, Simple Network Management (SNMP), audit logging, web server logging, Network Time Protocol (NTP), and the Reporting tool.

Authentication and Authorization	Configure authentication and authorization to manage access to the NetScaler and different parts of the NetScaler configuration.
SNMP	Learn how SNMP works with NetScaler and how to configure SNMP V1, V2, and V3 on NetScaler.
Audit Logging	Configure the NetScaler audit server log to log and monitor the NetScaler states and status information. Also, learn how to configure audit server logging on a server system and for a deployment scenario.
Web Server Logging	Configure web server log to maintain a history of the page requests that originate from the NetScaler.
Advanced Configurations	Learn how to set advanced configurations, such as NTP, PMTU, and auto detected services, on the NetScaler.
Reporting Tool	Learn how to use the Reporting tool to view performance statistics as reports with graphs that are based on statistics collected by the nscollect utility.

Administration

The following topics provide a conceptual reference and instructions for managing and monitoring the Citrix NetScaler appliance by using built-in features, such as command policies, Simple Network Management (SNMP), audit logging, web server logging, Network Time Protocol (NTP), and the Reporting tool.

Authentication and Authorization	Configure authentication and authorization to manage access to the NetScaler and different parts of the NetScaler configuration.
SNMP	Learn how SNMP works with NetScaler and how to configure SNMP V1, V2, and V3 on NetScaler.
Audit Logging	Configure the NetScaler audit server log to log and monitor the NetScaler states and status information. Also, learn how to configure audit server logging on a server system and for a deployment scenario.
Web Server Logging	Configure web server log to maintain a history of the page requests that originate from the NetScaler.
Advanced Configurations	Learn how to set advanced configurations, such as NTP, PMTU, and auto detected services, on the NetScaler.
Reporting Tool	Learn how to use the Reporting tool to view performance statistics as reports with graphs that are based on statistics collected by the nscollect utility.

Authentication and Authorization

To configure NetScaler authentication and authorization, you must first define the users who have access to the NetScaler appliance, and then you can organize these users into groups. After configuring users and groups, you need to configure command policies to define types of access, and assign the policies to users and/or groups.

You must log on as an administrator to configure users, groups, and command policies. The default NetScaler administrator user name is *nsroot*. After logging on as the default administrator, you should change the password for the nsroot account. Once you have changed the password, no user can access the NetScaler appliance until you create an account for that user. If you forget the administrator password after changing it from the default, you can reset it to nsroot.

Configuring Users and Groups

You must define your users by configuring accounts for them. To simplify the management of user accounts, you can organize them into groups.

You can also customize the command-line prompt for a user. Prompts can be defined in a user’s configuration, in a user-group configuration, and in the global configuration. The prompt displayed for a given user is determined by the following order of precedence:

1. Display the prompt as defined in the user's configuration.
2. Display the prompt as defined in the group configuration for the user’s group.
3. Display the prompt as defined in the system global configuration.

You can now specify a time-out value for inactive CLI sessions for a system user. If a user's CLI session is idle for a time that exceeds the time-out value, the NetScaler appliance terminates the connection. The timeout can be defined in a user’s configuration, in a user-group configuration, and in the global configuration. The time-out for inactive CLI sessions for a user is determined by the following order of precedence:

1. Time-out value as defined in the user's configuration.
2. Time-out value as defined in the group configuration for the user’s group.
3. Time-out value as defined in the system global configuration.

Configuring User Accounts

To configure user accounts, you simply specify user names and passwords. You can change passwords and remove user accounts at any time.

To create a user account by using the command line interface

At the command prompt, type the following commands to create a user account and verify the configuration:

- add system user <userName> [-promptString <string>] [-timeout <secs>]
- show system user <userName>

Example

> add system user johnd -promptString user-%u-at-%T

Enter password:
Confirm password:

To configure a user account by using the configuration utility

Navigate to System > Users, create the user.

Parameter Descriptions (of commands listed in the CLI procedure)

add system user

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show system user

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring User Groups

After configuring a user group, you can easily grant the same access rights to everyone in the group. To configure a group, you create the group and bind users to the group. You can bind each user account to more than one group. Binding user accounts to multiple groups may allow more flexibility when applying command policies.

To create a user group by using the command line interface

At the command prompt, type the following commands to create a user group and verify the configuration:

- add system group <groupName> [-promptString <string>] [-timeout <secs>]
- show system group <groupName>

Example

> add system group Managers -promptString Group-Managers-at-%h

To bind a user to a group by using the command line interface

At the command prompt, type the following commands to bind a user account to a group and verify the configuration:

- bind system group <groupName> -userName <userName>
- show system group <groupName>

Example

> bind system group Managers -userName user1

To configure a user group by using the configuration utility

Navigate to System > Groups, add create the group.

Note: To add members to the group, under the Members section, click Add. Select users from the Available list and add them to the Configured list.

Parameter Descriptions (of commands listed in the CLI procedure)

add system group

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show system group

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind system group

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Command Policies

Command policies regulate which commands, command groups, vservers, and other entities that users and user groups are permitted to use.

The appliance provides a set of built-in command policies, and you can configure custom policies. To apply the policies, you bind them to users and/or groups.

Here are the key points to keep in mind when defining and applying command policies.

- You cannot create global command policies. Command policies must be bound directly to the users and groups on the appliance.
- Users or groups with no associated command policies are subject to the default (DENY-ALL) command policy, and are therefore unable to execute any configuration commands until the proper command policies are bound to their accounts.
- All users inherit the policies of the groups to which they belong.
- You must assign a priority to a command policy when you bind it to a user account or group account. This enables the appliance to determine which policy has priority when two or more conflicting policies apply to the same user or group.
- The following commands are available by default to any user and are unaffected by any command you specify:

  help, show cli attribute, set cli prompt, clear cli prompt, show cli prompt, alias, unalias, history, quit, exit, whoami, config, set cli mode, unset cli mode, and show cli mode.

Built-in Command Policies

The following table describes the built-in policies.

Table 1. Built-in Command Policies

Policy name	Allows
read-only	Read-only access to all show commands except show ns runningConfig, show ns ns.conf, and the show commands for the NetScaler command group.
operator	Read-only access and access to commands to enable and disable services and servers.
network	Full access, except to the set and unset SSL commands, show ns ns.conf, show ns runningConfig, and show gslb runningConfig commands.

superuser	Full access. Same privileges as the nsroot user.

Creating Custom Command Policies

Regular expression support is offered for users with the resources to maintain more customized expressions, and for those deployments that require the flexibility that regular expressions offer. For most users, the built-in command policies are sufficient. Users who need additional levels of control but are unfamiliar with regular expressions may want to use only simple expressions, such as those in the examples provided in this section, to maintain policy readability.

When you use a regular expression to create a command policy, keep the following in mind.

- When you use regular expressions to define commands that will be affected by a command policy, you must enclose the commands in double quotation marks. For example, to create a command policy that includes all commands that begin with *show*, type the following:

  ```
  "^show .*$"
  ```

  To create a command policy that includes all commands that begin with *rm*, type the following:

  ```
  "^rm .*$"
  ```

- Regular expressions used in command policies are not case sensitive.

The following table lists examples of regular expressions:

Table 2. Examples of Regular Expressions for Command Policies

Command specification	Matches these commands
"^rm\s+.*$"	All remove actions, because all remove actions begin with the *rm* string, followed by a space and additional parameters and flags.
"^show\s+.*$"	All show commands, because all show actions begin with the *show* string, followed by a space and additional parameters and flags.
"^shell$"	The shell command alone, but not combined with any other parameters or flags.
"^add\s+vserver\s+.*$"	All create vserver actions, which consist of the *add vserver* command followed by a space and additional parameters and flags.
"^add\s+(lb\s+vserver)\s+.*"	All create lb vserver actions, which consist of the add lb vserver command followed by a space and additional parameters and flags.

The following table shows the command specifications for each of the built-in command policies.

Table 3. Expressions Used in the Built-in Command Policies

Policy name	Command specification regular expression
read-only	(^man.*)|(^show\s+(?!system)(?!configstatus)(?!ns ns\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gslb runningConfig)(?!audit messages)(?!techsupport).*)|(^stat.*)
operator	(^man.*)|(^show\s+(?!system)(?!configstatus)(?!ns ns\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gslb runningConfig)(?!audit messages)(?!techsupport).*)|(^stat.*)|(^(enable|disable) (server|service).*)
network	^(?!clear ns config.*)(?!scp.*)(?!set ssl fips)(?!reset ssl fips)(?!diff ns config)(?!shell)(?!reboot)(?!batch)\S+\s+(?!system)(?!configstatus)(?!ns ns\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gslb runningConfig)(?!techsupport).*
superuser	.*

To create a command policy by using the command line interface

At the command prompt, type the following commands to create a command policy and verify the configuration:

- add system cmdPolicy <policyname> <action> <cmdspec>
- show system cmdPolicy <policyName>

Example

> add system cmdPolicy read_all ALLOW (^show\s+(!system)(!ns ns.conf)(!ns runningConfig).*)|(^stat.*)

To configure a command policy by using the configuration utility

Navigate to System > Command Policies, and create the command policy.

Binding Command Policies to Users and Groups

Once you have defined your command policies, you must bind them to the appropriate user accounts and groups. When you bind a policy, you must assign it a priority so that the appliance can determine which command policy to follow when two or more applicable command policies are in conflict.

Command policies are evaluated in the following order:

- Command policies bound directly to users and the corresponding groups are evaluated according to priority number. A command policy with a lower priority number is evaluated before one with a higher priority number. Therefore, any privileges the lower-numbered command policy explicitly grants or denies are not overridden by a higher-numbered command policy.
- When two command policies, one bound to a user account and other to a group, have the same priority number, the command policy bound directly to the user account is evaluated first.

To bind command policies to a user by using the command line interface

At the command prompt, type the following commands to bind a command policy to a user and verify the configuration:

- bind system user <userName> -policyName <policyName> <priority>
- show system user <userName>

Example

> bind system user user1 -policyName read_all 1

To bind command policies to a user by using the configuration utility

Navigate to System > Users, select the user and bind command policies. Optionally, you can modify the default priority to ensure that the policy is evaluated in the proper order.

To bind command policies to a group by using the command line interface

At the command prompt, type the following commands to bind a command policy to a user group and verify the configuration:

- bind system group <groupName> -policyName <policyName> <priority>
- show system group <groupName>

Example

> bind system group Managers -policyName read_all 1

To bind command policies to a group by using the configuration utility

Navigate to System > Groups, select the group and bind command policies. Optionally, you can modify the default priority to ensure that the policy is evaluated in the proper order.

Parameter Descriptions (of commands listed in the CLI procedure)

help

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add system cmdPolicy

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show system cmdPolicy

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind system user

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show system user

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind system group

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show system group

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Resetting the Default Administrator (nsroot) Password

The nsroot account provides complete access to all features of the appliance. Therefore, to preserve security, the nsroot account should be used only when necessary, and only individuals whose duties require full access should know the password for the nsroot account. Frequently changing the nsroot password is advisable. If you lose the password, you can reset it to the default and then change it.

To reset the nsroot password, you must boot the appliance into single user mode, mount the file systems in read/write mode, and remove the set NetScaler user nsroot entry from the ns.conf file. You can then reboot, log on with the default password, and choose a new password.

To reset the nsroot password

1. Connect a computer to the console port of the NetScaler ADC and log on.

   Note: You cannot log on by using SSH to perform this procedure; you must connect directly to the appliance.

2. Reboot the NetScaler ADC.

3. Press CTRL+C when the following message appears:

   ```
   Press [Ctrl-C] for command prompt, or any other key to boot
   immediately.

   Booting [kernel] in # seconds.
   ```

4. Run the following command to start the NetScaler in a single user mode:

   boot -s

   Note: If boot -s does not work, then try reboot -- -s and appliance will reboot in single user mode.

   After the appliance boots, it displays the following message:

   ```
   Enter full path name of shell or RETURN for /bin/sh:
   ```

5. Press ENTER key to display the # prompt, and type the following commands to mount the file systems:

   a. Run the following command to check the disk consistency:

      fsck /dev/ad0s1a

      Note: Your flash drive will have a specific device name depending on your NetScaler; hence, you have to replace ad0s1a in the preceding command with the appropriate device name.

   b. Run the following command to display the mounted partitions:

      df

      If the flash partition is not listed, you need to mount it manually.

   c. Run the following command to mount the flash drive:

      mount /dev/ad0s1a /flash

6. Run the following command to change to the nsconfig directory:

   cd /flash/nsconfig

7. Run the following commands to rewrite the `ns.conf` file and remove the set of system commands defaulting to the nsroot user:

a. Run the following command to create a new configuration file that does not have commands defaulting to the nsroot user:

   grep –v “set system user nsroot” ns.conf > new.conf

b. Run the following command to make a backup of the existing configuration file:

   mv ns.conf old.ns.conf

c. Run the following command to rename the new.conf file to ns.conf:

   mv new.conf ns.conf

8. Run the following command to reboot the NetScaler:

   reboot

9. Log on using the default nsroot user credentials.

10. Run the following command to reset the nsroot user password:

    set system user nsroot <New_Password>

Example of a User Scenario

The following example shows how to create a complete set of user accounts, groups, and command policies and bind each policy to the appropriate groups and users. The company, Example Manufacturing, Inc., has three users who can access the NetScaler appliance:

- **John Doe.** The IT manager. John needs to be able to see all parts of the NetScaler configuration but does not need to modify anything.
- **Maria Ramiez.** The lead IT administrator. Maria needs to be able to see and modify all parts of the NetScaler configuration except for NetScaler commands (which local policy dictates must be performed while logged on as nsroot).
- **Michael Baldrock.** The IT administrator in charge of load balancing. Michael needs to be able to see all parts of the NetScaler configuration, but needs to modify only the load balancing functions.

The following table shows the breakdown of network information, user account names, group names, and command policies for the sample company.

Table 1. Sample Values for Creating Entities

Field	Value	Note
NetScaler host name	ns01.example.net	N/A
User accounts	johnd, mariar, and michaelb	John Doe, IT manager, Maria Ramirez, IT administrator and Michael Baldrock, IT administrator.
Groups	Managers and SysOps	All managers and all IT administrators.
Command Policies	read_all, modify_lb, and modify_all	Allow complete read-only access, Allow modify access to load balancing, and Allow complete modify access.

The following description walks you through the process of creating a complete set of user accounts, groups, and command policies on the NetScaler appliance named ns01.example.net.

The description includes procedures for binding the appropriate user accounts and groups to one another, and binding appropriate command policies to the user accounts and groups.

This example illustrates how you can use prioritization to grant precise access and privileges to each user in the IT department.

The example assumes that initial installation and configuration have already been performed on the NetScaler.

Configuration steps

1. Use the procedure described in "Configuring User Accounts" to create user accounts **johnd**, **mariar**, and **michaelb**.

2. Use the procedure described in "Configuring User Groups" to create user groups **Managers** and **SysOps**, and then bind the users **mariar** and **michaelb** to the **SysOps** group and the user **johnd** to the **Managers** group.

3. Use the procedure described in "Creating Custom Command Policies" to create the following command policies:

   - **read_all** with action **Allow** and command spec "(^show\s+(?!system)(?!ns ns.conf)(?!ns runningConfig).*)|(^stat.*)"

   - **modify_lb** with action as **Allow** and the command spec "^set\s+lb\s+.*$"

   - **modify_all** with action as **Allow** and the command spec **"^\S+\s+(?!system).*"**

4. Use the procedure described in "Binding Command Policies to Users and Groups" to bind the **read_all** command policy to the **SysOps** group, with priority value **1**.

5. Use the procedure described in "Binding Command Policies to Users and Groups" to bind the **modify_lb** command policy to user **michaelb**, with priority value **5**.

The configuration you just created results in the following:

- John Doe, the IT manager, has read-only access to the entire NetScaler configuration, but he cannot make modifications.

- Maria Ramirez, the IT lead, has near-complete access to all areas of the NetScaler configuration, having to log on only to perform NetScaler-level commands.

- Michael Baldrock, the IT administrator responsible for load balancing, has read-only access to the NetScaler configuration, and can modify the configuration options for load balancing.

The set of command policies that applies to a specific user is a combination of command policies applied directly to the user's account and command policies applied to the group(s) of which the user is a member.

Each time a user enters a command, the operating system searches the command policies for that user until it finds a policy with an ALLOW or DENY action that matches the command. When it finds a match, the operating system stops its command policy search and allows or denies access to the command.

If the operating system finds no matching command policy, it denies the user access to the command, in accordance with the NetScaler appliance's default deny policy.

Note: When placing a user into multiple groups, take care not to cause unintended user command restrictions or privileges. To avoid these conflicts, when organizing your users in groups, bear in mind the NetScaler command policy search procedure and policy ordering rules.

Configuring External User Authentication

External user authentication is the process of authenticating the users of the Citrix NetScaler appliance by using an external authentication server. The NetScaler supports LDAP, RADIUS, and TACACS+ authentication servers. To configure external user authentication, you must create authentication policies. You can configure one or many authentication policies, depending on your authentication needs. An authentication policy consists of an expression and an action. Authentication policies use NetScaler classic expressions, which are described in detail in "Policy Configuration and Reference."

After creating an authentication policy, you bind it to the system global entity and assign a priority to it. You can create simple server configurations by binding a single authentication policy to the system global entity. Or, you can configure a cascade of authentication servers by binding multiple policies to the system global entity. If no authentication policies are bound to the system, users are authenticated by the onboard system.

Configuring LDAP Authentication

You can configure the NetScaler appliance to authenticate user access with one or more LDAP servers. LDAP authorization requires identical group names in Active Directory, on the LDAP server, and on the appliance. The characters and case must also be the same.

By default, LDAP authentication is secured by using SSL/TLS protocol. There are two types of secure LDAP connections. In the first type, the LDAP server accepts the SSL/TLS connection on a port separate from the port used to accept clear LDAP connections. After users establish the SSL/TLS connection, LDAP traffic can be sent over the connection. The second type allows both unsecure and secure LDAP connections and is handled by a single port on the server. In this scenario, to create a secure connection, the client first establishes a clear LDAP connection. Then the LDAP command StartTLS is sent to the server over the connection. If the LDAP server supports StartTLS, the connection is converted to a secure LDAP connection by using TLS.

The port numbers for LDAP connections are:

- 389 for unsecured LDAP connections
- 636 for secure LDAP connections
- 3268 for Microsoft unsecure LDAP connections
- 3269 for Microsoft secure LDAP connections

LDAP connections that use the StartTLS command use port number 389. If port numbers 389 or 3268 are configured on the appliance, it tries to use StartTLS to make the connection. If any other port number is used, connection attempts use SSL/TLS. If StartTLS or SSL/TLS cannot be used, the connection fails.

When configuring the LDAP server, the case of the alphabetic characters must match that on the server and on the appliance. If the root directory of the LDAP server is specified, all of the subdirectories are also searched to find the user attribute. In large directories, this can affect performance. For this reason, Citrix recommends that you use a specific organizational unit (OU).

The following table lists examples of user attribute fields for LDAP servers.

Table 1. User Attribute Fields for LDAP Servers

LDAP server	User attribute	Case sensitive?
Microsoft Active Directory	Server sAMAccountName	No
Novell eDirectory	cn	Yes
IBM Directory Server	uid	Yes
Lotus Domino	CN	Yes
Sun ONE directory (formerly iPlanet)	uid or cn	Yes

The following table lists examples of the base distinguished name (DN).

Table 2. Examples of Base Distinguished Name

LDAP server	Base DN
Microsoft Active Directory	DC=citrix, DC=local
Novell eDirectory	dc=citrix, dc=net
IBM Directory Server	cn=users
Lotus Domino	OU=City, O=Citrix, C=US
Sun ONE directory (formerly iPlanet)	ou=People, dc=citrix, dc=com

The following table lists examples of the bind distinguished name (DN).

Table 3. Examples of Bind Distinguished Name

LDAP server	Bind DN
Microsoft Active Directory	CN=Administrator, CN=Users, DC=citrix, DC=local
Novell eDirectory	cn=admin, dc=citrix, dc=net
IBM Directory Server	LDAP_dn
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE directory (formerly iPlanet)	uid=admin, ou=Administrators, ou=TopologyManagement, o=NetscapeRoot

To configure LDAP authentication by using the command line interface

At the command prompt, do the following:

1. Create an LDAP action.

   add authentication ldapAction <name> {-serverIP <ip_addr|ipv6_addr|*> | {-serverName <string>}} >] [-authTimeout <positive_integer>] [-ldapBase <string>] [-ldapBindDn <string>] {-ldapBindDnPassword } [-ldapLoginName <string>] [-groupAttrName <string>] [-subAttributeName <string>]

   Example:

   add authentication ldapAction ldap70 -serverIP <IP> -authTimeout 30 -ldapBase "CN=xxxxx,DC=xxxx,DC=x

2. Create an LDAP policy.

   add authentication ldapPolicy <name> <rule> [<reqAction>]

   Example:

   add authentication ldappolicy ldap_pol ns_true ldap70

3. Bind the LDAP policy to the following bind points at which the policy will be evaluated.

   - **System Global**: bind system global <policyName> [-priority <positive_integer>]
   - **VPN Global**: bind vpn global <policyName> [-priority <positive_integer>]
   - **Authentication Server**: bind authentication vserver <name> [-policy <string> [-priority <positive_integer>]
   - **VPN Server**: bind vpn vserver <name> [-policy <string> [-priority <positive_integer>]

To configure LDAP authentication by using the configuration utility

1. Navigate to System > Authentication.
2. On the Policies tab, click Add.
3. In Name, type a name for the policy.
4. In Authentication Type, select LDAP.
5. Next to Server, click New.
6. In Name, type the name of the server.
7. Under Server, in IP Address and Port, type the IP address and port number of the LDAP server.
8. Under Connection Settings, provide the following information:
   - In Base DN (location of users), type the base DN under which users are located.

     Base DN is usually derived from the Bind DN by removing the user name and specifying the group where in which are located. Examples of syntax for base DN are:

     ou=users, dc=ace, dc=com
     cn=Users, dc=ace, dc=com

   - In Administrator Bind DN, type the administrator bind DN for queries to the LDAP directory. Examples for syntax of bind DN are:

     domain/user name
     ou=administrator, dc=ace, dc=com
     user@domain.name (for Active Directory)
     cn=Administrator, cn=Users, dc=ace, dc=com

     For Active Directory, the group name specified as cn=groupname is required. The group name that is defined in the appliance must be identical to the group name that is defined on the LDAP server. For other LDAP directories, the group name either is not required or, if required, is specified as ou=groupname.

     The appliance binds to the LDAP server, using the administrator credentials, and then searches for the user. After locating the user, the appliance unbinds the administrator credentials and rebinds with the user credentials.

   - In Administrator Password and Confirm Administrator Password, type the administrator password for the LDAP server.
9. To retrieve additional LDAP settings automatically, click Retrieve Attributes. The fields under Other Settings then populate automatically. If you do not want to do this, skip to Step 12.
10. Under Other Settings, in Server Logon Name Attribute, type the attribute under which the appliance should look for user logon names for the LDAP server that you are

configuring. The default is `samAccountName`.

11. In Group Attribute, leave the default memberOf for Active Directory or change it to that of the LDAP server type you are using. This attribute enables the appliance to obtain the groups associated with a user during authorization.

12. In Security Type, select the security type. If you select PLAINTEXT or TLS for security, use port number 389. If you select SSL, use port number 636.

13. To allow users to change their LDAP password, select Allow Password Change. If you select PLAINTEXT as the security type, allowing users to change their passwords is not supported.

14. Click Create.

15. In the Create Authentication Policy dialog box, next to Named Expressions, select the expression, click Add Expression, click Create, and click Close.

After the LDAP server settings are configured on the appliance, bind the policy to the system global entity. For more information about binding authentication policies globally, see "Binding the Authentication Policies to the System Global Entity."

Determining attributes in the LDAP directory

If you need help determining your LDAP directory attributes, you can easily look them up with the free LDAP browser from Softerra.

You can download the LDAP browser from the Softerra LDAP Administrator Web site at http://www.ldapbrowser.com. After the browser is installed, set the following attributes:

- The host name or IP address of your LDAP server.
- The port of your LDAP server. The default is 389.
- The base DN field can be left blank.
- The information provided by the LDAP browser can help you determine the base DN needed for the Authentication tab.
- The Anonymous Bind check determines whether the LDAP server requires user credentials for the browser to connect to it. If the LDAP server requires credentials, leave the check box cleared.

After completing the settings, the LDAP browser displays the profile name in the left pane and connects to the LDAP server.

Parameter Descriptions (of commands listed in the CLI procedure)

add authentication ldapAction

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add authentication ldapPolicy

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring RADIUS Authentication

You can configure the NetScaler appliance to authenticate user access with one or more RADIUS servers. If you are using RSA SecurID, SafeWord, or Gemalto Protiva products, use a RADIUS server.

Your configuration might require using a network access server IP address (NAS IP) or a network access server identifier (NAS ID). When configuring the appliance to use a RADIUS authentication server, use the following guidelines:

- If you enable use of the NAS IP, the appliance sends its configured IP address to the RADIUS server, rather than the source IP address used in establishing the RADIUS connection.
- If you configure the NAS ID, the appliance sends the identifier to the RADIUS server. If you do not configure the NAS ID, the appliance sends its host name to the RADIUS server.
- When the NAS IP is enabled, the appliance ignores any NAS ID that was configured by using the NAS IP to communicate with the RADIUS server.

To configure RADIUS authentication by using the configuration utility

1. Navigate to System > Authentication.
2. On the Policies tab, click Add.
3. In Name, type a name for the policy.
4. In Authentication Type, select RADIUS.
5. Next to Server, click New.
6. In Name, type a name for the server.
7. Under Server, in IP Address, type the IP address of the RADIUS server.
8. In Port, type the port. The default is 1812.
9. Under Details, in Secret Key and Confirm Secret Key, type the RADIUS server secret.
10. In NAS ID, type the identifier number, and then click Create.
11. In the Create Authentication Policy dialog box, next to Named Expressions, select the expression, click Add Expression, click Create, and click Close.

After the RADIUS server settings are configured on the appliance, bind the policy to the system global entity. For more information about binding authentication policies globally,

see "Binding the Authentication Policies to the System Global Entity."

Choosing RADIUS authentication protocols

The NetScaler appliance supports implementations of RADIUS that are configured to use any of several protocols for user authentication, including:

- Password Authentication Protocol
- Challenge-Handshake Authentication Protocol (CHAP)
- Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP Version 1 and Version 2)

If your deployment of the appliance is configured to use RADIUS authentication and your RADIUS server is configured to use Password Authentication Protocol, you can strengthen user authentication by assigning a strong shared secret to the RADIUS server. Strong RADIUS shared secrets consist of random sequences of uppercase and lowercase letters, numbers, and punctuation, and are at least 22 characters long. If possible, use a random character generation program to determine RADIUS shared secrets.

To further protect RADIUS traffic, assign a different shared secret to each appliance or virtual server. When you define clients on the RADIUS server, you can also assign a separate shared secret to each client. If you do this, you must configure separately each policy that uses RADIUS authentication.

Shared secrets are configured on the appliance when a RADIUS policy is created.

Configuring IP address extraction

You can configure the appliance to extract the IP address from a RADIUS server. When a user authenticates with the RADIUS server, the server returns a framed IP address that is assigned to the user. The following are attributes for IP address extraction:

- Allows a remote RADIUS server to supply an IP address from the internal network for a user logged on to the appliance.
- Allows configuration for any RADIUS attribute using the type ipaddress, including those that are vendor encoded.

When configuring the RADIUS server for IP address extraction, you configure the vendor identifier and the attribute type.

The vendor identifier enables the RADIUS server to assign an IP address to the client from a pool of IP addresses that are configured on the RADIUS server. The vendor ID and attributes are used to make the association between the RADIUS client and the RADIUS server. The vendor ID is the attribute in the RADIUS response that provides the IP address of the internal network. A value of zero indicates that the attribute is not vendor encoded. The attribute type is the remote IP address attribute in a RADIUS response. The minimum value is one and the maximum value is 255.

A common configuration is to extract the RADIUS attribute *framed IP address*. The vendor ID is set to zero or is not specified. The attribute type is set to eight.

To configure IP address extraction by using the configuration utility

1. Navigate to System > Authentication > Radius, and select a policy.
2. Modify the server parameters and set relevant values in Group Vendor Identifier and Group Attribute Type fields.

Configuring TACACS+ Authentication

You can configure a TACACS+ server for authentication. Similar to RADIUS authentication, TACACS+ uses a secret key, an IP address, and the port number. The default port number is 49. To configure the appliance to use a TACACS+ server, provide the server IP address and the TACACS+ secret. The port needs to be specified only when the server port number in use is something other than the default port number of 49.

To configure TACACS+ authentication by using the configuration utility

1. Navigate to System > Authentication.
2. On the Policies tab, click Add.
3. In Name, type a name for the policy.
4. In Authentication Type, select TACACS.
5. Next to Server, click New.
6. In Name, type a name for the server.
7. Under Server, type the IP address and port number of the TACACS+ server.
8. Under TACACS server information, in TACACS Key and Confirm TACACS key, type the key.
9. In Authorization, select ON and click Create.
10. In the Create Authentication Policy dialog box, next to Named Expressions, select the expression, click Add Expression, click Create, and click Close.

After the TACACS+ server settings are configured on the appliance, bind the policy to the system global entity. For more information about binding authentication policies globally, see "Binding the Authentication Policies to the System Global Entity."

Binding the Authentication Policies to the System Global Entity

When the authentication policies are configured, bind the policies to the system global entity.

To bind an authentication policy to system global using the command line interface

At the command line prompt, do the following:

bind system global <policyName> [-priority <positive_integer>]

Example:

bind system global ldappol1 -priority 10

To bind an authentication policy to system global using the configuration utility

1. Navigate to System > Authentication.
2. On the Policies tab, click Global Bindings.
3. Click Insert Policy and under Policy Name, select the policy and click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

bind system global

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

SNMP

You can use Simple Network Management Protocol (SNMP) to configure the SNMP agent on the Citrix NetScaler appliance to generate asynchronous events, which are called *traps*. The traps are generated whenever there are abnormal conditions on the NetScaler. The traps are then sent to a remote device called a *trap listener*, which signals the abnormal condition on the NetScaler appliance. Or, you can query the SNMP agent for System-specific information from a remote device called an *SNMP manager*. The agent then searches the management information base (MIB) for the data requested and sends the data to the SNMP manager.

The SNMP agent on the NetScaler can generate traps compliant with SNMPv1 and SNMPv2 only. For querying, the SNMP agent supports SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2), and SNMP version 3 (SNMPv3).

The following figure illustrates a network with a NetScaler that has SNMP enabled and configured. In the figure, each SNMP network management application uses SNMP to communicate with the SNMP agent on the NetScaler. The SNMP agent searches its management information base (MIB) to collect the data requested by the SNMP Manager and provides the information to the application.

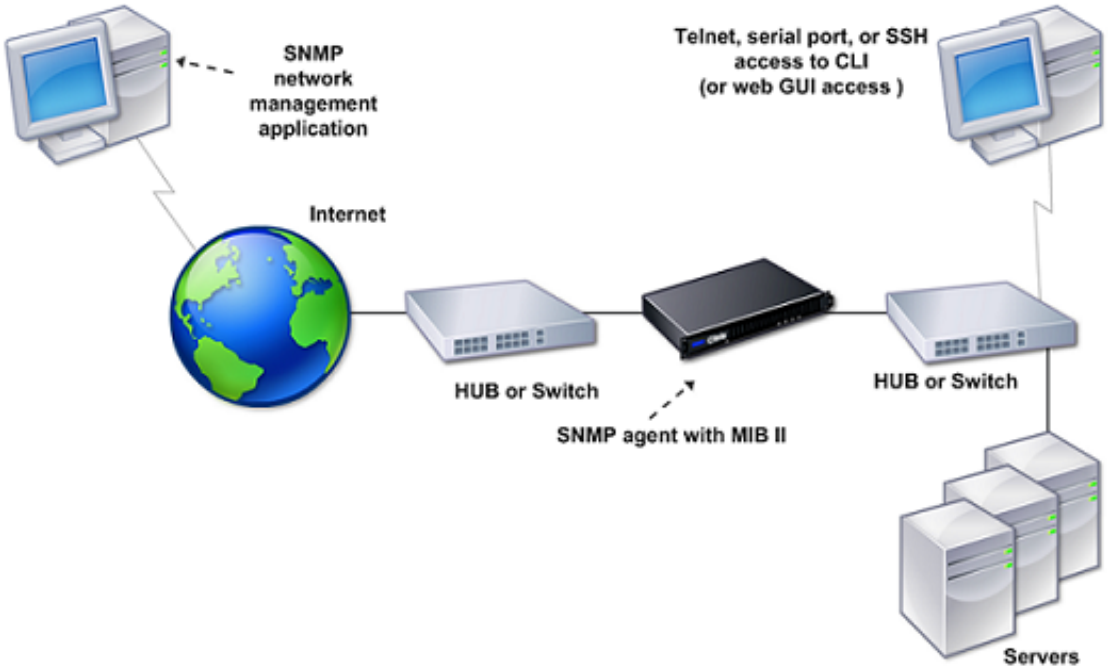


Figure 1. *NetScaler Supporting SNMP*

Importing MIB Files to the SNMP Manager and Trap Listener

To monitor a NetScaler appliance, you must download the MIB object definition files. The MIB files include the following:

- MIB-2 groups SYSTEM, IF, ICMP, UDP, and SNMP.
- NetScaler-specific configuration and statistics.

You can obtain the MIB object definition files from the /netscaler/snmp directory or from the Downloads tab of the NetScaler GUI.

If the SNMP management application is other than *WhatsUpGold*, download the following files to the SNMP management application:

- NS-MIB-smiv1.mib. Used by SNMPv1 managers and trap listeners.
- NS-MIB-smiv2.mib. Used by SNMPv2 and SNMPv3 managers and SNMPv2 trap listeners.

If the SNMP management application is *WhatsUpGold*, download the following files to the SNMP management application:

- mib.txt
- traps.txt

Configuring the NetScaler to Generate SNMP Traps

You can configure the NetScaler appliance to generate asynchronous events, which are called *traps*. The traps are generated whenever there are abnormal conditions on the appliance. The traps are sent to a remote device called a *trap listener*. This helps administrators monitor the appliance and respond promptly to any issues.

The NetScaler appliance provides a set of condition entities called *SNMP alarms*. When the condition in any SNMP alarm is met, the appliance generates SNMP trap messages that are sent to the configured trap listeners. For example, when the LOGIN-FAILURE alarm is enabled, a trap message is generated and sent to the trap listener whenever there is a login failure on the appliance.

To configure the NetScaler appliance to generate traps, you need to enable and configure alarms. Then, you specify trap listeners to which the appliance will send the generated trap messages.

Enabling an SNMP Alarm

The NetScaler appliance generates traps only for SNMP alarms that are enabled. Some alarms are enabled by default, but you can disable them.

When you enable an SNMP alarm, the appliance generates corresponding trap messages when some events occur. Some alarms are enabled by default.

To enable an SNMP alarm by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- enable snmp alarm `<trapName>`
- show snmp alarm `<trapName>`

To enable an SNMP alarm by using the configuration utility

1. Navigate to System > SNMP > Alarms, and select the alarm.
2. Click Actions and select Enable.

Parameter Descriptions (of commands listed in the CLI procedure)

enable snmp alarm

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show snmp alarm

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Alarms

The NetScaler appliance provides a set of condition entities called *SNMP alarms*. When the condition set for an SNMP alarm is met, the appliance generates SNMP traps messages that are sent to the configured trap listeners. For example, when the LOGIN-FAILURE alarm is enabled, a trap message is generated and sent to the trap listener whenever there is a login failure on the appliance.

You can assign an SNMP alarm with a severity level. When you do this, the corresponding trap messages are assigned that severity level.

The following are the severity levels, defined on the appliance, in decreasing order of severity.

- Critical
- Major
- Minor
- Warning
- Informational

For example, if you set a warning severity level for the SNMP alarm named LOGIN-FAILURE, the trap messages generated when there is a login failure will be assigned with the warning severity level.

You can also configure an SNMP alarm to log the corresponding trap messages generated whenever the condition on that alarm is met.

To configure an SNMP alarm by using the command line interface

At the command prompt, type the following commands to configure an SNMP alarm and verify the configuration:

- set snmp alarm <trapName> [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-time <secs>] [-state (ENABLED | DISABLED)] [-severity <severity>] [-logging (ENABLED | DISABLED)]
- show snmp alarm <trapName>

To configure SNMP alarms by using the configuration utility

Navigate to System > SNMP > Alarms, select an alarm and configure the alarm parameters.

Parameter Descriptions (of commands listed in the CLI procedure)

set snmp alarm

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show snmp alarm

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring SNMPv1 or SNMPv2 Traps

After configuring the alarms, you need to specify the trap listener to which the appliance sends the trap messages. Apart from specifying parameters such as IP or IPv6 address and the destination port of the trap listener, you can specify the type of trap (either generic or specific) and the SNMP version.

You can configure a maximum of 20 trap listeners for receiving either generic or specific traps.

You can also configure the appliance to send SNMP trap messages with a source IP address other than the NetScaler IP (NSIP or NSIP6) address to a particular trap listener. For a trap listener that has an IPv4 address, you can set the source IP to either a mapped IP (MIP) address or a subnet IP (SNIP) address configured on the appliance. For a trap listener that has an IPv6 address, you can set the source IP to subnet IPv6 (SNIP6) address configured on the appliance.

You can also configure the appliance to send trap messages to a trap listener on the basis of a severity level. For example, if you set the severity level as Minor for a trap listener, all trap messages of the severity level equal to or greater than Minor (Minor, Major, and Critical) are sent to the trap listener.

If you have defined a community string for the trap listener, you must also specify a community string for each trap that is to be sent to the listener. A trap listener for which a community string has been defined accepts only trap messages that include a community string matching the community string defined in the trap listener. Other trap messages are dropped.

To add an SNMP trap by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- add snmp trap <trapClass> <trapDestination> -version (V1 | V2) -destPort <port> -communityName <string> -srcIP <ip_addr> -severity <severity>
- show snmp trap

Example

```
> add snmp trap specific 10.102.29.3 -version V2 -destPort 80 -communityName com1 -severity Major
```

To configure SNMP Traps by using the configuration utility

Navigate to System > SNMP > Traps, and create the SNMP trap.

Parameter Descriptions (of commands listed in the CLI procedure)

add snmp trap

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show snmp trap

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Enabling Unconditional SNMP Trap Logging

By default, the NetScaler appliance logs any SNMP trap messages (for SNMP alarms in which logging is enabled) when at least one trap listener is specified on the appliance. However, you can specify that SNMP trap messages be logged even when no trap listeners are configured.

To enable unconditional SNMP trap logging by using the command line interface

At the command prompt, type the following commands to configure unconditional SNMP trap logging and verify the configuration:

- set snmp option -snmpTrapLogging (ENABLED | DISABLED)
- show snmp option

To enable unconditional SNMP trap logging by using the configuration utility

Navigate to System > SNMP, click Change SNMP Options and select SNMP Trap Logging.

Parameter Descriptions (of commands listed in the CLI procedure)

set snmp option

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show snmp option

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring the NetScaler for SNMP v1 and v2 Queries

You can query the NetScaler SNMP agent for system-specific information from a remote device called *SNMP managers*. The agent then searches the management information base (MIB) for the data requested and sends the data to the SNMP manager.

The following types of SNMP v1 and v2 queries are supported by the SNMP agent:

- GET
- GET NEXT
- ALL
- GET BULK

You can create strings called *community strings* and associate each of these to query types. You can associate one or more community strings to each query type. Community string are passwords and used to authenticate SNMP queries from SNMP managers.

For example, if you associate two community strings, such as **abc** and **bcd**, to the query type GET NEXT, the SNMP agent on the NetScaler appliance considers only those GET NEXT SNMP query packets that contain **abc** or **bcd** as the community string.

Specifying an SNMP Manager

You must configure the NetScaler appliance to allow the appropriate SNMP managers to query it. You must also provide the SNMP manager with the required NetScaler-specific information. You can add up to a maximum of 100 SNMP managers or networks.

For an IPv4 SNMP manager you can specify a host name instead of the manager's IP address. If you do so, you must add a DNS name server that resolves the host name of the SNMP manager to its IP address. You can add up to a maximum of five host-name based SNMP managers.

Note: The appliance does not support use of host names for SNMP managers that have IPv6 addresses. You must specify the IPv6 address.

If you do not configure at least one SNMP manager, the appliance accepts and responds to SNMP queries from all IP addresses on the network. If you configure one or more SNMP managers, the appliance accepts and responds only to SNMP queries from those specific IP addresses.

If you remove an SNMP manager from the configuration, that manager can no longer query the appliance.

To add SNMP managers by specifying IP addresses by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- add snmp manager <IPAddress> ... [-netmask <netmask>]
- show snmp manager

Example

```
> add snmp manager 10.102.29.10 10.102.29.15 10.102.29.30
```

To add an SNMP manager by specifying its host name by using the command line interface

Important: If you specify the SNMP manager’s host name instead of its IP address, you must configure a DNS name server to resolve the host name to the SNMP manager’s IP address. For more information, see "Adding a Name Server."

At the command prompt, type the following commands to set the parameters and verify the configuration:

- add snmp manager <IPAddress> [-domainResolveRetry <integer>]
- show snmp manager

Example

> add nameserver 10.103.128.15

> add snmp manager engwiki.eng.example.net –domainResolveRetry 10

To add an SNMP manager by using the configuration utility

1. Navigate to System > SNMP > Managers, and create the SNMP manager.

   Important: If you specify the SNMP manager's host name instead of its IPv4 address, you must configure a DNS name server to resolve the host name to the SNMP manager's IP address. For more information, see "Adding a Name Server."

   Note: The appliance does not support host names for SNMP managers that have IPv6 addresses.

Parameter Descriptions (of commands listed in the CLI procedure)

add snmp manager

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show snmp manager

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Specifying an SNMP Community

You can create strings called *community strings* and associate them with the following SNMP query types on the appliance:

- GET
- GET NEXT
- ALL
- GET BULK

You can associate one or more community strings to each query types. For example, when you associate two community strings, such as **abc** and **bcd**, to the query type GET NEXT, the SNMP agent on the appliance considers only those GET NEXT SNMP query packets that contain **abc** or **bcd** as the community string.

If you do not associate any community string to a query type then the SNMP agent responds to all SNMP queries of that type.

To specify an SNMP community by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- add snmp community <communityName> <permissions>
- show snmp community

Example

> add snmp community com all

To configure an SNMP community string by using the configuration utility

Navigate to System > SNMP > Community, and create the SNMP community.

Parameter Descriptions (of commands listed in the CLI procedure)

add snmp community

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show snmp community

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring SNMP Alarms for Rate Limiting

Citrix NetScaler appliances such as the NetScaler MPX 10500, 12500, and 15500 are rate limited. The maximum throughput (Mbps) and packets per second (PPS) are determined by the license purchased for the appliance. For rate-limited platforms, you can configure SNMP traps to send notifications when throughput and PPS approach their limits and when they return to normal.

Throughput and PPS are monitored every seven seconds. You can configure traps with high-threshold and normal-threshold values, which are expressed as a percentage of the licensed limits. The appliance then generates a trap when throughput or PPS exceeds the high threshold, and a second trap when the monitored parameter falls to the normal threshold. In addition to sending the traps to the configured destination device, the NetScaler logs the events associated with the traps in the /var/log/ns.log file as EVENT ALERTSTARTED and EVENT ALERTENDED.

Exceeding the throughput limit can result in packet loss. You can configure SNMP alarms to report packet loss.

For more information about SNMP alarms and traps, see "Configuring the NetScaler to generate SNMP v1 and v2 Traps."

Configuring an SNMP Alarm for Throughput or PPS

To monitor both throughput and PPS, you must configure separate alarms.

To configure an SNMP alarm for the throughput rate by using the command line interface

At the command prompt, type the following commands to configure the SNMP alarm and verify the configuration:

- set snmp alarm PF-RL-RATE-THRESHOLD [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-state (**ENABLED** | **DISABLED**)] [-severity <severity>] [-logging (**ENABLED** | **DISABLED**)]
- show snmp alarm PF-RL-RATE-THRESHOLD

Example

```
> set snmp alarm PF-RL-RATE-THRESHOLD -thresholdValue 70 -normalValue 50
```

To configure an SNMP alarm for PPS by using the command line interface

At the command prompt, type the following commands to configure the SNMP alarm for PPS and verify the configuration:

- set snmp alarm PF-RL-PPS-THRESHOLD [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-state (**ENABLED** | **DISABLED**)] [-severity <severity>] [-logging (**ENABLED** | **DISABLED**)]
- show snmp alarm PF-RL-PPS-THRESHOLD

Example

```
> set snmp alarm PF-RL-PPS-THRESHOLD -thresholdValue 70 -normalValue 50
```

To configure an SNMP alarm for throughput or PPS by using the configuration utility

1. Navigate to System > SNMP > Alarms, and select PF-RL-RATE-THRESHOLD (for throughput rate) or PF-RL-PPS-THRESHOLD (for packets per second).

2. Set the alarm parameters and enable the selected SNMP alarm.

Parameter Descriptions (of commands listed in the CLI procedure)

set snmp alarm

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show snmp alarm

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring SNMP Alarm for Dropped Packets

You can configure an alarm for packets dropped as a result of exceeding the throughput limit and an alarm for packets dropped as a result of exceeding the PPS limit.

To configure an SNMP alarm for packets dropped because of excessive throughput, by using the command line interface

At the command prompt, type:

set snmp alarm PF-RL-RATE-PKTS-DROPPED [-state (**ENABLED** | **DISABLED**)] [-severity <severity>] [-logging (**ENABLED** | **DISABLED**)]

To configure an SNMP alarm for packets dropped because of excessive PPS, by using the command line interface

At the command prompt, type:

set snmp alarm PF-RL-PPS-PKTS-DROPPED [-state (**ENABLED** | **DISABLED**)] [-severity <severity>] [-logging (**ENABLED** | **DISABLED**)]

To configure an SNMP alarm for dropped packets by using the configuration utility

1. Navigate to System > SNMP > Alarms, and select PF-RL-RATE-PKTS-DROPPED (for packets dropped because of excessive throughput) or PF-RL-PPS-PKTS-DROPPED (for packets dropped because of excessive PPS).

2. Set the alarm parameters and enable the selected SNMP alarm.

Parameter Descriptions (of commands listed in the CLI procedure)

set snmp alarm

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring the NetScaler for SNMPv3 Queries

Simple Network Management Protocol Version 3 (SNMPv3) is based on the basic structure and architecture of SNMPv1 and SNMPv2. However, SNMPv3 enhances the basic architecture to incorporate administration and security capabilities, such as authentication, access control, data integrity check, data origin verification, message timeliness check, and data confidentiality.

To implement message level security and access control, SNMPv3 introduces the user-based security model (USM) and the view-based access control model (VACM).

- **User-Based Security Model.** The user-based security model (USM) provides message-level security. It enables you to configure users and security parameters for the SNMP agent and the SNMP manager. USM offers the following features:
  - **Data integrity:** To protect messages from being modified during transmission through the network.
  - **Data origin verification:** To authenticate the user who sent the message request.
  - **Message timeliness:** To protect against message delays or replays.
  - **Data confidentiality:** To protect the content of messages from being disclosed to unauthorized entities or individuals.
- **View-Based Access Control Model.** The view-based access control model (VACM) enables you to configure access rights to a specific subtree of the MIB based on various parameters, such as security level, security model, user name, and view type. It enables you to configure agents to provide different levels of access to the MIB to different managers.

The Citrix NetScaler supports the following entities that enable you to implement the security features of SNMPv3:

- SNMP Engines
- SNMP Views
- SNMP Groups
- SNMP Users

These entities function together to implement the SNMPv3 security features. Views are created to allow access to subtrees of the MIB. Then, groups are created with the required security level and access to the defined views. Finally, users are created and assigned to the groups.

Note: The view, group, and user configuration are synchronized and propagated to the secondary node in a high availability (HA) pair. However, the engine ID is neither propagated nor synchronized as it is unique to each NetScaler appliance.

To implement message authentication and access control, you need to:

- Set the Engine ID
- Configure Views
- Configure Groups
- Configure Users

Setting the Engine ID

SNMP engines are service providers that reside in the SNMP agent. They provide services such as sending, receiving, and authenticating messages. SNMP engines are uniquely identified using engine IDs.

The NetScaler appliance has a unique engineID based on the MAC address of one of its interfaces. It is not necessary to override the engineID. However, if you want to change the engine ID, you can reset it.

To set the engine ID by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- set snmp engineId <engineID>
- show snmp engineId

Example

> set snmp engineId 8000173f0300c095f80c68

To set the engine ID by using configuration utility

Navigate to System > SNMP > Users, click Configure Engine ID and type an engine ID.

Parameter Descriptions (of commands listed in the CLI procedure)

set snmp engineId

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show snmp engineId

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring a View

SNMP views restrict user access to specific portions of the MIB. SNMP views are used to implement access control.

To add an SNMP view by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- add snmp view <name> <subtree> -type (included | excluded)
- show snmp view <name>

Example

> add snmp view View1 -type included

To configure an SNMP view by using the configuration utility

Navigate to System > SNMP > Views, and create the SNMP view.

Parameter Descriptions (of commands listed in the CLI procedure)

add snmp view

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show snmp view

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring a Group

SNMP groups are logical aggregations of SNMP users. They are used to implement access control and to define the security levels. You can configure an SNMP group to set access rights for users assigned to that group, thereby restricting the users to specific views.

You need to configure an SNMP group to set access rights for users assigned to that group.

To add an SNMP group by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- add snmp group <name> <securityLevel> -readViewName <string>
- show snmp group <name> <securityLevel>

Example

> add snmp group edocs_group2 authPriv -readViewName edocs_read_view

To configure an SNMP group by using the configuration utility

Navigate to System > SNMP > Groups, and create the SNMP group.

Parameter Descriptions (of commands listed in the CLI procedure)

add snmp group

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show snmp group

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring a User

SNMP users are the SNMP managers that the agents allow to access the MIBs. Each SNMP user is assigned to an SNMP group.

You need to configure users at the agent and assign each user to a group.

To configure a user by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- add snmp user <name> -group <string> [-authType (MD5 | SHA) {-authPasswd } [-privType (DES | AES) {-privPasswd }]]
- show snmp user <name>

Example

> add snmp user edocs_user -group edocs_group

To configure an SNMP user by using the configuration utility

Navigate to System > SNMP > Users, and create the SNMP user.

Parameter Descriptions (of commands listed in the CLI procedure)

add snmp user

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show snmp user

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Audit Logging

Auditing is a methodical examination or review of a condition or situation. The Audit Logging feature enables you to log the NetScaler states and status information collected by various modules in the kernel and in the user-level daemons. For audit logging, you have the options to configure SYSLOG, the native NSLOG protocol, or both.

SYSLOG is a standard protocol for logging. It has two components□ the SYSLOG auditing module, which runs on the NetScaler appliance, and the SYSLOG server, which can run on the underlying FreeBSD operating system (OS) of the NetScaler appliance or on a remote system. SYSLOG uses user data protocol (UDP) for the transfer of data.

Similarly, the native NSLOG protocol has two components□ the NSLOG auditing module, which runs on the NetScaler appliance, and the NSLOG server, which can run on the underlying FreeBSD OS of the NetScaler appliance or on a remote system. NSLOG uses transmission control protocol (TCP) for transfer of data.

When you run NSLOG or a SYSLOG server, it connects to the NetScaler appliance. The NetScaler appliance then starts sending all the log information to the SYSLOG or NSLOG server, and the server can filter the log entries before storing them in a log file. An NSLOG or SYSLOG server can receive log information from more than one NetScaler appliance and a NetScaler appliance can send log information to more than one SYSLOG server or NSLOG server.

The log information that a SYSLOG or NSLOG server collects from a NetScaler appliance is stored in a log file in the form of messages. These messages typically contain the following information:

- The IP address of a NetScaler appliance that generated the log message
- A time stamp
- The message type
- The predefined log levels (Critical, Error, Notice, Warning, Informational, Debug, Alert, and Emergency)
- The message information

To configure audit logging, you first configure the audit modules on the NetScaler that involves creating audit policies and specifying the NSLOG server or SYSLOG server information. You then install and configure the SYSLOG or the NSLOG server on the underlying FreeBSD OS of the NetScaler appliance or on a remote system.

Note: Because SYSLOG is an industry standard for logging program messages and because various vendors provide support, this documentation does not include SYSLOG server configuration information.

The NSLOG server has its own configuration file (auditlog.conf). You can customize logging on the NSLOG server system by making additional modifications to the configuration file (auditlog.conf).

Configuring the NetScaler Appliance for Audit Logging

Policies define the SYSLOG or NSLOG protocol, and server actions define what logs are sent where. For server actions, you specify the system information, which runs the SYSLOG or the NSLOG server.

The NetScaler logs the following information related to TCP connections:

- Source port
- Destination port
- Source IP
- Destination IP
- Number of bytes transmitted and received
- Time period for which the connection is open

Note:

- You can enable TCP logging on individual load balancing vservers. You must bind the audit log policy to a specific load balancing vserver that you want to log.
- When using the NetScaler as the audit log server, by default, the ns.log file is rotated (new file is created) when the file size reaches 100K and the last 25 copies of the ns.log are archived and compressed with gzip. To accommodate more archived files after 25 files, the oldest archive is deleted. You can modify the 100K limit or the 25 file limit by updating the following entry in the /etc/newsyslog.conf file:

  ```
  /var/log/ns.log  600  25  100  *  Z
  ```

  where, 25 is the number of archived files to be maintained and 100K is the size of the ns.log file after which the file will be archived.

Configuring Audit Servers

You can configure audit server actions for different servers and for different log levels.

To configure a SYSLOG server action by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> [-dateFormat (MMDDYYYY | DDMMYYYY)]
- show audit syslogAction [<name>]

Example

```
> add audit syslogaction audit-action1 10.102.1.1 -loglevel INFORMATIONAL -dateformat MMDDYYYY
```

To configure an NSLOG server action by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- add audit nslogAction <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> [-dateFormat (MMDDYYYY | DDMMYYYY)]
- show audit nslogAction [<name>]

Example

```
> add audit nslogAction nslog-action1 10.102.1.3 -serverport 520 -loglevel INFORMATIONAL -dateFormat MMD
```

To configure an auditing server action by using the configuration utility

1. In the navigation pane, expand System, expand Auditing, and then click Policies.
2. In the details pane, on the Servers tab, click Add.
3. In the Create Auditing Server dialog box, configure the auditing server. For a description of a parameter, hover the mouse cursor over the corresponding field.
4. Click Create, and then click Close.

To configure an auditing server action by using the configuration utility

Parameter Descriptions (of commands listed in the CLI procedure)

add audit syslogAction

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show audit syslogAction

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add audit nslogAction

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show audit nslogAction

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Audit Policies

The audit policies define the SYSLOG or NSLOG protocol.

To configure a SYSLOG policy by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- add audit syslogPolicy <name> <rule> <action>
- show audit syslogPolicy [<name>]

Example

> add audit syslogpolicy syslog-pol1 ns_true audit-action1

To configure an NSLOG policy by using the command line interface

At the command prompt, type the following commands to set the parameters and verify the configuration:

- add audit nslogPolicy <name> <rule> <action>
- show audit nslogPolicy [<name>]

Example

> add audit nslogPolicy nslog-pol1 ns_true nslog-action1

To configure an audit server policy by using the configuration utility

1. In the navigation pane, expand System, expand Auditing, and then click Policies.
2. In the details pane, on the Policies tab, click Add.
3. In the Create Auditing Policy dialog box, configure the audit policy. For a description of a parameter, hover the mouse cursor over the corresponding field.
4. Click Create, and then click Close.

To configure an audit server policy by using the configuration utility

Parameter Descriptions (of commands listed in the CLI procedure)

add audit syslogPolicy

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show audit syslogPolicy

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add audit nslogPolicy

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show audit nslogPolicy

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Binding the Audit Policies Globally

You must globally bind the audit log policies to enable logging of all NetScaler system events. By defining the priority level, you can set the evaluation order of the audit server logging. Priority 0 is the highest and is evaluated first. The higher the priority number, the lower is the priority of evaluation.

To configure a SYSLOG policy by using the command line interface

At the command prompt, type:

- bind system global [<policyName> [-priority <positive_integer>]]
- show system global

Example

> bind system global nslog-pol1 -priority 20

To globally bind the audit policy by using the configuration utility

1. In the navigation pane, expand System, expand Auditing, and then click Policies.
2. In the details pane, on the Policies tab, click Global Bindings.
3. In the Bind/Unbind Auditing Global Policies dialog box, click Insert Policy.
4. Select a policy from the drop-down list that appears under Policy Name, and click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

bind system global

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show system global

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Policy-Based Logging

You can configure policy-based logging for rewrite and responder policies. Audit messages are then logged in a defined format when the rule in a policy evaluates to TRUE. To configure policy-based logging, you configure an audit-message action that uses default syntax expressions to specify the format of the audit messages, and associate the action with a policy. The policy can be bound either globally or to a load balancing or content switching virtual server. You can use audit-message actions to log messages at various log levels, either in syslog format only or in both syslog and newnslog formats.

Pre Requisites

- User Configurable Log Messages (userDefinedAuditlog) option is enabled for when configuring the audit action server to which you want to send the logs in a defined format. For more information about enabling policy-based logging on an audit action server, see "Binding the Audit Policies Globally."
- The related audit policy is bound to system global. For more information about binding audit policies to system global, see "Binding the Audit Policies Globally."

Configuring an Audit Message Action

You can configure audit message actions to log messages at various log levels, either in syslog format only or in both syslog and newnslog formats. Audit-message actions use expressions to specify the format of the audit messages.

To create an audit message action by using the command line interface

At the command prompt, type:

add audit messageaction <name> <logLevel> <stringBuilderExpr> [-logtoNewnslog (YES|NO)] [-bypassSafetyCheck (YES|NO)]

Example

> add audit messageaction log-act1 CRITICAL '"Client:"+CLIENT.IP.SRC+" accessed "+HTTP.REQ.URL' -bypassSa

To configure an audit message action by using the configuration utility

Navigate to System > Auditing > Message Actions, and create the audit message action.

Binding Audit Message Action to a Policy

After you have created an audit message action, you must bind it to a rewrite or responder policy. For more information about binding log message actions to a rewrite or responder policy, see "Rewrite" or "Responder".

Parameter Descriptions (of commands listed in the CLI procedure)

add audit messageaction

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Installing and Configuring the NSLOG Server

During installation, the NSLOG server executable file (auditserver) is installed along with other files. The auditserver executable file includes options for performing several actions on the NSLOG server, including running and stopping the NSLOG server. In addition, you use the auditserver executable to configure the NSLOG server with the IP addresses of the NetScaler appliances from which the NSLOG server will start collecting logs. Configuration settings are applied in the NSLOG server configuration file (auditlog.conf).

Then, you start the NSLOG server by executing the auditserver executable. The NSLOG server configuration is based on the settings in the configuration file. You can further customize logging on the NSLOG server system by making additional modifications to the NSLOG server configuration file (auditlog.conf).

Attention: The version of the NSLOG server package must be the same as that of the NetScaler. For example, if the version of the NetScaler is 10.1 Build 125.9, the NSLOG server must also be of the same version.

The following table lists the operating systems on which the NSLOG server is supported.

Table 1. Supported Platforms for the NSLOG Server

Operating system	Software requirements	Remarks
Windows	· Windows XP Professional · Windows Server 2003 · Windows 2000/NT · Windows Server 2008 · Windows Server 2008 R2	
Linux	· RedHat Linux 4 or later · SUSE Linux Enterprise 9.3 or later	
FreeBSD	FreeBSD 6.3 or later	For NetScaler 10.5, use only FreeBSD 8.4.
Mac OS	Mac OS 8.6 or later	Not supported on NetScaler 10.1 and later releases.

The minimum hardware specifications for the platform running the NSLOG server are as follows:

- Processor- Intel x86 ~501 megahertz (MHz)

- RAM - 512 megabytes (MB)
- Controller - SCSI

Installing NSLOG Server on the Linux Operating System

Log on to the Linux system as an administrator. Use the following procedure to install the NSLOG server executable files on the system.

To install the NSLOG server package on a Linux operating system

1. At a Linux command prompt, type the following command to copy the NSauditserver.rpm file to a temporary directory:

   ```
   cp <path_to_cd>/Utilities/auditserver/Linux/NSauditserver.rpm /tmp
   ```

2. Type the following command to install the NSauditserver.rpm file:

   ```
   rpm -i NSauditserver.rpm
   ```

   This command extracts the files and installs them in the following directories:

   - /usr/local/netscaler/etc
   - /usr/local/netscaler/bin
   - /usr/local/netscaler/samples

To uninstall the NSLOG server package on a Linux operating system

1. At a command prompt, type the following command to uninstall the audit server logging feature:

   ```
   rpm -e NSauditserver
   ```

2. For more information about the NSauditserver RPM file, use the following command:

   ```
   rpm -qpi *.rpm
   ```

3. To view the installed audit server files use the following command:

   ```
   rpm -qpl *.rpm
   ```

   *.rpm: Specifies the file name.

Installing NSLOG Server on the FreeBSD Operating System

Before you can install the NSLOG server, you have to copy the NSLOG package from the NetScaler product CD or download it from www.citrix.com. The NSLOG package has the following name format `AuditServer _<release number>-<build number>.zip` (for example, `AuditServer_9.3-51.5.zip`). This package contains NSLOG installation packages for all supported platforms.

Note: NSLOG server is not supported on the underlying FreeBSD OS of the NetScaler appliance.

To download NSLOG package from www.Citrix.com

1. In a web browser, go to www.citrix.com.
2. In the menu bar, click Log In.
3. Enter your login credentials, and then click Log In.
4. In the menu bar, click Downloads.
5. Search to find the page that provides the appropriate release number and build.
6. On that page, under Audit Servers, click Download to download the NSLOG package, having the format `AuditServer_<release number>-<build number>.zip` , to your local system (for example, `AuditServer_9.3-51.5.zip`).

To install the NSLOG server package on a FreeBSD operating system

1. On the system to which you have downloaded the NSLOG package `AuditServer_<release number>-<build number>.zip` (for example, `AuditServer_9.3-51.5.zip`), extract the FreeBSD NSLOG server package `audserver_bsd-<release number>-<build number>.tgz` (for example, `audserver_bsd-9.3-51.5.tgz`) from the package.

2. Copy the FreeBSD NSLOG server package `audserver_bsd-<release number>-<build number>.tgz` (for example, `audserver_bsd-9.3-51.5.tgz`) to a directory on a system running FreeBSD OS.

3. At a command prompt for the directory into which the FreeBSD NSLOG server package was copied, run the following command to install the package:

   ```
   pkg_add audserver_bsd-<release number>-<build number>.tgz
   ```

   Example

   pkg_add audserver_bsd-9.3-51.5.tgz

   The following directories are extracted:

   - <root directory extracted from the FreeBSD NSLOG server package tgz file>\netscaler\bin (for example, `/var/auditserver/netscaler/bin`)
   - <root directory extracted from the FreeBSD NSLOG server package tgz file>\netscaler\etc (for example, `/var/auditserver/netscaler/etc`)
   - <root directory extracted from the FreeBSD NSLOG server package tgz file>\netscaler\samples (for example, `/var/auditserver/samples`)

4. At a command prompt, type the following command to verify that the package is installed:

   ```
   pkg_info | grep NSaudserver
   ```

To uninstall the NSLOG server package on a FreeBSD operating system

At a command prompt, type:

```
pkg_delete NSaudserver
```

Installing NSLOG Server Files on the Windows Operating System

Before you can install the NSLOG server, you have to copy the NSLOG package from the NetScaler product CD or download it from www.citrix.com. The NSLOG package has the following name format `AuditServer _<release number>-<build number>.zip` (for example, `AuditServer_9.3-51.5.zip`). This package contains NSLOG installation packages for all supported platforms.

To download NSLOG package from www.Citrix.com

1. In a web browser, go to www.citrix.com.
2. In the menu bar, click Log In.
3. Enter your login credentials, and then click Log In.
4. In the menu bar, click Downloads.
5. Search to find the page that provides the appropriate release number and build.
6. On that page, under Audit Servers, click Download to download the NSLOG package, having the format `AuditServer_<release number>-<build number>.zip` , to your local system (for example, `AuditServer_9.3-51.5.zip`).

To install NSLOG server on a Windows operating system

1. On the system, where you have downloaded the NSLOG package `AuditServer_<release number>-<build number>.zip` (for example, `AuditServer_9.3-51.5.zip`), extract `audserver_win-<release number>-<build number>.zip` (for example, `audserver_win-9.3-51.5.zip`) from the package.

2. Copy the extracted file `audserver_<release number>-<build number>.zip` (for example, `audserver_win-9.3-51.5.zip`) to a Windows system on which you want to install the NSLOG server.

3. Unzip the `audserver_<release number>-<build number>.zip` file (for example, `audserver_win-9.3-51.5.zip`).

4. The following directories are extracted:

   a. <root directory extracted from the Windows NSLOG server package zip file>\bin (for example, `C:\audserver_win-9.3-51.5\bin`)

   b. <root directory extracted from the Windows NSLOG server package zip file>\etc (for example, `C:\audserver_win-9.3-51.5\ etc`)

   c. < root directory extracted from the Windows NSLOG server package zip file >\samples (for example, `C:\audserver_win-9.3-51.5\ samples`)

5. At a command prompt, run the following command from the <root directory extracted from the Windows `NSLOG server package zip file>\bin path:`

   `audserver` -install -f <directorypath>**auditlog.conf**

   <directorypath>: Specifies the path to the configuration file (`auditlog.conf`). By default, log.conf is under <root directory extracted from Windows `NSLOG server package zip file>\samples` directory. But you can copy auditlog.conf to your desired directory.

To uninstall the NSLOG server on a Windows operating system

At a command prompt, run the following from the `<root directory extracted from Windows NSLOG server package zip file>\bin path:`

`audserver` -remove

NSLOG Server Command Options

The following table describes the commands that you can use to configure audit server options.

Table 1. Audit Server Options

Audit server commands	Specifies
`audserver -help`	The available Audit Server options.
`audserver -addns -f` <path to configuration file>	The system that gathers the log transaction data. You are prompted to enter the IP address of the NetScaler appliance. Enter the valid user name and password.
`audserver -verify -f` <path to configuration file>	Check for syntax or semantic errors in the configuration file (for example, auditlog.conf).
`audserver -start -f` <path to configuration file>	Start audit server logging based on the settings in the configuration file (auditlog.conf). Linux only: To start the audit server as a background process, type the ampersand sign (&) at the end of the command.
`audserver -stop` (Linux only)	Stops audit server logging when audit server is started as a background process. Alternatively, use the Ctrl+C key to stop audit server logging.
`audserver -install -f` <path to configuration file> (Windows only)	Installs the audit server logging client as a service on Windows.
`audserver -startservice` (Windows Only)	Start the audit server logging service, when you enter this command at a command prompt. You can also start audit server logging from Start > Control Panel > Services. **Note:** Audit server logging starts by using the configuration settings in the configuration file, for example, auditlog.conf file specified in the audit server install option.

`audserver -stopservice` (Windows Only)	Stop audit server logging.
`audserver -remove`	Removes the audit server logging service from the registry.

Run the `audserver` command from the directory in which the audit server executable is present:

- On Windows: \ns\bin
- On Solaris and Linux: \usr\local\netscaler\bin

The audit server configuration files are present in the following directories:

- On Windows: \ns\etc
- On Linux: \usr\local\netscaler\etc

The audit server executable is started as `./auditserver` in Linux and FreeBSD.

Adding the NetScaler Appliance IP Addresses on the NSLOG Server

In the configuration file (auditlog.conf), add the IP addresses of the NetScaler appliances whose events must be logged.

To add the IP addresses of the NetScaler appliance

At a command prompt, type the following command:

audserver -addns -f <directorypath>\auditlog.conf

<directorypath>: Specifies the path to the configuration file (auditlog.conf).

You are prompted to enter the information for the following parameters:

NSIP: Specifies the IP address of the NetScaler appliance, for example, 10.102.29.1.

Userid: Specifies the user name, for example, nsroot.

Password: Specifies the password, for example, nsroot.

If you add multiple NetScaler IP addresses (NSIP), and later you do not want to log all of the NetScaler appliance event details, you can delete the NSIPs manually by removing the NSIP statement at the end of the auditlog.conf file. For a high availability (HA) setup, you must add both primary and secondary NetScaler IP addresses to auditlog.conf by using the audserver command. Before adding the IP address, make sure the user name and password exist on the system.

Verifying the NSLOG Server Configuration File

Check the configuration file (audit log.conf) for syntax correctness to enable logging to start and function correctly.

To verify configuration, at a command prompt, type the following command:

audserver -verify -f <directorypath>\auditlog.conf

<directorypath>: Specifies the path to the configuration file (audit log.conf).

Running the NSLOG Server

To start audit server logging

Type the following command at a command prompt:

```
audserver -start -f <directorypath>\auditlog.conf
```

<directorypath>: Specifies the path to the configuration file (audit log.conf).

To stop audit server logging that starts as a background process in FreeBSD or Linux

Type the following command:

```
audserver -stop
```

To stop audit server logging that starts as a service in Windows

Type the following command:

```
audserver -stopservice
```

Customizing Logging on the NSLOG Server

You can customize logging on the NSLOG server by making additional modifications to the NSLOG server configuration file (log.conf). Use a text editor to modify the log.conf configuration file on the server system.

To customize logging, use the configuration file to define filters and log properties.

- **Log filters.** Filter log information from a NetScaler appliance or a set of NetScaler appliances.
- **Log properties.** Each filter has an associated set of log properties. Log properties define how to store the filtered log information.

Creating Filters

You can use the default filter definition located in the configuration file (audit log.conf), or you can modify the filter or create a new filter. You can create more than one log filter.

Note: For consolidated logging, if a log transaction occurs for which there is no filter definition, the default filter is used (if it is enabled.) The only way you can configure consolidated logging of all the NetScaler appliances is by defining the default filter.

To create a filter

At the command prompt, type the following command in the configuration file (auditlog.conf) :

filter <filterName> [IP <ip>] [NETMASK <mask>] [ON | OFF]

<filterName>: Specify the name of the filter (maximum of 64 alphanumeric characters).

<ip>: Specify the IP addresses.

<mask>: Specify the subnet mask to be used on a subnet.

Specify ON to enable the filter to log transactions, or specify OFF to disable the filter. If no argument is specified, the filter is ON

Examples

```
filter F1 IP 192.168.100.151 ON
```

To apply the filter F2 to IP addresses 192.250.100.1 to 192.250.100.254:

```
filter F2 IP 192.250.100.0 NETMASK 255.255.255.0 ON
```

filterName is a required parameter if you are defining a filter with other optional parameters, such as IP address, or the combination of IP address and Netmask.

Specifying Log Properties

Log properties associated with the filter are applied to all the log entries present in the filter. The log property definition starts with the key word BEGIN and ends with END as illustrated in the following example:

```
BEGIN <filtername>
   logFilenameFormat ...
   logDirectory ...
   logInterval ...
   logFileSizeLimit ....
END
```

Entries in the definition can include the following:

- **LogFilenameFormat** specifies the file name format of the log file. The name of the file can be of the following types:
  - Static: A constant string that specifies the absolute path and the file name.
  - Dynamic: An expression that includes the following format specifiers:
    - Date (%{format}t)
    - % creates file name with NSIP

  Example

  LogFileNameFormat Ex%{%m%d%y}t.log

  This creates the first file name as Exmmddyy.log. New files are named: Exmmddyy.log.0, Exmmddyy.log.1, and so on. In the following example, the new files are crated when the file size reaches 100MB.

  Example

  ```
  LogInterval size
  LogFileSize 100
  LogFileNameFormat Ex%{%m%d%y}t
  ```

  Caution: The date format %t specified in the LogFilenameFormat parameter overrides the log interval property for that filter. To prevent a new file being created every day instead of when the specified log file size is reached, do not use %t in the LogFilenameFormat parameter.
- **logDirectory** specifies the directory name format of the log file. The name of the file can be either of the following:

- Static: Is a constant string that specifies the absolute path and file name.
- Dynamic: Is an expression containing the following format specifiers:
  - Date (%{format}t)
  - % creates directory with NSIP

The directory separator depends on the operating system. In Windows, use the directory separator \.

Example:

LogDirectory dir1\dir2\dir3

In the other operating systems (Linux, FreeBsd, Mac, etc.), use the directory separator /.

- **LogInterval** specifies the interval at which new log files are created. Use one of the following values:
  - Hourly: A file is created every hour. Default value.
  - Daily: A file is created very day at midnight.
  - Weekly: A file is created every Sunday at midnight.
  - Monthly : A file is created on the first day of the month at midnight.
  - None: A file is created only once, when audit server logging starts.
  - Size: A file is created only when the log file size limit is reached.

Example

LogInterval Hourly

- **LogFileSizeLimit** specifies the maximum size (in MB) of the log file. A new file is created when the limit is reached.

  Note that you can override the loginterval property by assigning size as its value.

  The default LogFileSizeLimit is 10 MB.

  Example

  LogFileSizeLimit 35

Default Settings for the Log Properties

The following is an example of the default filter with default settings for the log properties:

```
begin default
 logInterval Hourly
 logFileSizeLimit 10
 logFilenameFormat  auditlog%{%y%m%d}t.log
 end default
```

Following are two examples of defining the default filters:

Example 1

```
Filter f1 IP 192.168.10.1
```

This creates a log file for NSI 192.168.10.1 with the default values of the log in effect.

Example 2

```
Filter f1 IP 192.168.10.1
begin f1
   logFilenameFormat logfiles.log
end f1
```

This creates a log file for NSIP 192.168.10.1. Since the log file name format is specified, the default values of the other log properties are in effect.

Sample Configuration File (audit.conf)

Following is a sample configuration file:

```
##############################
# This is the Auditserver configuration file
# Only the default filter is active
# Remove leading # to activate other filters
##############################
MYIP <NSAuditserverIP>
MYPORT 3023
#   Filter filter_nsip  IP <Specify the NetScaler IP address to filter on > ON
#   begin filter_nsip
#       logInterval         Hourly
#       logFileSizeLimit    10
#       logDirectory        logdir\%A\
#       logFilenameFormat   nsip%{%d%m%Y}t.log
#   end filter_nsip
Filter default
begin default
   logInterval      Hourly
   logFileSizeLimit    10
   logFilenameFormat   auditlog%{%y%m%d}t.log
end default
```

Web Server Logging

You can use the Web server logging feature to send logs of HTTP and HTTPS requests to a client system for storage and retrieval. This feature has two components:

- The Web log server, which runs on the NetScaler.
- The NetScaler Web Logging (NSWL) client, which runs on the client system.

When you run the NetScaler Web Logging (NSWL) client:

1. It connects to the NetScaler.
2. The NetScaler buffers the HTTP and HTTPS request log entries before sending them to the client.
3. The client can filter the entries before storing them.

To configure Web server logging, you first enable the Web logging feature on the NetScaler and configure the size of the buffer for temporarily storing the log entries. Then, you install NSWL on the client system. You then add the NetScaler IP address (NSIP) to the NSWL configuration file. You are now ready to start the NSWL client to begin logging. You can customize Web server logging by making additional modifications to the NSWL configuration file (log.conf).

Configuring the NetScaler for Web Server Logging

To configure the NetScaler for web server logging you are required to only enable the Web Server Logging feature. Optionally, you can perform the following configurations:

- Modify the size of the buffer (default size is 16 MB) that stores the logged information before it is sent to the NetScaler Web Logging (NSWL) client.
- Specify the custom HTTP headers that you want to export to the NSWL client. You can configure a maximum of two HTTP request and two HTTP response header names.

To configure web server logging by using the command line interface

At the command prompt, perform the following operations:

- Enable the web server logging feature.

  enable ns feature WL

- [Optional] Modify the buffer size for storing the logged information.

  set ns weblogparam -bufferSizeMB <size>

  Note: To activate your modification, you must disable and then re-enable the Web server logging feature.

- [Optional] Specify the custom HTTP header names that you want to export.

  set ns weblogparam [-customReqHdrs <*string*> ...] [-customRspHdrs <*string*> ...]

  Example

  > set ns weblogparam -customReqHdrs Accept-Encoding X-Forwarded -customRspHdrs Content-Encoding

To configure web server logging by using the configuration utility

Navigate to System > Settings and perform the following operations:

- To enable the web server logging feature, click Change Advanced Features and select Web Logging.

- To modify the buffer size, click Change Global System Settings and under Web Logging, enter the buffer size.
- To specify the custom HTTP headers to be exported, click Change Global System Settings and under Web Logging, specify the header values.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

set ns weblogparam

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Installing the NetScaler Web Logging (NSWL) Client

During installation, the NSWL client executable file (nswl) is installed along with other files. The nswl executable file provides a list of options that you can use. For details, see Configuring the NSWL Client.

Attention: The version of the NSWL client must be the same as that of the NetScaler. For example, if the version of the NetScaler is 10.1 Build 125.9, the NSWL client must also be of the same version.

The following table lists the operating systems on which the NSWL client can be installed.

Table 1. Supported Platforms for the NSWL Client with hardware requirements

Operating system	Version	Hardware requirements	Remarks
Windows	· Windows XP Professional · Windows Server 2003 · Windows 2000/NT · Windows Server 2008 · Windows Server 2008 R2	Processor - Intel x86 ~501 MHz RAM - 512 MB Controller - SCSI	
Mac OS	Mac OS 8.6 or later	-	Not supported on NetScaler 10.1 and later releases.
Linux	· RedHat Linux 4 or later · SUSE Linux Enterprise 9.3 or later	Processor - Intel x86 ~501 MHz RAM - 512 MB Controller - SCSI	
Solaris	Solaris Sun OS 5.6 or later	Processor - UltraSPARC-IIi 400 MHz RAM - 512 MB Controller - SCSI	Not supported on NetScaler 10.5 and later releases.

FreeBSD	FreeBSD 6.3 or later	Processor - Intel x86 ~501 MHz RAM - 512 MB Controller - SCSI	For NetScaler 10.5, use only FreeBSD 8.4.
AIX	AIX 6.1	-	Not supported on NetScaler 10.5 and later releases.

If the NSWL client system cannot process the log transaction because of a CPU limitation, the Web log buffer overruns and the logging process reinitiates.

Caution: Reinitiation of logging can result in loss of log transactions.

To temporarily solve a NSWL client system bottleneck caused by a CPU limitation, you can tune the Web server logging buffer size on the NetScaler appliance. To solve the problem, you need a client system that can handle the site's throughput.

Downloading the NSWL Client

You can obtain the NSWL client package from either the NetScaler product CD or the Citrix downloads site. Within the package there are separate installation packages for each supported platforms.

To download the NSWL client package from the Citrix site

1. Open the URL: https://www.citrix.com/downloads.html.
2. Log in to the site using your credentials.
3. Open the page for the required release number and build.
4. In the page, under Weblog Clients, click Download. The package has the name format as follows: Weblog-<release number>-<build number>.zip.

Installing the NSWL Client on a Solaris System

To install the NSWL client, perform the following operations on the system where you downloaded the package.

1. Extract the nswl_solaris-<release number>-<build number>.tar file from the package.
2. Copy the extracted file to a Solaris system on which you want to install the NSWL client.
3. Extract the files from the tar file with the following command:

   tar xvf nswl_solaris-9.3-51.5.tar

   A directory NSweblog is created in the temporary directory, and the files are extracted to the NSweblog directory.
4. Install the package with the following command:

   pkgadd -d

   The list of available packages appears. In the following example, one NSweblog package is shown:

   1 NSweblog NetScaler Weblogging (SunOS,sparc) 7.0
5. You are prompted to select the packages. Select the package number of the NSweblog to be installed.

   After you select the package number and press Enter, the files are extracted and installed in the following directories:

   - /usr/local/netscaler/etc
   - /usr/local/netscaler/bin
   - /usr/local/netscaler/samples
6. To check whether the NSWL package is installed, execute the following command:

   pkginfo | grep NSweblog

   Note: To uninstall the NSWL package, execute the following command:

   pkgrm NSweblog

Installing the NSWL Client on a Linux System

To install the NSWL client, perform the following operations on the system where you downloaded the package.

1. Extract the nswl_linux-<release number>-<build number>.rpm file from the package.
2. Copy the extracted file to a system, running Linux OS, on which you want to install the NSWL client.
3. To install the NSWL package, execute the following command:

   rpm -i nswl_linux-9.3-51.5.rpm

   This command extracts the files and installs them in the following directories.

   - /usr/local/netscaler/etc
   - /usr/local/netscaler/bin
   - /usr/local/netscaler/samples

   Note: To uninstall the NSWL package, execute the following command:

   rpm -e NSweblog

   Note: To get more information about the NSweblog RPM file, execute the following command:

   rpm -qpi *.rpm

   Note: To view the installed Web server logging files, execute the following command:

   rpm -qpl *.rpm

Installing the NSWL Client on a FreeBSD System

To install the NSWL client, perform the following operations on the system where you downloaded the package.

1. Extract the nswl_bsd-<release number>-<build number>.tgz file from the package.
2. Copy the extracted file to a system, running FreeBSD OS, on which you want to install the NSWL client.
3. To install the NSWL package, execute the following command:

   pkg_add nswl_bsd-9.3-51.5.tgz

   This command extracts the files and installs them in the following directories.

   - /usr/local/netscaler/etc
   - /usr/local/netscaler/bin
   - /usr/local/netscaler/samples

   Note: To uninstall the NSWL package, execute the following command:

   pkg_delete NSweblog

4. To verify that the package is installed, execute the following command:

   pkg_info | grep NSweblog

Installing the NSWL Client on a Mac System

To install the NSWL client, perform the following operations on the system where you downloaded the package.

1. Extract the nswl_macos-<release number>-<build number>.tgz file from the package.
2. Copy the extracted file to a system, running Mac OS, on which you want to install the NSWL client.
3. To install the NSWL package, execute the following command:

   pkg_add nswl_macos-9.3-51.5.tgz

   This command extracts the files and installs them in the following directories:

   - /usr/local/netscaler/etc
   - /usr/local/netscaler/bin
   - /usr/local/netscaler/samples

   Note: To uninstall the NSWL package, execute the following command:

   pkg_delete NSweblog

4. To verify that the package is installed, execute the following command:

   pkg_info | grep NSweblog

Installing the NSWL Client on a Windows System

To install the NSWL client, perform the following operations on the system where you downloaded the package.

1. Extract the nswl_win-<release number>-<build number>.zip file from the package.
2. Copy the extracted file to a Windows system on which you want to install the NSWL client.
3. On the Windows system, unzip the file in a directory (referred as <NSWL-HOME>). The following directories are extracted: bin, etc, and samples.
4. At the command prompt, run the following command from the <NSWL-HOME>\bin directory:

   nswl -install -f <directorypath>\log.conf

   where,

   <directorypath> refers to the path of the configuration file (log.conf). By default, the file is in the <NSWL-HOME>\etc directory. However, you can copy the configuration file to any other directory.

   Note: To uninstall the NSWL client, at the command prompt, run the following command from the <NSWL-HOME>\bin directory:

   > nswl -remove

Installing the NSWL Client on a AIX System

To install the NSWL client, perform the following operations on the system where you downloaded the package.

1. Extract the nswl_aix-<release number>-<build number>.rpm file from the package.
2. Copy the extracted file to a system, running AIX OS, on which you want to install the NSWL client.
3. To install the NSWL package, execute the following command:

   rpm -i nswl_aix-9.3-51.5.rpm

   This command extracts the files and installs them in the following directories.

   - /usr/local/netscaler/etc
   - /usr/local/netscaler/bin
   - /usr/local/netscaler/samples

   Note: To uninstall the NSWL package, execute the following command:

   rpm -e NSweblog

   Note: To get more information about the NSweblog RPM file, execute the following command:

   rpm -qpi *.rpm

   Note: To view the installed Web server logging files, execute the following command:

   rpm -qpl *.rpm

Configuring the NSWL Client

After installing the NSWL client, you can configure the NSWL client using the nswl executable. These configurations are then stored in the NSWL client configuration file (log.conf).

Note: You can further customize logging on the NSWL client system by making additional modifications to the NSWL configuration file (log.conf). For details, see Customizing Logging on the NSWL Client System.

The following table describes the commands that you can use to configure the NSWL client.

NSWL command	Specifies
nswl -help	The available NSWL help options.
nswl -addns -f <path-to-configuration-file>	The system that gathers the log transaction data. You are prompted to enter the IP address of the NetScaler appliance. Enter a valid user name and password.
nswl -verify -f <path-to-configuration-file>	Check for syntax or semantic errors in the configuration file.
nswl -start -f <path-to-configuration-file>	Start the NSWL client based on the settings in the configuration file. **Note:** For Solaris and Linux: To start Web server logging as a background process, type the ampersand sign (&) at the end of the command.
nswl -stop (Solaris and Linux only)	Stop the NSWL client if it was started as a background process; otherwise, use CTRL+C to stop Web server logging.
nswl -install -f <path-to-configuration-file> (Windows only)	Install the NSWL client as a service in Windows.
nswl -startservice (Windows only)	Start the NSWL client by using the settings in the configuration file specified in the nswl install option. You can also start NSWL client from Start > Control Panel > Services.
nswl -stopservice (Windows only)	Stops the NSWL client.
nswl -remove	Remove the NSWL client service from the registry.

Run the following commands from the directory in which the NSWL executable is located:

- Windows: \ns\bin
- Solaris and Linux: \usr\local\netscaler\bin

The Web server logging configuration files are located in the following directory path:

- Windows: \ns\etc
- Solaris and Linux: \usr\local\netscaler\etc

The NSWL executable is started as .\nswl in Linux and Solaris.

Adding the IP Addresses of the NetScaler Appliance

In the NSWL client configuration file (log.conf), add the NetScaler IP address (NSIP) from which the NSWL client will start collecting logs.

To add the NSIP address of the NetScaler appliance

1. At the client system command prompt, type:

   `nswl -addns -f` < directorypath > `\log.conf`

   < directorypath >: Specifies the path to the configuration file (log.conf).

2. At the next prompt, enter the following information:

   - **NSIP**: Specify the IP address of the NetScaler appliance.
   - Username and Password: Specify the `nsroot` user credentials of the NetScaler appliance.

Note: If you add multiple NetScaler IP addresses (NSIP), and later you do not want to log all of NetScaler system log details, you can delete the NSIPs manually by removing the NSIP statement at the end of the log.conf file. During a failover setup, you must add both primary and secondary NetScaler IP addresses to the log.conf by using the command. Before adding the IP address, make sure the user name and password exist on the NetScaler appliances.

Verifying the NSWL Configuration File

To make sure that logging works correctly, check the NSWL configuration file (log.conf) on the client system for syntax errors.

To verify the configuration in the NSWL configuration file

At the client system command prompt, type:

`nswl` -verify -f <directorypath>\log.conf

< directorypath >: Specifies the path to the configuration file (log.conf).

Running the NSWL Client

To start Web server logging

At the client system command prompt, type:

`nswl -start -f <directorypath>\log.conf`

<directorypath>: Specifies the path to the configuration file (log.conf).

To stop Web server logging started as a background process on the Solaris or Linux operating systems

At the command prompt, type:

`nswl -stop`

To stop Web server logging started as a service on the Windows operating system

At the command prompt, type:

`nswl -stopservice`

Customizing Logging on the NSWL Client System

You can customize logging on the NSWL client system by making additional modifications to the NSWL client configuration file (log.conf). Use a text editor to modify the log.conf configuration file on the client system.

To customize logging, use the configuration file to define filters and log properties.

- **Log filters.** Filter log information based on the host IP address, domain name, and host name of the Web servers.
- **Log properties.** Each filter has an associated set of log properties. Log properties define how to store the filtered log information.

Sample Configuration File

Following is a sample configuration file:

```
##########
# This is the NSWL configuration file
# Only the default filter is active
# Remove leading # to activate other filters
##########
##########
# Default filter (default on)
# W3C Format logging, new file is created every hour or on reaching 10MB file size,
# and the file name is Exyymmdd.log
##########
Filter default
begin default
	logFormat		W3C
	logInterval		Hourly
	logFileSizeLimit	10
	logFilenameFormat	Ex%{%y%m%d}t.log
end default
##########
# netscaler caches example
# CACHE_F filter covers all the transaction with HOST name www.netscaler.com and the listed server ip's
##########
#Filter CACHE_F HOST www.netscaler.com IP 192.168.100.89 192.168.100.95 192.168.100.52 192.168.100.53
##########
# netscaler origin server example
# Not interested in Origin server to Cache traffic transaction logging
##########
#Filter ORIGIN_SERVERS IP 192.168.100.64 192.168.100.65 192.168.100.66 192.168.100.67 192.168.100.225 1
100.227 192.168.100.228 OFF
##########
# netscaler image server example
# all the image server logging.
##########
#Filter IMAGE_SERVER HOST www.netscaler.images.com IP 192.168.100.71 192.168.100.72 192.168.100.169
0.171 ON
##########
# NCSA Format logging, new file is created every day midnight or on reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.log.
# Exclude objects that ends with .gif .jpg .jar.
##########
#begin ORIGIN_SERVERS
#	logFormat		NCSA
#	logInterval		Daily
#	logFileSizeLimit	40
#	logFilenameFormat	/datadisk5/ORGIN/log/%v/NS%{%m%d%y}t.log
#	logExclude		.gif .jpg .jar
```

```
#end ORIGIN_SERVERS

##########
# NCSA Format logging, new file is created every day midnight or on reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.log with log record timestamp as
##########
#begin CACHE_F
#       logFormat             NCSA
#       logInterval           Daily
#       logFileSizeLimit       20
#       logFilenameFormat /datadisk5/netscaler/log/%v/NS%{%m%d%y}t.log
#       logtime               GMT
#end CACHE_F

##########
# W3C Format logging, new file on reaching 20MB and the log file path name is
# atadisk6/netscaler/log/server's ip/Exmmyydd.log with log record timestamp as LOCAL.
##########
#begin IMAGE_SERVER
#       logFormat             W3C
#       logInterval           Size
#       logFileSizeLimit       20
#       logFilenameFormat /datadisk6/netscaler/log/%AEx%{%m%d%y}t
#       logtime               LOCAL
#end IMAGE_SERVER

##########
# Virtual Host by Name firm, can filter out the logging based on the host name by,
##########

#Filter VHOST_F IP 10.101.2.151 NETMASK 255.255.255.0
#begin VHOST_F
#       logFormat             W3C
#       logInterval           Daily
#       logFileSizeLimit       10
logFilenameFormat /ns/prod/vhost/%v/Ex%{%m%d%y}t
#end VHOST_F

########## END FILTER CONFIGURATION ##########
```

Creating Filters

You can use the default filter definition located in the configuration file (log.conf), or you can modify the filter or create a new filter. You can create more than one log filter.

Note: Consolidated logging, which logs transactions for which no filter is defined, uses the default filter if it is enabled. Consolidated logging of all servers can be done by defining only the default filter.

If the server hosts multiple Web sites and each Web site has its own domain name, and each domain is associated with a virtual server, you can configure Web server logging to create a separate log directory for each Web site. The following table displays the parameters for creating a filter.

Table 1. Parameters for Creating a Filter

Parameter	Specifies
filterName	Name of the filter. The filter name can include alphanumeric characters and cannot be longer than 59 characters. Filter names longer than 59 characters are truncated to 59 characters.
HOST name	Host name of the server for which the transactions are being logged.
IP ip	IP address of the server for which transactions are to be logged (for example, if the server has multiple domains that have one IP address).
IP ip 2...ip n:	Multiple IP addresses (for example, if the server domain has multiple IP addresses).
ip6 ip	IPv6 address of the server for which transactions are to be logged.
IP ip NETMASK mask	IP addresses and netmask combination to be used on a subnet.
ON | OFF	Enable or disable the filter to log transactions. If no argument is selected, the filter is enabled (ON).

To create a filter

To create a filter, enter the following command in the log.conf file:

- `filter` <filterName> <HOST name> | [IP<ip>] | [IP<ip 2...ip n>] | <IP ip NETMASK mask> [ON | OFF]

- `filter` <filterName> <HOST name> | [IP6 ip/<prefix length>] [ON | OFF]

To create a filter for a virtual server

To create a filter for a virtual server, enter the following command in the log.conf file:

`filter` <filterName> <VirtualServer IP address>

Example

In the following example, you specify an IP address of 192.168.100.0 and netmask of 255.255.255.0. The filter applies to IP addresses 192.168.100.1 through 192.168.100.254.

Filter F1 HOST www.netscaler.com ON
Filter F2 HOST www.netscaler.com IP 192.168.100.151 ON
Filter F3 HOST www.netscaler.com IP 192.168.100.151 192.165.100.152 ON
Filter F4 IP 192.168.100.151
Filter F5 IP 192.168.100.151 HOST www.netscaler.com OFF
Filter F6 HOST www.netscaler.com HOST www.xyz.com HOST www.abcxyz.com IP 192.168.100.200 ON
Filter F7 IP 192.250.100.0 NETMASK 255.255.255.0
Filter F8 HOST www.xyz.com IP 192.250.100.0 NETMASK 255.255.255.0 OFF
For creating filters for servers having IPv6 addresses.
Filter F9 2002::8/112 ON
Filter F10 HOST www.abcd.com IP6 2002::8 ON

Specifying Log Properties

Log properties are applied to all log entries associated with the filter. The log property definition begins with the keyword BEGIN and ends with END as illustrated in the following example:

```
BEGIN <filtername>
 logFormat ...
 logFilenameFormat ...
 logInterval ...
 logFileSize ....
 logExclude ....
 logTime ….
 END
```

Entries in the definition can include the following:

- **LogFormat** specifies the Web server logging feature that supports NCSA, W3C Extended, and custom log file formats.

  By default, the logformat property is w3c. To override, enter custom or NCSA in the configuration file, for example:

  ```
  LogFormat NCSA
  ```

  Note: For the NCSA and custom log formats, local time is used to time stamp transactions and for file rotation.

- **LogInterval** specifies the intervals at which new log files are created. Use one of the following values:

  - Hourly: A file is created every hour.
  - Daily: A file is created every day at midnight. Default value.
  - Weekly: A file is created every Sunday at midnight.
  - Monthly: A file is created on the first day of the month at midnight.
  - None: A file is created only once, when Web server logging starts.

  Example

  ```
  LogInterval Daily
  ```

- **LogFileSizeLimit** specifies the maximum size of the log file in MB. It can be used with any log interval (weekly, monthly, and so on.) A file is created when the maximum file size limit is reached or when the defined log interval time elapses.

To override this behavior, specify the size as the loginterval property so that a file is created only when the log file size limit is reached.

The default LogFileSizeLimit is 10 MB.

Example

```
LogFileSizeLimit 35
```

- **LogFilenameFormat** specifies the file name format of the log file. The name of the file can be of the following types:
  - Static: Specifies a constant string that contains the absolute path and file name.
  - Dynamic: Specifies an expression containing the following format:
    - Server IP address (%A)
    - Date (%{format}t)
    - URL suffix (%x)
    - Host name (%v)

Example

```
LogFileNameFormat Ex%{%m%d%y}t.log
```

This command creates the first file name as Exmmddyy.log, then every hour creates a file with file name: Exmmddyy.log.0, Exmmddyy.log.1,..., Exmmddyy.log.n.

Example

```
LogInterval size
LogFileSize 100
LogFileNameFormat Ex%{%m%d%y}t
```

Caution: The date format %t specified in the LogFilenameFormat command overrides the log interval property for that filter. To prevent a new file being created every day instead of when the specified log file size is reached, do not use %t in the LogFilenameFormat.

- **LogExclude** prevents logging of transactions with the specified file extensions.

Example

```
LogExclude .html
```

This command creates a log file that excludes log transactions for *.html files.

- **LogTime** specifies log time as either GMT or LOCAL.

The defaults are:

- NCSA log file format: LOCAL
- W3C log file format: GMT.

Understanding the NCSA and W3C Log Formats

The NetScaler supports the following standard log file formats:

- NCSA Common Log Format
- W3C Extended Log Format

NCSA Common Log Format

If the log file format is NCSA, the log file displays log information in the following format:

Client_IP_address -User_Name [Date:Time -TimeZone] "Method Object HTTP_version" HTTP_StatusCode BytesSent

To use the NCSA Common log format, enter NCSA in the LogFormat argument in the log.conf file.

The following table describes the NCSA Common log format.

Table 1. NCSA Common Log Format

Argument	Specifies
Client _IP_address	The IP address of the client computer.
User Name	The user name.
Date	The date of the transaction.
Time	The time when the transaction was completed.
Time Zone	The time zone (Greenwich Mean Time or local time).
Method	The request method (for example; GET, POST).
Object	The URL.
HTTP_version	The version of HTTP used by the client.
HTTP_StatusCode	The status code in the response.
Bytes Sent	The number of bytes sent from the server.

W3C Extended Log Format

An extended log file contains a sequence of lines containing ASCII characters terminated by either a Line Feed (LF) or the sequence Carriage Return Line Feed (CRLF.) Log file generators must follow the line termination convention for the platform on which they are run.

Log analyzers must accept either LF or CRLF form. Each line may contain either a directive or an entry. If you want to use the W3C Extended log format, enter W3C as the Log-Format argument in the log.conf file.

By default, the standard W3C log format is defined internally as the custom log format, shown as follows:

```
%{%Y-%m-%d%H:%M:%S}t %a %u %S %A %p %m %U %q %s %j %J %T %H %+{user-agent}i %+{cookie} i%+{referer}i
```

For a description of the meaning of this each custom format, see "Appendix A: Arguments for Defining a Custom Log Format." You can also change the order or remove some fields in this W3C log format. For example:

```
logFormat W3C %{%Y-%m-%d%H:%M:%S}t %m %U
```

W3C log entries are created with the following format:

```
#Version: 1.0
#Fields: date time cs-method cs-uri
#Date: 12-Jun-2001 12:34
2001-06-12 12:34:23 GET /sports/football.html
2001-06-12 12:34:30 GET /sports/football.html
```

Entries

Entries consist of a sequence of fields relating to a single HTTP transaction. Fields are separated by white space; Citrix recommends the use of tab characters. If a field in a particular entry is not used, a dash (-) marks the omitted field.

Directives

Directives record information about the logging process. Lines beginning with the pound sign (#) contain directives.

The following table describes the directives.

Table 2. Directive Descriptions

Directive	Description

Version: <integer>.<integer>	Displays the version of the extended log file format used. This document defines version 1.0.
Fields: [<specifier>...]	Identifies the fields recorded in the log.
Software: <string>	Identifies the software that generated the log.
Start-Date: <date> <time>	Displays the date and time at which the log was started.
End-Date: <date> <time>	Displays the date and time at which logging finished.
Date: <date> <time>	Displays the date and time when the entry was added.
Remark: <text>	Displays comments. Analysis tools ignore data recorded in this field.

Note: The Version and Fields directives are required. They precede all other entries in the log file.

Example

The following sample log file shows the log entries in W3C Extended log format:

```
#Version: 1.0
#Fields: time cs-method cs-uri
#Date: 12-Jan-1996 00:00:00
00:34:23 GET /sports/football.html
12:21:16 GET /sports/football.html
12:45:52 GET /sports/football.html
12:57:34 GET /sports/football.html
```

Fields

The Fields directive lists a sequence of field identifiers that specify the information recorded in each entry. Field identifiers may have one of the following forms:

- **identifier:** Relates to the transaction as a whole.
- **prefix-identifier:** Relates to information transfer between parties defined by the value *prefix*.
- **prefix (header):** Specifies the value of the HTTP header field header for transfer between parties defined by the value *prefix*. Fields specified in this manner always have the type <string>.

The following table describes defined prefixes.

Table 3. Prefix Descriptions

Prefix	Specifies
c	Client
s	Server
r	Remote
cs	Client to server
sc	Server to client
sr	Server to remote server (prefix used by proxies)
rs	Remote server to server (prefix used by proxies)
x	Application-specific identifier

Examples

The following examples are defined identifiers that use prefixes:

cs-method: The method in the request sent by the client to the server.

sc(Referer): The Referer field in the reply.

c-ip: The IP address of the client.

Identifiers

The following table describes the W3C Extended log format identifiers that do not require a prefix.

Table 4. W3C Extended Log Format Identifiers (No Prefix Required)

Identifier	Description
date	The date on which the transaction was done.
time	The time when the transaction is done.
time-taken	The time taken (in seconds) for the transaction to complete.
bytes	The number of bytes transferred.
cached	Records whether a cache hit has occurred. A zero indicates a cache miss.

The following table describes the W3C Extended log format identifiers that require a prefix.

Table 5. W3C Extended Log Format Identifiers (Requires a Prefix)

Identifier	Description
IP	The IP address and the port number.
dns	The DNS name.
status	The status code.

comment	The comment returned with status code.
method	The method.
url	The URL.
url-stem	The stem portion of the URL.
url-query	The query portion of the URL.

The W3C Extended Log file format allows you to choose log fields. These fields are shown in the following table.

Table 6. W3C Extended Log File Format (Allows Log Fields)

Field	Description
Date	The date on which the transaction is done.
Time	The time when the transaction is done.
Client IP	The IP address of the client.
User Name	The user name.
Service Name	The service name, which is always HTTP.
Server IP	The server IP address.
Server Port	The server port number
Method	The request method (for example; GET, POST).
Url Stem	The URL stem.
Url Query	The query portion of the URL.
Http Status	The status code in the response.
Bytes Sent	The number of bytes sent to the server (request size, including HTTP headers).
Bytes Received	The number of bytes received from the server (response size, including HTTP headers).
Time Taken	The time taken for transaction to complete, in seconds.
Protocol Version	The version number of HTTP being used by the client.
User Agent	The User-Agent field in the HTTP protocol.
Cookie	The Cookie field of the HTTP protocol.
Referer	The Referer field of the HTTP protocol.

Creating a Custom Log Format

You can customize the display format of the log file data manually or by using the NSWL library. By using the custom log format, you can derive most of the log formats that Apache currently supports.

Creating a Custom Log Format by Using the NSWL Library

Use one of the following NSWL libraries depending on whether the NSWL executable has been installed on a Windows or Solaris host computer:

- **Windows:** The nswl.lib library located in \ns\bin directory on the system manager host computer.
- **Solaris:** The libnswl.a library located in /usr/local/netscaler/bin.

To create the custom log format by using the NSWL Library

1. Add the following two C functions defined by the system in a C source file:

   ns_userDefFieldName() : This function returns the string that must be added as a custom field name in the log record.

   ns_userDefFieldVal() : This function implements the custom field value, then returns it as a string that must be added at the end of the log record.

2. Compile the file into an object file.
3. Link the object file with the NSWL library (and optionally, with third party libraries) to form a new NSWL executable.
4. Add a %d string at the end of the logFormat string in the configuration file (log.conf).

Example

```
##########
# A new file is created every midnight or on reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.log and create digital
#signature field for each record.
BEGIN CACHE_F
   logFormat   custom "%a - "%{user-agent}i" [%d/%B/%Y %T -%g] "%x" %s %b%{referrer}i "%{user-agent}i" "%{coo
   logInterval         Daily
   logFileSizeLimit        20
   logFilenameFormat       /datadisk5/netscaler/log/%v/NS%{%m%d%y}t.log
END CACHE_F
```

Creating a Custom Log Format Manually

To customize the format in which log file data should appear, specify a character string as the argument of the LogFormat log property definition. For more information, see "Appendix A: Arguments for Defining a Custom Log Format." The following is an example where character strings are used to create a log format:

```
LogFormat Custom ""%a - "%{user-agent}i" %[%d/%m/%Y]t %U %s %b %T"
```

- The string can contain the “c” type control characters \n and \t to represent new lines and tabs.
- Use the <Esc> key with literal quotes and backslashes.

The characteristics of the request are logged by placing % directives in the format string, which are replaced in the log file by the values.

If the %v (Host name) or %x (URL suffix) format specifier is present in a log file name format string, the following characters in the file name are replaced by an underscore symbol in the log configuration file name:

" * . / : < > ? \ |

Characters whose ASCII values lie in the range of 0-31 are replaced by the following:

%<ASCII value of character in hexadecimal>.

For example, the character with ASCII value 22 is replaced by %16.

Caution: If the %v format specifier is present in a log file name format string, a separate file is opened for each virtual host. To ensure continuous logging, the maximum number of files that a process can have open should be sufficiently large. See your operating system documentation for a procedure to change the number of files that can be opened.

Creating Apache Log Formats

You can derive from the custom logs most of the log formats that Apache currently supports. The custom log formats that match Apache log formats are:

NCSA/combined: LogFormat custom `%h %l %u [%t] "%r" %s %B "%{referer}i" "%{user-agent}i"`

NCSA/Common: LogFormat custom `%h %l %u [%t] "%r" %s %B`

Referer Log: LogFormat custom `"%{referer}i" -> %U`

Useragent: LogFormat custom `%{user-agent}i`

Similarly, you can derive the other server log formats from the custom formats.

Arguments for Defining a Custom Log Format

The following table describes the data that you can use as the Log Format argument string:

Table 1. Custom Log Format

Argument	Specifies
%a	Remote IPv4 address.
%A	Local IPv4 address.
%a6	Remote IPv6 address.
%A6	Local IPv6 address.
%B	Bytes sent, excluding the HTTP headers (response size).
%b	Bytes received, excluding the HTTP headers (request size).
%d	User-defined field.
%g	Greenwich Mean Time offset (for example, -0800 for Pacific Standard Time).
%h	Remote host.
%H	Request protocol.
%{Foobar}i	Contents of the Foobar: header line(s) in the request sent to the server. The system supports the User-Agent, Referer and cookie headers. The + after the % in this format informs the logging client to use the + as a word separator.
%j	Bytes received, including headers (request size)
%J	Bytes sent, including headers (response size)
%l	Remote log name (from identd, if supplied).
%m	Request method.
%M	Time taken to serve the request (in microseconds)
%{Foobar}o	Contents of Foobar: header line(s) in the reply. USER-AGENT, Referer, and cookie headers (including set cookie headers) are supported.

%p	Canonical port of the server serving the request.
%q	Query string (prefixed with a question mark (?) if a query string exists).
%r	First line of the request.
%s	Requests that were redirected internally, this is the status of the original request.
%t	Time, in common log format (standard English time format).
%{format}t	Time, in the form given by format, must be in the strftime(3) format. For format descriptions, see "Appendix B: Time Format Definition."
%T	Time taken to serve the request, in seconds.
%u	Remote user (from auth; may be bogus if return status (%s) is 401).
%U	URL path requested.
%v	Canonical name of the server serving the request.
%V	Virtual server IPv4 address in the system, if load balancing, content switching, and/or cache redirection is used.
%V6	Virtual server IPv6 address in the system, if load balancing, content switching, and/or cache redirection is used.

For example, if you define the log format as `%+{user-agent}i`, and if the user agent value is Citrix NetScaler system Web Client, then the information is logged as NetScaler system+Web+Client. An alternative is to use double quotation marks. For example, `“%{user-agent}i”` logs it as “Citrix NetScaler system Web Client.” Do not use the <Esc> key on strings from `%.. .r, %. . .i` and, `%. . .o`. This complies with the requirements of the Common Log Format. Note that clients can insert control characters into the log. Therefore, you should take care when working with raw log files.

Time Format Definition

The following table lists the characters that you can enter as the format part of the %{format}t string described in the Custom Log Format table of "Arguments for Defining a Custom Log Format." Values within brackets ([ ]) show the range of values that appear. For example, [1,31] in the %d description in the following table shows %d ranges from 1 to 31.

Table 1. Time Format Definition

Argument	Specifies
%%	The same as %.
%a	The abbreviated name of the week day for the locale.
%A	The full name of the week day for the locale.
%b	The abbreviated name of the month for the locale.
%B	The full name of the month for the locale.
%C	The century number (the year divided by 100 and truncated to an integer as a decimal number [1,99]); single digits are preceded by a 0.
%d	The day of month [1,31]; single digits are preceded by 0.
%e	The day of month [1,31]; single digits are preceded by a blank.
%h	The abbreviated name of the month for the locale.
%H	The hour (24-hour clock) [0,23]; single digits are preceded by a 0.
%I	The hour (12-hour clock) [1,12]; single digits are preceded by a 0.
%j	The number of the day in the year [1,366]; single digits are preceded by 0.
%k	The hour (24-hour clock) [0,23]; single digits are preceded by a blank.
%l	The hour (12-hour clock) [1,12]; single digits are preceded by a blank.
%m	The number of the month in the year [1,12]; single digits are preceded by a 0.
%M	The minute [00,59]; leading 0 is permitted but not required.

%n	Inserts a new line.
%p	The equivalent of either a.m. or p.m. for the locale.
%r	The appropriate time representation in 12-hour clock format with %p.
%S	The seconds [00,61]; the range of values is [00,61] rather than [00,59] to allow for the occasional leap second and for the double leap second.
%t	Inserts a tab.
%u	The day of the week as a decimal number [1,7]. 1 represents Sunday, 2 represents Tuesday and so on.
%U	The number of the week in the year as a decimal number [00,53], with Sunday as the first day of week 1.
%w	The day of the week as a decimal number [0,6]. 0 represents Sunday.
%W	Specifies the number of the week in the year as a decimal number [00,53]. Monday is the first day of week 1.
%y	The number of the year within the century [00,99]. For example, 5 would be the fifth year of that century.
%Y	The year, including the century (for example, 1993).

Note: If you specify a conversion that does not correspond to any of the ones described in the preceding table, or to any of the modified conversion specifications listed in the next paragraph, the behavior is undefined and returns 0.

The difference between %U and %W (and also between modified conversions %OU and %OW) is the day considered to be the first day of the week. Week number 1 is the first week in January (starting with a Sunday for %U, or a Monday for %W). Week number 0 contains the days before the first Sunday or Monday in January for %U and %W.

Advanced Configurations

If you enable path maximum transmission unit (PMTU) discovery, the NetScaler can use it to determine the maximum transmission unit of any Internet channel. For more efficient data transfer, you can configure TCP window scaling and selective acknowledgment. You can view statistics associated with HTTP request and response sizes. For applying a specific HTTP and TCP settings to vservers and services, you can configure HTTP and TCP profiles.

Configuring Clock Synchronization

You can configure your NetScaler appliance to synchronize its local clock with a Network Time Protocol (NTP) server. This ensures that its clock has the same date and time settings as the other servers on your network.

You can configure clock synchronization on your appliance by adding NTP server entries to the ntp.conf file from either the configuration utility or the command line interface, or by manually modifying the ntp.conf file and then starting the NTP daemon (NTPD). The clock synchronization configuration does not change if the appliance is restarted, upgraded, or downgraded. However, the configuration does not get propagated to the secondary NetScaler in a high availability setup.

Note: If you do not have a local NTP server, you can find a list of public, open access, NTP servers at the official NTP site, http://www.ntp.org, under Public Time Servers List. Before configuring your NetScaler to use a public NTP server, be sure to read the Rules of Engagement page (link included on all Public Time Servers pages).

Setting Up Clock Synchronization

To configure clock synchronization, you must add NTP servers and then enable NTP synchronization.

To add an NTP server by using the command line interface

At the command prompt, type the following commands to add an NTP server and verify the configuration:

- add ntp server (<serverIP> | <serverName>) [-minpoll <positive_integer>] [-maxpoll <positive_integer>]
- show ntp server

Example

> add ntp server 10.102.29.30 -minpoll 6 -maxpoll 11

To configure an NTP server by using the configuration utility

Navigate to System > NTP Servers, and create the NTP server.

Parameter Descriptions (of commands listed in the CLI procedure)

add ntp server

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ntp server

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Starting the NTP Daemon

When you enable NTP synchronization, the NetScaler starts the NTP daemon and uses the NTP server entries in the ntp.conf file to synchronize its local time setting. If you do not want to synchronize the appliance time with the other servers in the network, you can disable NTP synchronization, which stops the NTP daemon (NTPD).

To enable NTP synchronization by using the command line interface

At the command prompt, type one of the following commands:

enable ntp sync

To enable NTP synchronization by using the configuration utility

Navigate to System > NTP Servers, click Action and select NTP Synchronization.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ntp sync

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Clock Synchronization Manually

You can configure clock synchronization manually by logging on to the NetScaler and editing the ntp.conf file.

To enable clock synchronization on your NetScaler by modifying the ntp.conf file

1. Log on to the command line interface.
2. Switch to the shell prompt.
3. Copy the /etc/ntp.conf file to /nsconfig/ntp.conf, unless the /nsconfig directory already contains an ntp.conf file.
4. Check the /nsconfig/ntp.conf file for the following entries and, if they are present, remove them:

   restrict localhost

   restrict 127.0.0.2
5. Add the IP address for the desired NTP server to the /nsconfig/ntp.conf file, beneath the file's server and restrict entries.

   Note: For security reasons, there should be a corresponding restrict entry for each server entry.
6. If the /nsconfig directory does not contain a file named rc.netscaler, create the file.
7. Add the following entry to /nsconfig/rc.netscaler: `/usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ntpd.log &`

   This entry starts the ntpd service, checks the ntp.conf file, and logs messages in the /var/log directory.

   This process runs every time the NetScaler is restarted.
8. Reboot the NetScaler to enable clock synchronization.

   Note:

   If you want to start the time synchronization process without restarting the NetScaler, run the following command from the shell prompt:

   ```
   /usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ntpd.log &
   ```

Viewing the System Date and Time

To change the system date and time, you must use the shell interface to the underlying FreeBSD OS. However, to view the system date and time, you can use the command line interface or the configuration utility.

To view the system date and time by using the command line interface

At the command prompt, type:

show ns config

To view the system date and time by using the configuration utility

Navigate to System and select the System Information tab to view the system date.

Parameter Descriptions (of commands listed in the CLI procedure)

show ns config

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring TCP Window Scaling

The TCP window scaling option, which is defined in RFC 1323, increases the TCP receive window size beyond its maximum value of 65,535 bytes. This option is required for efficient transfer of data over long fat networks (LFNs).

A TCP window determines the amount of outstanding (unacknowledged by the recipient) data a sender can send on a particular connection before receiving any acknowledgment from the receiver. The main purpose of the window is flow control.

The window size field in the TCP header is 16 bits, which limits the ability of the sender to advertise a window size larger than 65535 (2^16 - 1). The TCP window scale extension expands the definition of the TCP window by applying a scale factor to the value in the 16 bit window size field of the TCP header. (Although RFC 1323 describes expanding the definition to up to 30 bits, NetScaler window scaling expands the definition of the TCP window to up to 24 bits.) The scale factor is carried in the new TCP window scale field. This field is sent only in a SYN packet (a segment with the SYN bit on)

To fit a larger window size value into the 16-bit field, the sender right shifts the value by the number of bit positions specified by the scale factor. The receiver left shifts the value by the same number of positions. Therefore, the actual window size is equivalent to:

(2^<scale factor>) * <received window size>

Before configuring window scaling, make sure that:

- You do not set a high value for the scale factor, because this could have adverse effects on the appliance and the network.
- You have enabled selective acknowledgment (SACK).
- You do not configure window scaling unless you clearly know why you want to change the window size.
- Both hosts in the TCP connection send a window scale option during connection establishment. If only one side of a connection sets this option, windows scaling is not used for the connection.
- Each connection for same session is an independent Window Scaling session. For example, when a client's request and the server's response flow through the appliance, it is possible to have window scaling between the client and the appliance without window scaling between the appliance and the server.

By default, window scaling is not enabled.

To configure window scaling by using the command line interface

At the command prompt, type the following commands to configure window scaling and verify the configuration:

- set ns tcpParam -WS (ENABLED | DISABLED) -WSVal <positive_integer>
- show ns tcpParam

Example

```
> set ns tcpParam -WS ENABLED -WSVal 6
```

To configure window scaling by using the configuration utility

1. Navigate to System > Settings.
2. In the details pane, under Settings, click Configure TCP Parameters.
3. In the Configure TCP Parameters dialog box, under TCP Window Scaling, select the Windows Scaling check box to enable window scaling and set the window scaling Factor.
4. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set ns tcpParam

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns tcpParam

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Selective Acknowledgment (SACK)

NetScaler appliances support Selective Acknowledgment (SACK), as defined in RFC 2018. Using SACK, the data receiver (either a NetScaler appliance or a client) notifies the sender about all the segments that have been received successfully. As a result, the sender (either a NetScaler appliance or a client) needs to retransmit only those segments that were lost during transmission. This improves the performance of data transmission. SACK is important in long fat networks (LFNs). By default, SACK is disabled.

To enable Selective Acknowledgment (SACK) by using the command line interface

At the command prompt, type the following commands to enable Selective Acknowledgment (SACK) and verify the configuration:

- set ns tcpParam -SACK (ENABLED | DISABLED)
- show ns tcpParam

Example

```
> set ns tcpParam -SACK ENABLED
```

To enable Selective Acknowledgment (SACK) by using the configuration utility

1. Navigate to System > Settings.
2. In the details pane, under Settings, click Change TCP Parameters.
3. In the Configure TCP Parameters dialog box, under TCP, select the Selective Acknowledgment check box. For a description of a parameter, hover the mouse cursor over the check box.
4. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set ns tcpParam

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns tcpParam

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Clearing the NetScaler Configuration

You have the following three options for clearing the NetScaler configuration.

Basic level. Clearing your configuration at the basic level clears all settings except the following:

- NSIP, MIP(s), and SNIP(s)
- Network settings (Default Gateway, VLAN, RHI, NTP, and DNS settings)
- HA node definitions
- Feature and mode settings
- Default administrator password (nsroot)

Extended level. Clearing your configuration at the extended level clears all settings except the following:

- NSIP, MIP(s), and SNIP(s)
- Network settings (Default Gateway, VLAN, RHI, NTP, and DNS settings)
- HA node definitions

Feature and mode settings revert to their default values.

Full level. Clearing your configuration at the full level returns all settings to their factory default values. However, the NSIP and default gateway are not changed, because changing them could cause the appliance to lose network connectivity.

To clear the configuration by using the command line interface

At the command prompt, type:

clear ns config -force <level>

Example: To forcefully clear the basic configurations on an appliance.

clear ns config -force basic

To clear the configuration by using the configuration utility

Navigate to System > Diagnostics and, in the Maintenance group, click Clear Configuration and select the configuration level to be cleared from the appliance.

Parameter Descriptions (of commands listed in the CLI procedure)

clear ns config

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Viewing the HTTP Band Statistics

You can view HTTP band statistics to obtain useful information such as:

- Average request/response band size.
- The size range to which most requests/responses belong.
- Contribution of HTTP pages, in a certain size range, to the overall HTTP traffic.

To view HTTP request and response size statistics by using the command line interface

At the command prompt, type:

show protocol httpBand –type (REQUEST|RESPONSE)

Example

> show protocol httpBand -type REQUEST

To view HTTP request and response size statistics by using the configuration utility

1. Navigate to System > Settings.
2. In the details pane, under Settings, click HTTP data band statistics.
3. In the HTTP Data Band Statistics dialog box, view the HTTP request and HTTP response size statistics on the Request and Response tabs, respectively.

You can also modify the band range for HTTP request or response size statistics.

To modify the band range by using the command line interface

At the command prompt, type:

set protocol httpBand reqBandSize <value> respBandSize <value>

Example

```
> set protocol httpBand reqBandSize 300 respBandSize 2048
```

To modify the band range by using the configuration utility

1. Navigate to System > Settings.
2. In the details pane, under Settings, click HTTP data band statistics.
3. In the HTTP Data Band Statistics dialog box, select the Request or the Response tab.
4. Click Configure and in the dialog box, specify the band size.
5. Click Close.

Parameter Descriptions (of commands listed in the CLI procedure)

show protocol httpBand

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

set protocol httpBand

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring HTTP Profiles

An HTTP profile is a collection of HTTP parameter settings that can be applied to virtual servers and services. An HTTP profile can be reused on multiple virtual servers or services.

You can use built-in HTTP profiles or configure custom profiles. The following table describes the built-in HTTP profiles.

Table 1. Built-in HTTP Profiles

Built-in profile	Description
nshttp_default_strict_validation	Settings for deployments that require strict validation of HTTP requests and responses.
nshttp_default_profile	The default global HTTP settings for the appliance.

To add an HTTP profile by using the command line interface

At the command prompt, type the following commands to add an HTTP profile and verify the configuration:

- add ns httpProfile <name> [-maxReusePool <positive_integer>] [-dropInvalReqs (ENABLED | DISABLED)] [-markHttp09Inval (ENABLED | DISABLED)] [-markConnReqInval (ENABLED | DISABLED)] ...
- show ns httpProfile <name>

Example

> add ns httpProfile http_profile1 -maxReusePool 30 -dropInvalReqs ENABLED -markHttp09Inval ENABLED -ma

To add an HTTP profile by using the configuration utility

1. Navigate to System > Profiles.
2. In the details pane, click the HTTP Profiles tab, and then click Add.
3. In the Create HTTP Profile dialog box, configure the parameters for the HTTP profile. For a description of a parameter, hover the mouse cursor over the corresponding field.
4. Click Create.

Parameter Descriptions (of commands listed in the CLI procedure)

add ns httpProfile

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns httpProfile

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring WebSocket Connections

WebSocket protocol allows browsers and other clients to create a bi-directional, full duplex TCP connection to the servers. It allows data to be passed back and forth without a request/response model, and so enables live content and creation of real-time games.

The initial handshake is HTTP compliant to satisfy any intermediate devices. During the handshake, the HTTP client connection is upgraded to a WebSocket connection in an HTTP compliant manner. After the upgrade is successful, this connection can be used like a normal TCP connection and does not have to follow any HTTP protocol semantics. When such a connection goes through, the NetScaler appliance tries to interpret any data transfer after the handshake as HTTP, and fails. The WebSocket connections are marked as non-trackable and invalid.

If the HTTP profile that is bound to the virtual server is configured to drop invalid requests, the appliance abruptly closes and resets the connection. However, when the HTTP profile is configured to allow WebSocket connections, the appliance understands the WebSocket handshake. The connection is still marked as non-trackable but it is not marked invalid, and the connection is not dropped.

Configuring WebSocket connections by using the command line interface

At the command prompt, type the following commands to enable websocket connections and verify the configuration:

- set ns httpProfile <name> -webSocket (ENABLED | DISABLED)
- show ns httpProfile <name>

Example: To enable websocket on HTTP profile.

```
> set ns httpProfile http_profile1 -webSocket ENABLED
```

Configuring WebSocket connections by using the configuration utility

1. Navigate to System > Profiles.
2. In the details pane, click the HTTP Profiles tab.
3. Select the HTTP profile for which you want to enable WebSocket connections, and then click Open.
4. In the Configure HTTP Profile dialog box, select the Enable WebSocket connections check box. For a description of the parameter, hover the mouse cursor over the check box.
5. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set ns httpProfile

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns httpProfile

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring TCP Profiles

A Transmission Control Protocol (TCP) profile is a collection of TCP parameter settings that can be applied to virtual servers and services. A TCP profile can be reused on multiple virtual servers or services. You can use built-in TCP profiles or configure custom profiles. The following table describes the built-in TCP profiles.

Table 1. Built-in TCP Profiles

Built-in profile	Description
nstcp_default_tcp_lfp	This profile is useful for long fat pipe networks (WAN) on the client side. Long fat pipe networks have long delay, high bandwidth lines with minimal packet drops.
nstcp_default_tcp_lnp	This profile is useful for long narrow pipe networks (WAN) on the client side. Long narrow pipe networks have considerable packet loss once in a while.
nstcp_default_tcp_lan	This profile is useful for back-end server connections, where these servers reside on the same LAN as the appliance.
nstcp_default_tcp_lfp_thin_stream	This profile is similar to the nstcp_default_tcp_lfp profile; however, the settings are tuned for small size packet flows.
nstcp_default_tcp_lnp_thin_stream	This profile is similar to the nstcp_default_tcp_lnp profile; however, the settings are tuned for small size packet flows.
nstcp_default_tcp_lan_thin_stream	This profile is similar to the nstcp_default_tcp_lan profile; however, the settings are tuned to small size packet flows.
nstcp_default_tcp_interactive_stream	This profile is similar to the nstcp_default_tcp_lan profile; however, it has a reduced delayed ACK timer and ACK on PUSH packet settings.
nstcp_internal_apps	This profile is useful for internal applications on the appliance (for example, GSLB sitesyncing). This contains tuned window scaling and SACK options for the desired applications. This profile should not be bound to applications other than internal applications.

nstcp_default_profile	This profile represents the default global TCP settings on the appliance.

To add a TCP profile by using the command line interface

At the command prompt, type the following commands to add a TCP profile and verify the configuration:

- add ns tcpProfile <name> [-WS (ENABLED | DISABLED)] [-SACK (ENABLED | DISABLED)] [-WSVal <positive_integer>] [-nagle (ENABLED | DISABLED)] [-ackOnPush (ENABLED | DISABLED)] [-maxBurst <positive_integer>] ...
- show ns tcpProfile

Example

> add ns tcpProfile tcp_profile1 -nagle DISABLED -ackOnPush ENABLED -maxBurst 10 -initialCwnd 6 -delayedA

To add a TCP profile by using the configuration utility

1. Navigate to System > Profiles.
2. In the details pane, click on the TCP Profiles tab and then click Add.
3. In the Create TCP Profiles dialog box, configure the parameters for the TCP profile. For a description of a parameter, hover the mouse cursor over the corresponding field.
4. Click Create.

Parameter Descriptions (of commands listed in the CLI procedure)

add ns tcpProfile

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns tcpProfile

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Specifying a TCP Buffer Size

You can set the TCP buffer size, both globally and for individual virtual servers and services, through TCP profiles. The value that you set is the minimum value that is advertised by the appliance, and this buffer size is reserved when a client initiates a connection that is associated with an endpoint-application function, such as compression or SSL. The managed application can request a larger buffer, but if it requests a smaller buffer, the request is not honored, and the specified buffer size is used. If the TCP buffer size is set both at the global level and at the entity level (virtual server or service level), the buffer specified at the entity level takes precedence. If the buffer size that you specify for a service is not the same as the buffer size that you specify for the virtual server to which the service is bound, the appliance uses the buffer size specified for the virtual server for the client-side connection and the buffer size specified for the service for the server-side connection. However, for optimum results, make sure that the values specified for a virtual server and the services bound to it have the same value. The buffer size that you specify is used only when the connection is associated with endpoint-application functions, such as SSL and compression.

You set the TCP buffer size in a custom, entity-level TCP profile by setting the bufferSize parameter for the profile. To apply the buffer size setting specified in a custom, entity-level profile, you bind the profile to the virtual server or service. You set the global TCP buffer size by setting the bufferSize parameter in the global TCP profile `nstcp_default_profile`. You do not bind `nstcp_default_profile` to an entity. The settings in `nstcp_default_profile` are automatically applied globally.

Note: A high TCP buffer value could limit the number of connections that can be made to the appliance. Additionally, the global TCP parameter recvBuffSize, which was set by the use of the set ns tcpParam command, has been deprecated. You can now specify the buffer size only through TCP profiles.

To set the TCP buffer size in an entity-level TCP profile by using the command line interface

At the command prompt, type the following commands to set the TCP buffer size and verify the configuration:

- set ns tcpProfile <name> -bufferSize <positive_integer>
- show ns tcpProfile <name>

Example: To set the buffer size to 12000 bytes.

```
> set ns tcpProfile profile1 -bufferSize 12000
```

Note: You can set the TCP buffer size in the global TCP profile by specifying the profile name as *nstcp_default_profile*.

To set the TCP buffer size in a TCP profile by using the configuration utility

1. Navigate to System > Profiles.
2. In the details pane, click the TCP Profiles tab.
3. Select the profile for which you want to set the TCP buffer size and then click Open.

   Note: Select **nstcp_default_profile** if you want to set the TCP buffer size in the global TCP profile, .
4. In the Configure TCP Profile dialog box, set the TCP buffer size as required. For a description of the parameter, hover the mouse cursor over the text box.
5. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set ns tcpProfile

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns tcpProfile

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Optimizing the TCP Maximum Segment Size for a Virtual Server Configuration

You can specify the Maximum Segment Size (MSS) that the NetScaler appliance advertises to a client when the client initiates a connection to a virtual server on the appliance. You can configure the MSS for the virtual servers configured on the appliance in two ways:

- You can set the MSS for each virtual server to a value of your choice in a TCP profile.
- You can set the `learnVsvrMSS` global TCP parameter to `ENABLED` to enable MSS learning for all the virtual servers configured on the appliance.

If you know the optimal MSS value for a given virtual server, you can specify the MSS in a TCP profile and bind the profile to the virtual server. When a client initiates a connection with the virtual server, the appliance advertises the specified MSS value to the client. However, if the appliance is also configured to learn the optimum MSS value from bound services (as described in the following section), the learned MSS value takes precedence, and the value specified in the TCP profile is used only until the appliance learns the optimum MSS value. The appliance uses the learned MSS value until the appliance is restarted. If the appliance is restarted, the appliance defaults to the MSS value specified in the virtual server's TCP profile until it learns the MSS value again.

Specifying the MSS Value in a TCP Profile

If you know the optimal MSS value for a given virtual server, you can specify the MSS in a TCP profile and bind the profile to the virtual server. When a client initiates a connection with the virtual server, the NetScaler appliance advertises the specified MSS value to the client.

To specify the MSS value in a TCP profile by using the command line interface

At the command prompt, type the following commands to specify the MSS value in a TCP profile and verify the configuration:

- add ns tcpProfile <name> -mss <positive_integer>
- show ns tcpProfile

> add ns tcpProfile tcp_prof1 -mss 1000

To specify the MSS value in a TCP profile by using the configuration utility

1. Navigate to System > Profiles.
2. In the details pane, do one of the following:
   - To create a TCP profile, click **Add**.
   - To specify the MSS in an existing TCP profile, click the name of the profile, and then click **Open**.
3. In the Create TCP Profile or Configure TCP Profile dialog box, specify the name and the MSS value. For a description of a parameter, hover the mouse cursor over the corresponding field.
4. Click **Create** or **OK**.

Parameter Descriptions (of commands listed in the CLI procedure)

add ns tcpProfile

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns tcpProfile

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring the NetScaler to Learn the MSS Value from Bound Services

If you set the global TCP parameter `learnVsvrMSS` to `ENABLED`, the appliance learns the most frequently used MSS value for each configured virtual server. When a client connects to a virtual server, the appliance advertises to the client the MSS value that is optimum for that virtual server. The optimum value is the MSS of the service or subset of bound services that are most frequently selected during load balancing. Consequently, each virtual server configuration uses its own MSS value. This enhancement enables the appliance to optimize the consumption of system resources.

The default value of the `learnVsvrMSS` parameter is `DISABLED`. When enabled, MSS learning is applicable only to virtual servers of type TCP, HTTP, and FTP.

To configure the appliance to learn the MSS for a virtual server by using the command line interface

At the command prompt, type the following commands to configure the appliance to learn the MSS for a virtual server and verify the configuration:

- set ns tcpParam -learnVsvrMSS (ENABLED|DISABLED)
- show ns tcpParam

Example

```
> set ns tcpParam -learnVsvrMSS ENABLED
```

To configure the appliance to learn the MSS for a virtual server by using the configuration utility

1. Navigate to System > Settings.
2. In the details pane, under Settings, click Change TCP parameters.
3. In the Configure TCP Parameters dialog box, select the **Learn MSS** check box.

Parameter Descriptions (of commands listed in the CLI procedure)

set ns tcpParam

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns tcpParam

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Call Home

The Call Home feature monitors your NetScaler appliance for common error conditions. Call Home registers your appliance with the Citrix Technical Support server. If your appliance is successfully registered with the Support server, Call Home automatically uploads system data to that server in the event that one of the conditions occurs. The NetScaler Appliance keeps a full log of all upload events. If you are unable to correct the problem after reviewing the appliance's log, you can contact the Citrix Technical Support team and open a service request. The team can analyze the uploaded system data and recommend possible solutions.

Following is a typical set up for Call Home.

The process flow for using Call Home can be categorized as follows:

- Registration of the NetScaler appliance to the Citrix Technical Support server.
- Uploading of the appliance's data to the Citrix Technical Support server. The support server has the following URL: https://taas.citrix.com/.
- Opening a Technical Support case (Optional).

Registration of the NetScaler appliance. The appliance has to be registered to the Citrix Technical Support server before Call Home can upload the system data to the server when predefined error conditions occur on the appliance. Enabling the Call Home feature on the NetScaler appliance initiates the registration process. The process flow is as follows:

1. The Call Home process sends the unique serial number of the appliance to the Citrix Technical Support server.
2. The server checks its database for an active technical support service contract for the appliance.
3. If there is an active technical support service contract, the support server registers the NetScaler appliance for Call Home and sends a successful-registration response to the appliance. If there is no active technical support service contract, the server sends a registration-failure response to the NetScaler appliance.
4. The NetScaler appliance stores the status of the registration in its memory.

The following table lists the error conditions that Call Home monitors on a NetScaler Appliance:

Table 1. List of error conditions monitored by Call Home

Error Condition	Indicates	Call Home Monitoring Interval	Corresponding SNMP Alarm Name
Compact flash drive errors	The compact flash drive on the appliance that encountered read or write errors.	6 hours	COMPACT-FLASH-ERRORS
Hard disk drive errors	The hard drives on the appliance that encountered read or write errors.	6 hours	HARD-DISK-DRIVE-ERRORS
Power supply unit failure	One of the power supply units on the NetScaler appliance has failed.	7 seconds	POWER-SUPPLY-FAILURE
SSL card failure	One of the SSL cards on the NetScaler appliance has failed.	7 seconds	SSL-CARD-FAILED
Warm restart	The appliance has warm restarted due to a failure of a system process.	After every restart of the NetScaler appliance.	WARM-RESTART-EVENT

Uploading of appliance's data to the Support server. An error condition triggers the following sequence of events:

1. The Call Home process checks the registration status, which is stored on the appliance. If the status indicates successful registration, the process advances to the next step.

2. The Call Home process runs a script that collects all of the system related data in a tar file, which is called the *Call Home* tar file. The data in the tar file includes configurations, logs, and statistics. Call Home locally saves the tar file at /var/tmp/support/callhome.

3. Call Home uploads a copy of the tar file to the Citrix Technical Support server. The Appliance logs the uploading of the tar file in a log file named *callhome.log* located at /var/log. You can also configure the CALLHOME-UPLOAD-EVENT SNMP alarm to generate an SNMP alert whenever Call Home uploads a tar file.

4. If the SNMP alarm related to the error condition is enabled, the SNMP agent on the appliance generates an SNMP trap message and sends it to all of the configured SNMP trap destinations. For more information about configuring SNMP alarms and trap destinations, see "Configuring the NetScaler to Generate SNMPv1 and SNMPv2 Traps."

Note: Call Home creates the Call Home tar file and uploads it to the CITRIX tech support server for only the first occurrence of a particular error condition since the appliance was last restarted. If you want the NetScaler appliance to send you alerts each time a particular error condition occurs, configure the corresponding SNMP alarm for the error condition.

The Call Home tar file has the following name format:

`collector_callhome_<NSIP of the appliance>_<P for Primary or standalone, or S for Secondary>_<date>_<hours, in 24 hr format, according to the local time zone>_<minutes>.tar.gz`. For example, `collector_callhome_10.105.13.100_P_2Feb2012_20_30.tar.gz`.

Opening a Technical Support Service Request . After you review the logs and SNMP trap messages for Call Home upload events, you have the option of contacting the Citrix Technical Support team and opening a service request. For more information about contacting the team and opening a service request, see http://support.citrix.com/article/CTX132307.

The Support team can then analyze the system data in the uploaded Call Home tar files and sends recommendations for possible solutions to the administrator's email address.

Before you begin configuring Call Home, do the following:

- Make sure that the NetScaler appliance is connected to the Internet.
- Make sure that you have an active Citrix Technical Support service contract for the appliance.

Configuring Call Home on the NetScaler appliance consists of the following tasks:

1. **Enable the Call Home feature**. When you enable the Call Home feature, the Call Home process registers the appliance with the Citrix Technical Support server. The registration takes some time to complete. During that time, the appliance displays the status as IN PROGRESS. When the registration is complete, the appliance displays the status as SUCCESSFUL.

   Note: While upgrading the NetScaler appliance from an older release to release 10.1 or later, the NetScaler appliance prompts you to enable the Call Home feature in one of the following cases:

   - The Call Home feature is not supported in the older release.
   - The Call Home feature is disabled in the older release.
2. **(Optional) Specify the administrator's email address**. The Call Home process sends the email address to the Support server, where it is stored for future correspondence regarding Call Home.
3. **Enable the CALLHOME-UPLOAD-EVENT SNMP alarm**. The SNMP agent on the NetScaler appliance generates a trap message and sends to all the configured SNMP trap destinations. The message includes the status of uploading of the Call Home tar file by the Call Home process. For more information about configuring SNMP alarms and trap destinations, see "Configuring the NetScaler to Generate SNMPv1 and SNMPv2 Traps."
4. **(Optional) Enable all of the corresponding SNMP alarms**. Call Home creates and uploads a Call Home tar file for the first occurrence of a monitored error condition since the appliance was last restarted. If you want to be alerted each time the error condition occurs, you can configure the corresponding SNMP alarm for the error condition. Table 1 lists all the corresponding SNMP alarms. For more information about configuring SNMP alarms and trap destinations, see "Configuring the NetScaler to Generate SNMPv1 and SNMPv2 Traps."

To enable Call Home by using the command line interface

At the command prompt, type:

enable ns feature ch

To check the status of the appliance's registration to the Support server by using the command line interface

At the command prompt, type:

show callhome

Example

```
> enable ns feature ch
Done

> show callhome
 Callhome feature: ENABLED
 Registration with Citrix upload server IN PROGRESS

 E-mail address configured:

 Trigger event               State     First occurrence   Latest occurrence
 -------------              -----     ----------------   -----------------
 1) Compact flash errors       Enabled   ..                ..
 2) Hard disk drive errors     Enabled   ..                ..
 3) Power supply unit failure  Enabled   ..                ..
 4) SSL card failure           Enabled   ..                ..
 5) Warm restart               Enabled   N/A               ..
 Done

> show callhome
Callhome feature: ENABLED
Registration with Citrix upload server SUCCESSFUL

E-mail address configured:

Trigger event               State     First occurrence   Latest occurrence
-------------              -----     ----------------   -----------------
1) Compact flash errors       Enabled    ..                ..
2) Hard disk drive errors     Enabled    ..                ..
3) Power supply unit failure  Enabled    ..                ..
4) SSL card failure           Enabled    ..                ..
5) Warm restart               Enabled    N/A               ..
Done
```

To specify the administrator's email address by using the command line interface

At the command prompt, type:

- set callhome -emailAddress <string>
- show callhome

Example

```
> set callhome -emailAddress exampleadmin@example.com
Done

> show callhome
 E-mail address configured: exampleadmin@example.com

 Trigger event               State     First occurrence   Latest occurrence
 -------------               -----     ----------------   -----------------
 1) Compact flash errors      Enabled   ..                  ..
 2) Hard disk drive errors    Enabled   ..                 ..
 3) Power supply unit failure Enabled   ..                  ..
 4) SSL card failure          Enabled   ..                ..
 5) Warm restart              Enabled   N/A                ..
 Done
```

To enable Call Home by using the configuration utility

Navigate to System > Settings, click Configure Advanced Features and select the Call Home option.

To check the status of the appliance's registration with the Support server by using the configuration utility

Navigation to System > Diagnostics and, in the Technical Support Tools group, select Call Home option to view the status of registration.

To specify the administrator's email address by using the configuration utility

Navigation to System > Diagnostics and, in the Technical Support Tools group, select Call Home option to specify the administrator's email address.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show callhome

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

set callhome

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Reporting Tool

Use the Citrix® NetScaler® Reporting tool to view NetScaler performance statistics data as reports. Statistics data are collected by the nscollect utility and are stored in a database. When you want to view certain performance data over a period of time, the Reporting tool pulls out specified data from the database and displays them in charts.

Reports are a collection of charts. The Reporting tool provides built-in reports as well as the option to create custom reports. In a report, you can modify the charts and add new charts. You can also modify the operation of the data collection utility, nscollect, and stop or start its operation.

Using the Reporting Tool

The Reporting tool is a Web-based interface accessed from the Citrix® NetScaler® appliance. Use the Reporting tool to display the performance statistics data as reports containing graphs. In addition to using the built-in reports, you can create custom reports, which you can modify at any time. Reports can have between one and four charts. You can create up to 256 custom reports.

To invoke the Reporting tool

1. Use the Web browser of your choice to connect to the IP address of the NetScaler (for example, http://10.102.29.170/). The Web Logon screen appears.
2. In the User Name text box, type the user name assigned to the NetScaler.
3. In the Password text box, type the password.
4. In the Start in drop-down box, select Reporting.
5. Click Login.

The following screen shots show the report toolbar and the chart toolbar, which are frequently referenced in this documentation.

Figure 1. *Report Toolbar*

Figure 2. *Chart Toolbar*

Working with Reports

You can plot and monitor statistics for the various functional groups configured on the NetScaler over a specified time interval. Reports enable you to troubleshoot or analyze the behavior of your appliance. There are two types of reports: built-in reports and custom reports. Report content for built-in or custom reports can be viewed in a graphical format or a tabular format. The graphical view consists of line, area, and bar charts that can display up to 32 sets of data (counters). The tabular view displays the data in columns and rows. This view is useful for debugging error counters.

The default report that is displayed in the Reporting tool is CPU vs. Memory Usage and HTTP Requests Rate. You can change the default report view by displaying the report you want as your default view, and then clicking Default Report.

Reports can be generated for the last hour, last day, last week, last month, last year, or you can customize the duration.

You can do the following with reports:

- Toggle between a tabular view of data and a graphical view of data.
- Change the graphical display type, such as bar chart or line chart.
- Customize charts in a report.
- Export the chart as an Excel comma-separated value (CSV) file.
- View the charts in detail by zooming in, zooming out, or using a drag-and-drop operation (scrolling).
- Set a report as the default report for viewing whenever you log on.
- Add or remove counters.
- Print reports.
- Refresh reports to view the latest performance data.

Using Built-in Reports

The Reporting tool provides built-in reports for frequently viewed data. Built-in reports are available for the following functional groups: System, Network, SSL, Compression, Integrated Cache, Access Gateway, and Citrix® Application Firewall™. By default, the built-in reports are displayed for the last day. However, you can view the reports for the last hour, last week, last month, or last year.

Note: You cannot save changes to built-in reports, but you can save a modified built-in report as a custom report.

To display a built-in report

1. In the left pane of the Reporting tool, under Built-in Reports, expand a group (for example, SSL).

2. Click a report (for example, SSL > All Backend Ciphers).

Creating and Deleting Reports

You can create your own custom reports and save them with user-defined names for reuse. You can plot different counters for different groups based on your requirements. You can create up to 256 custom reports.

You can either create a new report or save a built-in report as a custom report. By default, a newly created custom report contains one chart named System Overview, which displays the CPU Usage counter plotted for the last day. You can customize the interval and set the data source and time zone from the report toolbar. Within a report, you can use the chart toolbars to add, modify, or delete charts, as described in "Working with Charts."

By default, newly created custom reports contain one chart named System Overview that displays a CPU Usage counter plotted for the last day.

To create a custom report

1. In the Reporting tool, on the report toolbar, click Create, or if you want to create a new custom report based on an existing report, open the existing report, and then click Save As.

2. In Report Name box, type a name for the custom report.

3. Do one of the following:

   - To add the report to an existing folder, in Create in or Save in, click the down arrow to choose an existing folder, and then click OK.

   - To create a new folder to store the report, click the Click to add folder icon, in Folder Name, type the name of the folder, and in Create in, specify where you want the new folder to reside in the hierarchy, and then click OK.

   Note: You can create up to 128 folders.

To delete a custom report

1. In the left pane of the Reporting tool, next to Custom Reports, click the Click to manage custom reports icon.

2. Select the check box that corresponds with the report you want to delete, and then click Delete.

   Note: When you delete a folder, all the contents of that folder are deleted.

Modifying the Time Interval

By default, built-in reports display data for the last day. However, if you want to change the time interval for a built-in report, you can save the report as a custom report. The new interval applies to all charts in the report. The following table describes the time-interval options.

Table 1. Time Intervals

Time interval	Displays
 Last Hour	Statistics data collected for the last hour.
 Last Day	Statistics data collected for the last day (24 hours).
 Last Week	Statistics data collected for the last week (7 days).
 Last Month	Statistics data collected for the last month (31 days).
 Last Year	Statistics data collected for the last year (365 days).
 Custom	Statistics data collected for a time period that you are prompted to specify.

To modify the time interval

1. In the left pane of the Reporting tool, click a report.
2. On the report toolbar, click Duration, and then click a time interval.

Setting the Data Source and Time Zone

You can retrieve data from different data sources to display them in the reports. You can also define the time zone for the reports and apply the currently displayed report's time selection to all the reports, including the built-in reports.

To set the data source and time zone

1. In the Reporting tool, on the report toolbar, click Settings.
2. In the Settings dialog box, in Data Source, select the data source from which you want to retrieve the counter information.
3. Do one or both of the following:
   - If you want the tool to remember the time period for which a chart is plotted, select the Remember time selection for charts check box.
   - If you want the reports to use the time settings of your NetScaler appliance, select the Use Appliance's time zone check box.

Exporting and Importing Custom Reports

You can share reports with other NetScaler administrators by exporting reports. You can also import reports.

To export or import custom reports

1. In the left pane of the Reporting tool, next to Custom Reports, click the Click to manage custom reports icon.
2. Select the check box that corresponds with the report you want to export or import, and then click Export or Import.

   Note: When you export the file, it is exported in a .gz file format.

Working with Charts

Use charts to plot and monitor counters or groups of counters. You can include up to four charts in one report. In each chart, you can plot up to 32 counters. The charts can use different graphical formats (for example, area and bar). You can move the charts up or down within the report, customize the colors and visual display for each counter in a chart, and delete a chart when you do not want to monitor it.

In all report charts, the horizontal axis represents time and the vertical axis represents the value of the counter.

Adding a Chart

When you add a chart to a report, the System Overview chart appears with the CPU Usage counter plotted for the last one day. To plot a different group of statistics or select a different counter, see "Modifying a Chart."

Note: If you add charts to a built-in report, and you want to retain the report, you must save the report as a custom report.

Use the following procedure to add a chart to a report.

To add a chart to a report

1. In the left pane of the Reporting tool, click a report.
2. Under the chart where you want to add the new chart, click the Add icon.

Modifying a Chart

You can modify a chart by changing the functional group for which the statistics are displayed and by selecting different counters.

To modify a chart

1. In the left pane of the Reporting tool, click a report.
2. Under the chart that you want to modify, click Counters.
3. In the dialog box that appears, in the Title box, type a name for the chart.
4. Next to Plot chart for, do one of the following:
   - To plot counters for global counters, such as Integrated Cache and Compression, click System global statistics.
   - To plot entity counters for entity types, such as Load Balancing and GSLB, click System entities statistics.
5. In Select group, click the desired entity.
6. Under Counters, in Available, click the counter name(s) that you want to plot, and then click the > button.
7. If you selected System entities statistics in step 4, on the Entities tab, under Available, click the entity instance name(s) you want to plot, and then click the > button.
8. Click OK.

Viewing a Chart

You can specify the graphical formats of the plotted counters in a chart. Charts can be viewed as line charts, spline charts, step-line charts, scatter charts, area charts, bar charts, stacked area charts, and stacked bar charts. You can also zoom in, zoom out, or scroll inside the plot area of a chart. You can zoom in or out for all data sources for 1 hour, 1 day, 1 week, 1 month, 1 year, and 3 years.

Other options for customizing the view of a chart include customizing the axes of the charts, changing the background and edge color of the plot area, customizing the color and size of the grids, and customizing the display of each data set (counter) in a chart.

Data set numbers, such as Data Set 1, correspond to the order in which the counters in your graph are displayed at the bottom of the chart. For example, if CPU usage and Memory usage are displayed in first and second order at the bottom of the chart, CPU usage is equal to Data Set 1 and Memory usage is equal to Data Set 2.

Whenever you modify a built-in report, you need to save the report as a custom report to retain your changes.

To change the graph type of a chart

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, under the chart you want to view, on the chart toolbar, click Customize.
3. On the Chart tab, under Category, click Plot type, and then click the graph type you want to display for the chart. If you want to display the graph is 3D, select the Use 3D check box.

To refocus a chart with detailed data

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, on the report toolbar, click Zoom In, and do one or both of the following:
   - To refocus the chart to display data for a specific time window, drag and drop the cursor from the start time to the end time. For example, you can view data for a one-hour period on a certain day.
   - To refocus the chart to display data for a data point, simply click once on chart where you want to zoom in and get more detailed information.
3. Once you have the desired range of time for which you want to view detailed data, on the report toolbar, click Tabular View. Tabular view displays the data in numeric form in rows and columns.

To view numeric data for a graph

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, on the report toolbar, click Tabular View. To return to the graphical view, click Graphical View.

   Note: You can also view the numeric data in the graphical view by hovering your cursor over the notches in the gridlines.

To scroll through time in a chart

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, on the report toolbar, click Scroll, and then click inside the chart and drag the cursor in the direction for which you want to see data for a new time period. For example, if you want to view data in the past, click and drag to the left.

To change the background color and text color of a chart

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, under the chart for which you want to customize the axes, click Customize.
3. On the Chart tab, under Category, click one or more of the following:
   - To change the background color, click Background Color, and then select the options for color, transparency, and effects.
   - To change the text color, click Text Color, and then select the options for color, transparency, and effects.

To customize the axes of a chart

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, under the chart for which you want to customize the axes, click Customize.
3. On the Chart tab, under Category, click one or more of the following:
   - To change the scale of the left y-axis, click Left Y-Axis, and then select the scale you want.
   - To change the scale of the right y-axis, click Right Y-Axis, in Data set to plot, select the date set, and then select the scale you want.

     Note: The data set numbers, such as Data Set 1, correspond to the order in which the counters in your graph are displayed at the bottom of the chart. For example, if CPU usage and Memory usage are displayed in first and second order at the bottom of the chart, CPU usage is equal to Data Set 1 and Memory usage is equal to Data Set 2.
   - To plot each data set in its own hidden y-axis, click Multiple Axes, and then click Enable.

To change the background color, edge color, and gridlines for a plot area of a chart

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, under the chart for which you want to customize the plot area, click Customize.
3. On the Plot Area tab, under Category, click one or more of the following:
   - To change the background color and edge color of the chart, click Background Color and Edge Color, and then select the options for color, transparency, and effects.
   - To change the horizontal or vertical grids of the chart, click Horizontal Grids or Vertical Grids, and then select the options for displaying the grids, grid width, grid color, transparency, and effects.

To change the color and graph type of a data set

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, under the chart for which you want to customize the display of the data set (counters), click Customize.
3. On the Data Set tab, in Select Data Set, select the data set (counter) for which you want to customize the graphical display.

   Note: The data set numbers, such as Data Set 1, correspond to the order in which the counters in your graph are displayed at the bottom of the chart. For example, if CPU usage and Memory usage are displayed in first and second order at the bottom of the chart, CPU usage is equal to Data Set 1 and Memory usage is equal to Data Set 2.
4. Under Category, do one of more of the following:
   - To change the background color, click Color, and then select the options for color, transparency, and effects.
   - To change the graph type, click Plot type, and then select the graph type you want to display for the data set. If you want to display the graph as 3D, select the Use 3D check box.

Exporting Chart Data to Excel

For further data analysis, you can export charts to Excel in a comma-separated value (CSV) format.

To export chart data to Excel

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, under the chart with the data you want to export to Excel, click Export.

Deleting a Chart

If you do not want to use a chart, you can remove it from the report. You can permanently remove charts from custom reports only. If you delete a chart from a built-in report and want to retain the changes, you need to save the report as a custom report.

To delete a chart

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, under the chart that you want to delete, click the Delete icon.

Examples

To display the trend report for CPU usage and memory usage for the last week

1. In the left pane of the Reporting tool, under Built-in Reports, expand System.
2. Click the report CPU vs. Memory Usage and HTTP Requests Rate.
3. In the right pane, on the report toolbar, click Duration, and then click Last Week.

To compare the bytes received rate and the bytes transmitted rate between two interfaces for the last week

1. In the right pane, on the report toolbar, click Create.
2. In the Report Name box, type a name for the custom report (for example, `Custom_Interfaces`), and then click OK. The report is created with the default System Overview chart, which displays the CPU Usage counter plotted for the last hour.
3. Under System Overview, on the chart toolbar, click Counters.
4. In the counter selection pane, in Title, type a name for the chart (for example, `Interfaces bytes data`).
5. In Plot chart for, click System entities statistics, and then in Select Group, select Interface.
6. On the Entities tab, click the interface name(s) you want to plot (for example, 1/1 and 1/2), and then click the > button.
7. On the Counters tab, click Bytes received (Rate) and Bytes transmitted (Rate) and then click the > button.
8. Click OK.
9. On the report toolbar, click Duration, and then click Last Week.

Stopping and Starting the Data Collection Utility

The data collection utility, nscollect, runs automatically when you start the NetScaler ADC. This utility retrieves the application performance data and stores it in the form of data sources on the ADC. You can create up to 32 data sources. The default data source is /var/log/db/default.

The data collection utility creates databases for global counters and entity-specific counters, and uses this data to generate reports. Global-counter databases are created at /var/log/db/<DataSourceName> . The entity-specific databases are created based on the entities configured on the NetScaler, and a separate folder is created for each entity type in /var/log/db/<DataSourceName/EntityNameDB>.

Nscollect retrieves data once every 5 minutes. It retains data in 5-minute granularity for one day, hourly for the last 30 days, and daily for three years.

You might have to stop and restart the data collection utility if data is not updated accurately or the reports display corrupted data.

To stop nscollect

At the command prompt, type:

/netscaler/nscollect stop

To start nscollect on the local system

At the command prompt, type:

/netscaler/nscollect start

AppFlow

The Citrix NetScaler appliance is a central point of control for all application traffic in the data center. It collects flow and user-session level information valuable for application performance monitoring, analytics, and business intelligence applications. It also collects web page performance data and database information. AppFlow transmits the information by using the Internet Protocol Flow Information eXport (IPFIX) format, which is an open Internet Engineering Task Force (IETF) standard defined in RFC 5101. IPFIX (the standardized version of Cisco's NetFlow) is widely used to monitor network flow information. AppFlow defines new Information Elements to represent application-level information, web page performance data, and database information.

Using UDP as the transport protocol, AppFlow transmits the collected data, called *flow records*, to one or more IPv4 collectors. The collectors aggregate the flow records and generate real-time or historical reports.

AppFlow provides visibility at the transaction level for HTTP, SSL, TCP, and SSL_TCP flows. You can sample and filter the flow types that you want to monitor.

AppFlow use actions and policies to send records for a selected flow to specific set of collectors. An AppFlow action specifies which set of collectors will receive the AppFlow records. Policies, which are based on Advanced expressions can be configured to select flows for which flow records will be sent to the collectors specified by the associated AppFlow action.

To limit the types of flows, you can enable AppFlow for a virtual server. AppFlow can also provide statistics for the virtual server.

You can also enable AppFlow for a specific service, representing an application server, and monitor the traffic to that application server.

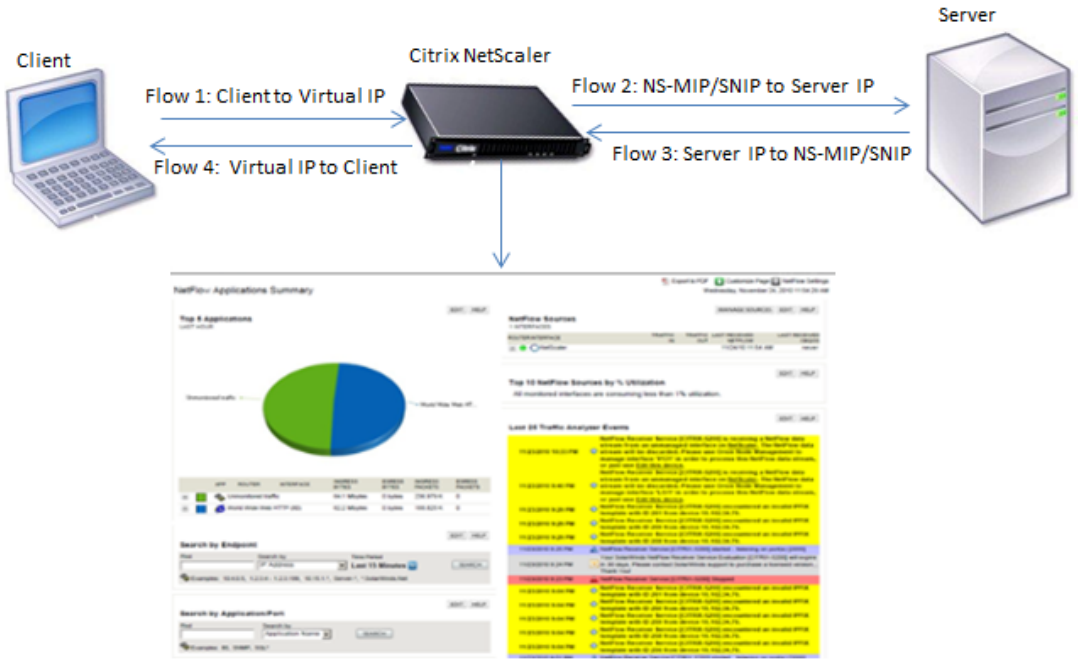
Note: This feature is supported only on NetScaler nCore builds.

How AppFlow Works

In the most common deployment scenario, inbound traffic flows to a Virtual IP address (VIP) on the NetScaler appliance and is load balanced to a server. Outbound traffic flows from the server to a mapped or subnet IP address on the NetScaler and from the VIP to the client. A flow is a unidirectional collection of IP packets identified by the following five tuples: sourceIP, sourcePort, destIP, destPort, and protocol.

The following figure describes how the AppFlow feature works.

Figure 1. NetScaler Flow Sequence



As shown in the figure, the network flow identifiers for each leg of a transaction depend on the direction of the traffic.

The different flows that form a flow record are:

Flow1: <Client-IP, Client-Port, VIP-IP, VIP-port, Protocol>

Flow2: <NS-MIP/SNIP, NS-port, Server-IP, Server-Port, Protocol>

Flow3: <Server-IP, Server-Port, NS-MIP/SNIP, NS-Port, Protocol>

Flow4: <VIP-IP, VIP-port, Client-IP, Client-Port, Protocol>

To help the collector link all four flows in a transaction, AppFlow adds a custom transactionID element to each flow. For application-level content switching, such as HTTP, it is possible for a single client TCP connection to be load balanced to different backend TCP connections for each request. AppFlow provides a set of records for each transaction.

Flow Records

AppFlow records contain standard NetFlow or IPFIX information, such as time stamps for the beginning and end of a flow, packet count, and byte count. AppFlow records also contain application-level information (such as HTTP URLs, HTTP request methods and response status codes, server response time, and latency), web page performance data (such as page load time, page render time, and time spent on the page), and database information (such as database protocol, database response status and database response size). IPFIX flow records are based on templates that need to be sent before sending flow records.

Templates

AppFlow defines a set of templates, one for each type of flow. Each template contains a set of standard Information Elements (IEs) and Enterprise-specific Information Elements (EIEs). IPFIX templates define the order and sizes of the Information Elements (IE) in the flow record. The templates are sent to the collectors at regular intervals, as described in RFC 5101.

A template can include the following EIEs:

transactionID

An unsigned 32-bit number identifying an application-level transaction. For HTTP, this corresponds to a request and response pair. All flow records that correspond to this request and response pair have the same transaction ID. In the most common case, there are four uniflow records that correspond to this transaction. If the NetScaler generates the response by itself (served from the integrated cache or by a security policy), there may be only two flow records for this transaction.

connectionID

An unsigned 32-bit number identifying a layer-4 connection (TCP or UDP). The NetScaler flows are usually bidirectional, with two separate flow records for each direction of the flow. This information element can be used to link the two flows.

For the NetScaler, connectionID is an identifier for the connection data structure to track the progress of a connection. In an HTTP transaction, for instance, a given connectionID may have multiple transactionID elements corresponding to multiple requests that were made on that connection.

tcpRTT

The round trip time, in milliseconds, as measured on the TCP connection. This can be used as a metric to determine the client or server latency on the network.

httpRequestMethod

An 8-bit number indicating the HTTP method used in the transaction. An options template with the number-to-method mapping is sent along with the template.

httpRequestSize

An unsigned 32-bit number indicating the request payload size.

httpRequestURL

The HTTP URL requested by the client.

httpUserAgent

The source of incoming requests to the Web server.

httpResponseStatus

An unsigned 32-bit number indicating the response status code.

httpResponseSize

An unsigned 32-bit number indicating the response size.

httpResponseTimeToFirstByte

An unsigned 32-bit number indicating the time taken to receive the first byte of the response.

httpResponseTimeToLastByte

An unsigned 32-bit number indicating the time taken to receive the last byte of the response.

flowFlags

An unsigned 64-bit flag used to indicate different flow conditions.

EIEs for web page performance data

clientInteractionStartTime

Time at which the browser receives the first byte of the response to load any objects of the page such as images, scripts, and stylesheets.

clientInteractionEndTime

Time at which the browser received the last byte of response to load all the objects of the page such as images, scripts, and stylesheets.

clientRenderStartTime

Time at which the browser starts to render the page.

clientRenderEndTime

Time at which browser finished rendering the entire page, including the embedded objects.

EIEs for database information

dbProtocolName

An unsigned 8-bit number indicating the database protocol. Valid values are 1 for MS SQL and 2 for MySQL.

dbReqType

An unsigned 8-bit number indicating the database request method used in the transaction. For MS SQL, valid values are 1 is for QUERY, 2 is for TRANSACTION, and 3 is for RPC. For valid values for MySQL, see the MySQL documentation.

dbReqString

Indicates the database request string without the header.

dbRespStatus

An unsigned 64-bit number indicating the status of the database response received from the web server.

dbRespLength

An unsigned 64-bit number indicating the response size.

dbRespStatString

The response status string received from the web server.

Configuring the AppFlow Feature

You configure AppFlow in the same manner as most other policy-based features. First, you enable the AppFlow feature. Then you specify the collectors to which the flow records are sent. After that, you define actions, which are sets of configured collectors. Then you configure one or more policies and associate an action to each policy. The policy tells the NetScaler appliance to select requests the flow records of which are sent to the associated action. Finally, you bind each policy either globally or to specific vservers to put it into effect.

You can further set AppFlow parameters to specify the template refresh interval and to enable the exporting of httpURL, httpCookie, and httpReferer information. On each collector, you must specify the NetScaler IP address as the address of the exporter.

Note: For information about configuring the NetScaler as an exporter on the collector, see the documentation for the specific collector.

The configuration utility provides tools that help users define the policies and actions that determine exactly how the NetScaler appliance export records for a particular flow to a set of collectors(action.) The command line interface provides a corresponding set of CLI-based commands for experienced users who prefer a command line.

Enabling AppFlow

To be able to use the AppFlow feature, you must first enable it.

Note: AppFlow can be enabled only on nCore NetScaler appliances.

To enable the AppFlow feature by using the command line interface

At the command prompt, type one of the following commands:

enable ns feature `AppFlow`

To enable the AppFlow feature by using the configuration utility

Navigate to System > Settings, click Configure Advanced Features and select the AppFlow option.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Specifying a Collector

A collector receives flow records generated by the NetScaler appliance. To be able to send flow records, you must specify at least one collector. You can specify up to four. However, you cannot export the same data to multiple collectors. You can remove unused collectors. By default, the collector listens to IPFIX messages on UDP port 4739. You can change the default port, when configuring the collector. Similarly, by default, NSIP is used as the source IP for appflow traffic. You can change this default source IP to a SNIP or MIP address when configuring a collector.

To specify a collector by using the command line interface

At the command prompt, type the following commands to add a collector and verify the configuration:

- add appflow collector <*name*> -IPAddress <*ipaddress*> -port <*port_number*> -netprofile <*netprofile_name*>
- show appflow collector <*name*>

Example

> add appflow collector col1 -IPaddress 10.102.29.251 -port 8000 -netprofile n2

To specify a collector by using the configuration utility

In the navigation pane, expand AppFlow, and then click Collectors, and create the AppFlow collector.

Parameter Descriptions (of commands listed in the CLI procedure)

add appflow collector

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show appflow collector

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring an AppFlow Action

An AppFlow action is a set collectors, to which the flow records are sent if the associated AppFlow policy matches.

To configure an AppFlow action by using the command line interface

At the command prompt, type the following commands to configure an Appflow action and verify the configuration:

- add appflow action <name> --collectors <string> ... [-comment <string>]
- show appflow action

Example

> add appflow action apfl-act-collector-1-and-3 -collectors collector-1 collecter-3

To configure an AppFlow action by using the configuration utility

1. In the navigation pane, expand AppFlow, and then click Actions.
2. In the details pane, do one of the following:
   - To create a new action, click Add.
   - To modify an existing action, select the action, and then click Open.
3. In the Add AppFlow Action or Configure AppFlow Action dialog box, type a name for the new action or the name of an existing action, respectively.
4. Do one of the following to associate collectors with the action:
   - If the collectors that you want are listed, click the corresponding check boxes.
   - If you want to specify all the collectors, click Activate All.
   - If you want to specify a new collector, click Add.
5. Click Create or OK, depending on whether you are creating a new action or modifying an existing action.
6. Click Close. A message appears in the status bar, stating that the configuration has been successfully implemented.

Parameter Descriptions (of commands listed in the CLI procedure)

add appflow action

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show appflow action

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring an AppFlow Policy

After you configure an AppFlow action, you must next configure an AppFlow policy. An AppFlow policy is based on a rule, which consists of one or more expressions.

Note: For creating and managing AppFlow policies, the configuration utility provides assistance that is not available at the command line interface.

To configure an AppFlow policy by using the command line interface

At the command prompt, type the following command to add an AppFlow policy and verify the configuration:

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

Example

```
> add appflow policy apfl-pol-tcp-dsprt client.TCP.DSTPORT.EQ(22) apfl-act-collector-1-and-3
```

To configure an AppFlow policy by using the configuration utility

In the navigation pane, expand AppFlow, and then click Policies, and create the AppFlow policy.

To add an expression by using the Add Expression dialog box

1. In the Add Expression dialog box, in the first list box choose the first term for your expression.

   HTTP

   The HTTP protocol. Choose this if you want to examine some aspect of the request that pertains to the HTTP protocol.

   SYS

   The protected Web site(s). Choose this if you want to examine some aspect of the request that pertains to the recipient of the request.

   CLIENT

   The computer that sent the request. Choose this if you want to examine some aspect of the sender of the request.

   When you make your choice, the rightmost list box lists appropriate terms for the next part of your expression.

2. In the second list box, choose the second term for your expression. The choices depend upon which choice you made in the previous step, and are appropriate to the context. After you make your second choice, the Help window below the Construct Expression window (which was blank) displays help describing the purpose and use of the term you just chose.

3. Continue choosing terms from the list boxes that appear to the right of the previous list box, or typing strings or numbers in the text boxes that appear to prompt you to enter a value, until your expression is finished.

Parameter Descriptions (of commands listed in the CLI procedure)

add appflow policy

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show appflow policy

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Binding an AppFlow Policy

To put a policy into effect, you must bind it either globally, so that it applies to all traffic that flows through the NetScaler, or to a specific virtual server, so that the policy applies only to the traffic related to that virtual server.

When you bind a policy, you assign it a priority. The priority determines the order in which the policies you define are evaluated. You can set the priority to any positive integer.

In the NetScaler operating system, policy priorities work in reverse order—the higher the number, the lower the priority. For example, if you have three policies with priorities of 10, 100, and 1000, the policy assigned a priority of 10 is performed first, then the policy assigned a priority of 100, and finally the policy assigned an order of 1000.

You can leave yourself plenty of room to add other policies in any order, and still set them to evaluate in the order you want, by setting priorities with intervals of 50 or 100 between each policy when you globally bind it. You can then add additional policies at any time without having to change the priority of an existing policy.

To globally bind an AppFlow policy by using the command line interface

At the command prompt, type the following command to globally bind an AppFlow policy and verify the configuration:

- bind appflow global <policyName> <priority> [<gotoPriorityExpression [-type <type>] [-invoke (<labelType> <labelName>)]
- show appflow global

Example

bind appflow global af_policy_lb1_10.102.71.190 1 NEXT -type REQ_OVERRIDE -invoke vserver google

To bind an AppFlow policy to a specific virtual server by using the command line interface

At the command prompt, type the following command to bind an appflow policy to a specific virtual server and verify the configuration:

bind lb vserver <name> -policyname <policy_name> -priority <priority>

Example

bind lb vserver google -policyname af_policy_google_10.102.19.179 -priority 251

To globally bind an AppFlow policy by using the configuration utility

In the navigation pane, expand AppFlow, click AppFlow policy Manager and select the relevant Bind Point (Default Global) and Connection Type, and then bind the AppFlow policy.

To bind an AppFlow policy to a specific virtual server by using the configuration utility

In the navigation pane, expand Load Balancing, and then click Virtual Servers, select the virtual server, and click Policies, and bind the AppFlow policy.

Parameter Descriptions (of commands listed in the CLI procedure)

bind appflow global

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show appflow global

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Enabling AppFlow for Virtual Servers

If you want to monitor only the traffic through certain virtual servers, enable AppFlow specifically for those virtual servers. You can enable AppFlow for load balancing, content switching, cache redirection, SSL VPN, GSLB, and authentication virtual servers.

To enable AppFlow for a virtual server by using the command line interface

At the command prompt, type:

set cs vserver <name> <protocol> <IPAddress> <port> -appflowLog ENABLED

Example

> set cs vserver Vserver-CS-1 HTTP 10.102.29.161 80 -appflowLog ENABLED

To enable AppFlow for a virtual server by using the configuration utility

In the navigation pane, expand the feature node for which you want to enable AppFlow, and then click Virtual Servers, and enable AppFlow Logging option. For example, to enable AppFlow for a content switching virtual server, expand Content Switching and then click Virtual Servers.

Parameter Descriptions (of commands listed in the CLI procedure)

set cs vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Enabling AppFlow for a Service

You can enable AppFlow for services that are to be bound to the load balancing virtual servers.

To enable AppFlow for a service by using the command line interface

At the command prompt, type:

set service <name> -appflowLog ENABLED

Example

set service ser -appflowLog ENABLED

To enable AppFlow for a service by using the configuration utility

In the navigation pane, expand Load Balancing, and then click Services, select the service, and enable AppFlow Logging option.

Parameter Descriptions (of commands listed in the CLI procedure)

set service

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Setting the AppFlow Parameters

You can set AppFlow parameters to customize the exporting of data to the collectors.

To set the AppFlow Parameters by using the command line interface

At the command prompt, type the following commands to set the AppFlow parameters and verify the settings:

- set appflow param [-templateRefresh <secs>] [-appnameRefresh <secs>] [-flowRecordInterval <secs>] [-udpPmtu <positive_integer>] [-httpUrl (**ENABLED** | **DISABLED**)] [-httpCookie (**ENABLED** | **DISABLED**)] [-httpReferer (**ENABLED** | **DISABLED**)] [-httpMethod (**ENABLED** | **DISABLED**)] [-httpHost (**ENABLED** | **DISABLED**)] [-httpUserAgent (**ENABLED** | **DISABLED**)] [-httpXForwardedFor (**ENABLED** | **DISABLED**)][-clientTrafficOnly (**YES** | **NO**)]
- show appflow Param

Example

> set appflow Param -templateRefresh 240 -udpPmtu 128 -httpUrl enabled

To set the AppFlow parameters by using the configuration utility

In the navigation pane, click AppFlow, select Change AppFlow Settings, and specify relevant AppFlow parameters.

Parameter Descriptions (of commands listed in the CLI procedure)

set appflow param

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show appflow Param

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Example: Configuring AppFlow for DataStream

The following example illustrates the procedure for configuring AppFlow for DataStream using the command line interface.

```
> enable feature appflow
> add db user sa password freebsd
> add lbvserver lb0 MSSQL 10.102.147.97 1433 -appflowLog ENABLED
> add service sv0 10.103.24.132 MSSQL 1433 -appflowLog ENABLED
> bind lbvserver lb0 sv0
> add appflow collector col0 -IPAddress 10.102.147.90
> add appflow action act0 -collectors col0
> add appflow policy pol0 "mssql.req.query.text.contains(\"select\")" act0
> bind lbvserver lb0 -policyName pol0 -priority 10
```

When the Netscaler appliance receives a database request, the appliance evaluates the request against a configured policy. If a match is found, the details are sent to the AppFlow collector configured in the policy.

Exporting Performance Data of Web Pages to AppFlow Collector

The EdgeSight Monitoring application provides web page monitoring data with which you can monitor the performance of various Web applications served in a Netscaler environment. You can now export this data to AppFlow collectors to get an in-depth analysis of the web page applications. AppFlow, which is based on IPFIX standard, provides more specific information about web application performance than does EdgeSight monitoring alone.

You can configure both load balancing and content switching virtual servers to export EdgeSight Monitoring data to AppFlow collectors. Before configuring a virtual server for AppFlow export, associate an Appflow action with the EdgeSight Monitoring responder policy.

The following web page performance data is exported to AppFlow:

- **Page Load Time**. Elapsed time, in milliseconds, from when the browser starts to receive the first byte of a response until the user starts to interact with the page. At this stage, all the page content might not be loaded.
- **Page Render Time**.Elapsed time, in milliseconds, from when the browser receives the first byte of response until either all page content has been rendered or the page load action has timed out.
- **Time Spent on the Page**. Time spent by users on a page. Represents the period of time from one page request to the next one.

AppFlow transmits the performance data by using the Internet Protocol Flow Information eXport (IPFIX) format, which is an open Internet Engineering Task Force (IETF) standard defined in RFC 5101. The AppFlow templates use the following enterprise-specific Information Elements (EIEs) to export the information:

- **Client Load End Time**. Time at which the browser received the last byte of a response to load all the objects of the page such as images, scripts, and stylesheets.
- **Client Load Start Time.**Time at which the browser receives the first byte of the response to load any objects of the page such as images, scripts, and stylesheets.
- **Client Render End Time**. Time at which browser finished rendering the entire page, including the embedded objects.
- **Client Render Start Time**. Time at which the browser started rendering the page.

Prerequisites for Exporting Performance Data of Web Pages to AppFlow Collectors

Before associating the AppFlow action with the AppFlow policy, verify that the following prerequisites have been met:

- The AppFlow feature has been enabled and configured. For instructions, see "Configuring the AppFlow feature".
- The Responder feature has been enabled. For instructions, see "Enabling a Responder Feature".
- The EdgeSight Monitoring feature has been enabled. For instructions, see "Enabling an Application for EdgeSight Monitoring."
- EdgeSight Monitoring has been enabled on the load balancing or content switching virtual servers bound to the services of applications for which you want to collect the performance data. For instructions, see "Enabling an Application for EdgeSight Monitoring."

Associating an AppFlow Action with the EdgeSight Monitoring Responder Policy

To export the web page performance data to the AppFlow collector, you must associate an AppFlow action with the EdgeSight Monitoring responder policy. An AppFlow action specifies which set of collectors receive the traffic.

To associate an AppFlow action with the EdgeSight Monitoring Responder policy by using the command line interface

At the command prompt, type:

set responder policy <name> -appflowAction <action_Name>

Example

set responder policy pol -appflowAction actn

To associate an AppFlow action with the EdgeSight Monitoring Responder policy by using the configuration utility

1. In the navigation page, expand **Responder**, and then click **Policies**.
2. In the details pane, select an EdgeSight Monitoring responder policy, and then click **Open**.
3. In the **Configure Responder Policy** dialog box, in the **AppFlow Action** drop-down list, select the AppFlow action associated with the collectors to which you want to send the web-page performance data.
4. Click **OK**.

Configuring a Virtual Server to Export EdgeSight Statistics to Appflow Collectors

To export EdgeSight statistics information from a virtual server to the AppFlow collector, you must associate an AppFlow action with the virtual server.

To associate an AppFlow action with a Load Balancing or Content Switching virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing or Content Switching, and then click Virtual Servers.
2. In the details pane, select a virtual server, or multiple virtual servers, and then click Enable EdgeSight Monitoring.
3. In the Enable EdgeSight Monitoring dialog box, select the Export EdgeSight statistics to Appflow check box.
4. From the Appflow Action drop-down list, select the AppFlow action. The AppFlow action defines the list of AppFlow collectors to which it exports EdgeSight Monitoring statistics. If you have selected multiple load balancing virtual servers, the same AppFlow Action will be associated with the responder policies bound to them. You can later change the AppFlow Action configured for each of the selected Load Balancing virtual server individually, if required.
5. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set responder policy

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

AutoScale: Automatic Scaling in the Citrix CloudPlatform Environment

Note: The AutoScale feature is supported only on NetScaler 10.e.

Efficient hosting of applications in a cloud requires continuous optimization of application availability. To meet increasing demand, you have to scale network resources upward. When demand subsides, you need to scale down to avoid the unnecessary cost of idle resources. To minimize the cost of running the application by deploying only as many instances as are necessary during any given period of time, you have to constantly monitor traffic. However, monitoring traffic manually is not a feasible option. For the application environment to be able to scale up or down rapidly, you need to automate the processes of monitoring traffic and of scaling resources up and down whenever necessary.

If your organization uses Citrix CloudPlatform to deploy and manage the cloud environment, a Citrix NetScaler appliance can automatically scale users' applications as needed. The CloudPlatform elastic load balancing feature includes a feature called *AutoScale*. A CloudPlatform user can use the AutoScale feature to specify thresholds for various conditions for automatically scaling the application fleet upward and downward. The scale-up and scale-down conditions can vary from simple use cases, such as a server's CPU usage, to complex use cases, such as a combination of a server's CPU usage and responsiveness. CloudPlatform, in turn, configures the NetScaler appliance to load balance traffic to the application virtual machines (VMs), monitor application thresholds and performance, and trigger scale-up and scale-down actions to add or remove VMs to or from the application fleet.

The CloudPlatform user performs all AutoScale configuration tasks by using the CloudPlatform user interface or APIs. The CloudPlatform user:

1. Creates a load balancing rule, with the necessary load balancing algorithm and stickiness.

2. Configures AutoScale parameters by specifying the application instance template, the minimum number of instances to maintain, the maximum number of instances permitted, scale-up and scale-down policies, and other information necessary for the functioning of the feature.

3. Submits the configuration.

For information about configuring a load balancing rule and AutoScale, see *Citrix CloudPlatform 3.0.5 (powered by Apache CloudStack) Administrator's Guide*, at http://support.citrix.com/article/CTX134823.

When the CloudPlatform user completes the AutoScale configuration, CloudPlatform uses the NetScaler NITRO API to push all the necessary configuration commands to the NetScaler appliance. As the NetScaler administrator, you do not have to perform any tasks for configuring AutoScale on the NetScaler appliance. However, you might have to be aware of certain prerequisites, and you might have to troubleshoot the configuration if issues arise in the AutoScale configuration. To troubleshoot the configuration, you have to be aware of how CloudPlatform works and what configuration CloudPlatform pushes to the NetScaler

appliance. You also need a working knowledge of how to troubleshoot issues on a NetScaler appliance.

How AutoScale Works

When the CloudPlatform user completes the AutoScale configuration, CloudPlatform uses the NetScaler NITRO API to create an AutoScale-related configuration on the NetScaler appliance. For information about the configuration commands that CloudPlatform uses to configure the NetScaler appliance, see "NetScaler Configuration Details."

The following diagram shows the sequence of operations, beginning with CloudPlatform pushing the AutoScale configuration to the NetScaler appliance. The events are numbered in the order in which they occur, and are described below.

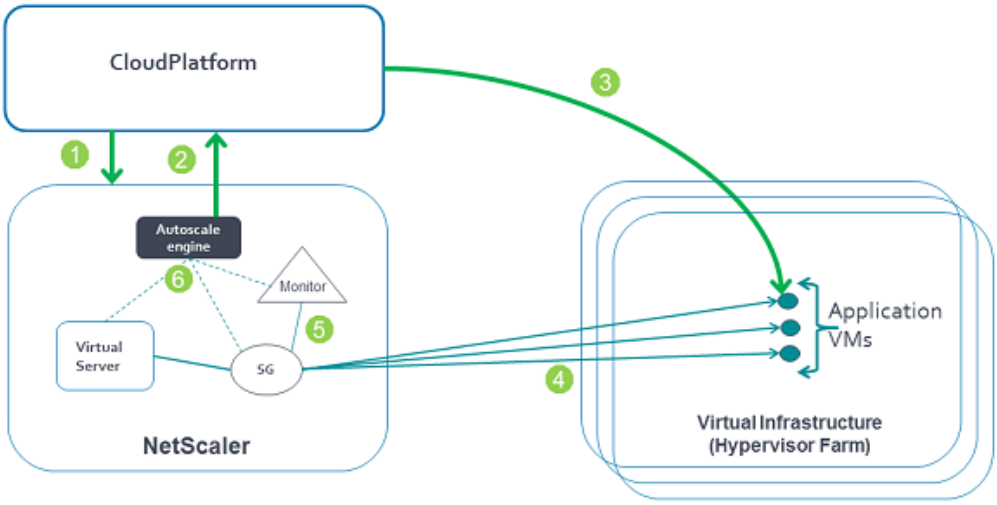


Figure 1. AutoScale Architecture

When the CloudPlatform user submits the AutoScale configuration, the following events occur:

1. CloudPlatform uses the NetScaler NITRO API to push the AutoScale configuration to the NetScaler appliance, creating AutoScale-related entities on the appliance. The entities include a load balancing virtual server, a service group, and monitors.

2. The AutoScale engine on the NetScaler appliance sends API requests to CloudPlatform to initially deploy the minimum number of virtual machines required.

3. CloudPlatform provisions the minimum number of instances (VMs) on the hypervisors (virtualization hosts) that it manages.

4. The NetScaler appliance discovers the IP addresses assigned by CloudPlatform to the newly created VMs and binds them, as services, to the service group representing them. The NetScaler appliance can then load balance traffic to the VMs.

5. NetScaler monitors bound to the service group start monitoring the load by collecting SNMP metrics from the instances.

6. The AutoScale engine on the NetScaler appliance monitors the metrics collected from the VMs and triggers scale-up and scale-down events whenever the metrics breach the configured threshold for the specified period. As part of the scale-up trigger, the NetScaler AutoScale engine sends an API request to CloudPlatform to deploy a new VM. After the virtual machine is deployed, the AutoScale engine binds the service representing the VM (IP address and port) to the service group and, after the configured quiet time, starts forwarding load balanced traffic to the new virtual machine. Likewise, as part of the scale-down trigger, the NetScaler AutoScale engine selects a VM, stops forwarding new requests to that instance, and waits for the configured quiet time (to allow for the processing of current requests to complete) before it sends an API request to CloudPlatform to destroy the chosen instance.

In this way, the NetScaler appliance monitors the application and triggers scale-up and scale-down events on the basis of application load and/or performance.

Supported Environment

AutoScale is supported in the following environment:

- Citrix CloudPlatform 3.0.5.
- Citrix NetScaler MPX/SDX/virtual appliance running Citrix NetScaler release 10.e and later.
- SNMP v1/v2.

Prerequisites

Before you set up AutoScale, do the following:

- Make sure that CloudPlatform is reachable from the NetScaler appliance. You can do so by logging on to the NetScaler appliance and sending ping requests to the CloudPlatform server's IP address.
- Make sure that the network service offering used in CloudPlatform includes the NetScaler appliance as an external load balancing device.
- Use a CloudPlatform and NetScaler release that supports AutoScale. For information about NetScaler releases that support AutoScale, see "Supported Environment."

If you have to troubleshoot an AutoScale setup, you also have to know the prerequisites for setting up AutoScale in CloudPlatform. See the "Prerequisites" section of "Configuring AutoScale" in the *Citrix CloudPlatform 3.0.5 (powered by Apache CloudStack) Administrator's Guide*, at http://support.citrix.com/article/CTX134823.

NetScaler Configuration Details

The following table describes the AutoScale configuration commands that are used by Citrix CloudPlatform to configure a NetScaler appliance.

Table 1. NetScaler Configuration for AutoScale

ROBIN -cltTimeout 9000 -minAutoscaleMembers 2 -maxAutoscaleMembers 5
useproxyport YES -cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB NO -CMP NO -autoScale POLICY -memberP
a35a6b6b76614006b97476e841b80f79 476e841b80f79 22

```
 Cloud-MTbl-192.0.2.116-22
```

```
080/client/api" -apiKey t0fEWPtk_ncQYbofjAm1jjlgGTR7UNZrkZ3sdEpLREBNzBPLSNpNz8qNSbc439xNtYnEYdWn_MsUC_
```

```
ale-Profile-192.0.2.116-22 -parameters
4c89-a88d-04d8b17fe8e9&templateid=1a4a5084-208c-47a8-9c16-d582550cf759&displayname=AutoScale-LB-lb&net
```

```
toScale-Profile-192.0.2.116-22 -parameters "command=destroyVirtualMachine&lbruleid=f96b7f3b-19ec-4123-
```

```
2.0.2.116-22\").ACTIVESERVICES.LT(SYS.VSERVER(\"Cloud-VirtualServer-192.0.2.116-22\").MINAUTOSCALEMEMB
```

```
2.0.2.116-22\").ACTIVESERVICES.GT(SYS.VSERVER(\"Cloud-VirtualServer-192.0.2.116-22\").MAXAUTOSCALEMEMB
```

```
.0.2.116-22\").ACTIVESERVICES.LT(SYS.VSERVER(\"Cloud-VirtualServer-192.0.2.116-22\").MAXAUTOSCALEMEMBE
toScale-ScaleUpAction-192.0.2.116-22
```

```
.0.2.116-22\").ACTIVESERVICES.GT(SYS.VSERVER(\"Cloud-VirtualServer-192.0.2.116-22\").MINAUTOSCALEMEMBE
toScale-ScaleDownAction-192.0.2.116-22
```

```
priority 1 -gotoPriorityExpression END -sampleSize 1 -threshold 1

priority 2 -gotoPriorityExpression END -sampleSize 1 -threshold 1

riority 3 -gotoPriorityExpression END -sampleSize 2 -threshold 2

riority 4 -gotoPriorityExpression END -sampleSize 2 -threshold 2
```

Troubleshooting

Before you attempt to resolve an AutoScale issue, make sure that the prerequisites have been adhered to, on both the CloudPlatform server and the NetScaler appliance, as described in "Prerequisites." If that does not resolve the issue, your problem could be one of the following.

The AutoScale configuration was successfully configured in CloudPlatform. Yet, the minimum number of VMs has not been created.

- Recommend that the CloudPlatform user deploy one VM manually in the network before configuring AutoScale. Ask the user to remove the AutoScale configuration from the NetScaler appliance or the load balancer from the network, manually deploy one VM (preferably using the template created for the AutoScale configuration), and then create the AutoScale configuration.
- Verify that the CloudPlatform user has configured the VM template in such a way that the VMs that are created from the template can accept traffic without manual intervention. If a provisioned VM cannot accept traffic automatically, the metric remains above the threshold, and the AutoScale configuration continues to provision additional VMs, as designed. To remedy the issue, disable AutoScale from CloudPlatform, fix the template, and then enable AutoScale.
- Verify that the CloudPlatform user has not exceeded the limit for the number of VMs imposed by the user's account.
- Verify that the CloudPlatform server is up and is reachable from the NetScaler appliance.
- Verify that the CloudPlatform log file, management-server.log, has reported the successful creation of the AutoScale configuration in CloudPlatform.
- Verify that the scale-up policy that is responsible for initial scale up (the policy name is prefixed with Cloud-AutoScale-Policy-Min) is receiving hits.

The AutoScale configuration is rapidly spawning a large number of VMs

- Verify that the CloudPlatform user has configured the VM template in such a way that the VMs that are created from the template can accept traffic without manual intervention. If a provisioned VM cannot accept traffic automatically, the metric remains above the threshold, and the AutoScale configuration continues to provision additional VMs, as designed. To remedy the issue, disable AutoScale from CloudPlatform, fix the template, and then enable AutoScale.
- Verify that the quiet time that the CloudPlatform user has configured in the AutoScale configuration is sufficient to ensure even traffic distribution to all the VMs, including the new VM. If the quiet time is too low, and traffic distribution has not stabilized, the metrics might remain above the threshold, and additional VMs might be spawned.

When I ran the top command on my VM, I noticed that the CPU usage on my VM had breached the threshold that was configured for the scale-up action in AutoScale. Yet, the application is not scaling up.

- Verify that the CloudPlatform user has installed an SNMP agent in the VM template, and that the SNMP agent is up and running on every VM.
- Verify that the CloudPlatform user has not exceeded the limit for the number of VMs imposed by the user's account.
- Verify that the CloudPlatform user has correctly configured the SNMP parameters to collect metrics from the VM (for example, the community string and the port).
- Verify that the scale-up or scale-down policy is receiving hits.
- Verify that the CloudPlatform server is up, and that the CloudPlatform server is reachable from the NetScaler appliance.

One or more additional VMs have been created, but they are not accepting traffic (that is, VMs have been created, but the average value of the metrics is still above the threshold)

- Verify that the user has configured the templates in such a way that the VMs created from the templates can start serving traffic without any manual intervention.
- Verify that the service is running on the VMs, on the configured member port.
- Send a ping request to the gateway (virtual router), from the VM that is not accepting traffic.

The AutoScale configuration has been deleted, but the VMs continue to exist

- The VMs might not be deleted immediately after the AutoScale configuration is deleted. Wait for about 5 minutes after you have deleted the AutoScale configuration, and then check again.
- If the destruction of VMs has not commenced after 5 minutes, you might have to delete the VMs manually.

Clustering

A NetScaler cluster is a group of nCore appliances working together as a single system image. Each appliance of the cluster is called a *node*. The cluster can include as few as 2 or as many as 32 NetScaler nCore hardware or virtual appliances as nodes.

The client traffic is distributed between the nodes to provide high availability, high throughput, and scalability.

To create a cluster, you must add the appliances as cluster nodes, set up communication between the nodes, set up links to the client and server networks, configure the appliances, and configure the distribution of client and server traffic.

NetScaler Features Supported on a Cluster

The following table provides the NetScaler features that are supported or not supported in different NetScaler versions.

Note: The entry "Node-level" in the table indicates that the feature is supported only on individual cluster nodes.

NetScaler Feature	10	10.1	10.5
Basic load balancing	Yes	Yes	Yes
Load balancing persistency	Yes	Yes	Yes
SIP	Yes	Yes	Yes
maxClient	Yes	Yes	Yes
Spillover (connection and dynamic)	Yes	Yes	Yes
Spillover based on bandwidth	Yes	Yes	Yes
SSL (advanced policies)	Yes	Yes	Yes
SSL (classic policies)	No	No	No
SSL FIPS	No	No	No
SSL Certificate Bundle	No	No	No
Content switching	Yes	Yes	Yes
Content switching actions	No	Yes	Yes
Policy-based logging for content switching policies	No	Yes	Yes
DataStream	Yes	Yes	Yes
DNS load balancing	Yes	Yes	Yes
Rate limiting	No	Yes	Yes
Action analytics	No	Yes	Yes
Branch Repeater load balancing	No	Yes	Yes
GSLB	No	No	Yes

RTSP	No	No	No
DNSSEC	No	No	No
DNS64	No	No	No
FTP	No	No	No
TFTP	No	No	No
Connection mirroring	No	No	No
Compression control	Yes	Yes	Yes
Content filtering	Yes	Yes	Yes
TCP buffering	Yes	Yes	Yes
Cache redirection	Yes	Yes	Yes
Integrated caching	Node-Level	Node-level	Node-level
Large shared cache	No	Node-level	Node-level
Application firewall	No	No	Node-level
Distributed Denial-of-Service (DDoS)	Yes	Yes	Yes
Client Keep-alive	Yes	Yes	Yes
HTTP Denial-of-Service Protection (HDOSP)	Node-level	Node-level	Node-level
Priority queuing (PQ)	Node-level	Node-level	Node-level
Sure connect (SC)	Node-level	Node-level	Node-level
AppQoE	NA	Node-level	Yes
Surge protection	Node-level	Node-level	Node-level
MPTCP	No	No	Yes
Basic networking (IPv4 and IPv6)	Yes	Yes	Yes
OSPF (IPv4 and IPv6)	Yes	Yes	Yes
RIP (IPv4 and IPv6)	Yes	Yes	Yes
BGP (IPv4 and IPv6)	Yes	Yes	Yes
IS-IS (IPv4 and IPv6)	No	Yes	Yes
VLAN	Yes	Yes	Yes
ICMP	Yes	Yes	Yes
Fragmentation	Yes	Yes	Yes
MAC-Based Forwarding (MBF)	Yes	Yes	Yes
RNAT	Yes	Yes	Yes

ACL	Yes	Yes	Yes
Simple ACL	Yes	Yes	Yes
PBR	Yes	Yes	Yes
MSR	Yes	Yes	Yes
Policy-based RNAT	Yes	Yes	Yes
Path MTU Discovery	Yes	Yes	Yes
INAT	Yes	Yes	Yes
IP-ID	Yes	Yes	Yes
SNMP	Yes	Yes	Yes
IP-IP tunneling	No	Yes	Yes
Link load balancing	No	No	Yes
FIS (Failover Interface Set)	No	No	Yes
Link redundancy (LR)	No	No	Yes
NAT46	No	No	No
NAT64	No	No	No
v6 ReadyLogo	No	No	No
Traffic domains	No	No	Yes
Route monitor	No	No	No
GRE tunneling (CB)	No	No	No
Layer 2 mode	No	No	Yes
Net profiles	No	No	Yes
Policies (classic and advanced)	Yes	Yes	Yes
Rewrite	Yes	Yes	Yes
Responder	Yes	Yes	Yes
HTTP callout	Yes	Yes	Yes
HTTPS callout	No	Yes	Yes
Web server logging	Yes	Yes	Yes
Audit logging (syslog and nslog)	Yes	Yes	Yes
AAA-TM	No	Node-level	Node-level
AppFlow	No	Node-level	Node-level
Insight	No	No	No
HDX Insight	No	No	No
Use Source IP (USIP)	Yes	Yes	Yes
Location commands	Yes	Yes	Yes

HTML Injection	Yes	Yes	Yes
NITRO API	Yes	Yes	Yes
AppExpert	Yes	Yes	Yes
KRPC	Yes	Yes	Yes
VMAC/VRRP	No	No	Yes
NetScaler Push	No	No	No
Stateful Connection Failover	No	No	No
Graceful Shutdown	No	No	No
DBS AutoScale	No	No	No
DSR using TOS	No	No	No
Finer Startup-RR Control	Node-level	Node-level	Node-level
XML XSM	No	No	No
DHCP RA	No	No	No
Bridge Group	No	No	Yes (supported from NetScaler 10.5 Build 52.1115.e onwards)
Network Bridge	No	No	No
Web Interface on NetScaler (WIonNS)	No	No	No
EdgeSight Monitoring	No	No	No
Metrics tables - Local	No	No	No
DNS Caching	Node-level	Node-level	Node-level
Call Home	Node-level	Node-level	Node-level
NetScaler Gateway or SSL VPN	No	No	Node-level
CloudBridge Connector	No	No	No

Hardware and Software Requirements

Appliances that you add to a NetScaler cluster must:

- Be NetScaler nCore appliances. Clustering of NetScaler Classic appliances is not supported.
- Be of the same platform type (physical appliances or virtual appliances).
- Be of the same platform model type (for physical appliances).
- Be on the same subnet.
- Have the following licenses:

Till NetScaler 10.5 Build 51.10	For NetScaler 10.5 Build 52.11 and later releases
A separate cluster license file is required. This file must be copied to the /nsconfig/license/ directory of the configuration coordinator.	No separate cluster license is required.
Because of the separate cluster license file, cluster is available with Standard, Enterprise, and Platinum licenses.	Cluster is licensed with the Enterprise and Platinum licenses. Cluster is not available for Standard license.
All cluster nodes must have the same licenses.	All cluster nodes must have the same licenses.

- Be of the same software version and build.
- Be initially configured and connected to a common client-side and server-side network.

Note: For a cluster of virtual appliances, that has large configurations, it is recommended to use 6 GB RAM for each node of the cluster.

How Clustering Works

A NetScaler cluster is formed by grouping NetScaler appliances that satisfy the requirements specified in Hardware and Software Requirements.

The cluster must be configured through a management address called the *cluster IP address*. Configurations that are performed on the cluster IP address are propagated to all the cluster nodes.

Note: The NetScaler restricts the configurations that you can perform by accessing individual cluster nodes through their NetScaler IP (NSIP) address. These configurations are not propagated across the cluster nodes. For more information, see Operations Supported on Individual Cluster Nodes.

The cluster IP address is owned by a cluster node that is referred to as the *configuration coordinator*. The following figure shows a cluster configured through a cluster IP address:

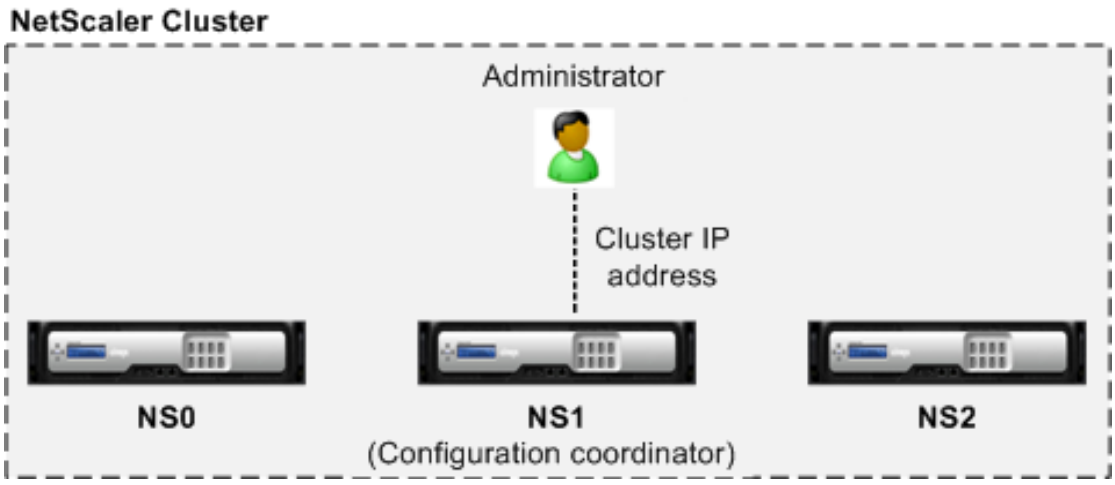


Figure 1. Configuring the NetScaler cluster

Synchronization Across Cluster Nodes

When a node is added to a cluster, the configurations and the files (SSL certificates, licenses, DNS, and so on) that are available on the configuration coordinator are synchronized to the newly added cluster node.

When an existing cluster node, that was intentionally disabled or that had failed, is once again added, the cluster compares the configurations available on the node with the configurations available on the configuration coordinator. If there is a mismatch in configurations, the node is synchronized by using one of the following:

- **Full synchronization.** If the difference between configurations exceeds 255 commands, all the configurations of the configuration coordinator are applied to the node that is rejoining the cluster. The node remains operationally unavailable for the duration of the synchronization.

- **Incremental Synchronization.** If the difference between configurations is less than or equal to 255 commands, only the configurations that are not available are applied to the node that is rejoining the cluster. The operational state of the node remains unaffected.

Command Propagation

While the above section talks about synchronizing the configurations of a configuration coordinator to a newly added (or re-added) node, the NetScaler also automatically propagates the configurations to all the existing cluster nodes as and when the configurations are performed.

Note: Because the cluster configurations are based on a quorum of the available nodes, a command is propagated to the other cluster nodes only when a majority of the nodes are in synch. If a majority of the nodes are not in synch or are in the process of synchronizing, the new commands cannot be accepted and therefore command propagation is temporarily halted.

Striped and Spotted IP Addresses

In a clustered deployment, VIP and SNIP addresses, can be striped or spotted.

- A *striped IP address* is active on all the nodes of the cluster. IP addresses configured on the cluster without specifying an owner node are active on all the cluster nodes.
- A *spotted IP address* is active on and owned exclusively by one node. IP addresses configured on the cluster by specifying an owner node are active only on the node that is specified as the owner.

The following figure shows striped and spotted IP addresses in a three-node cluster.

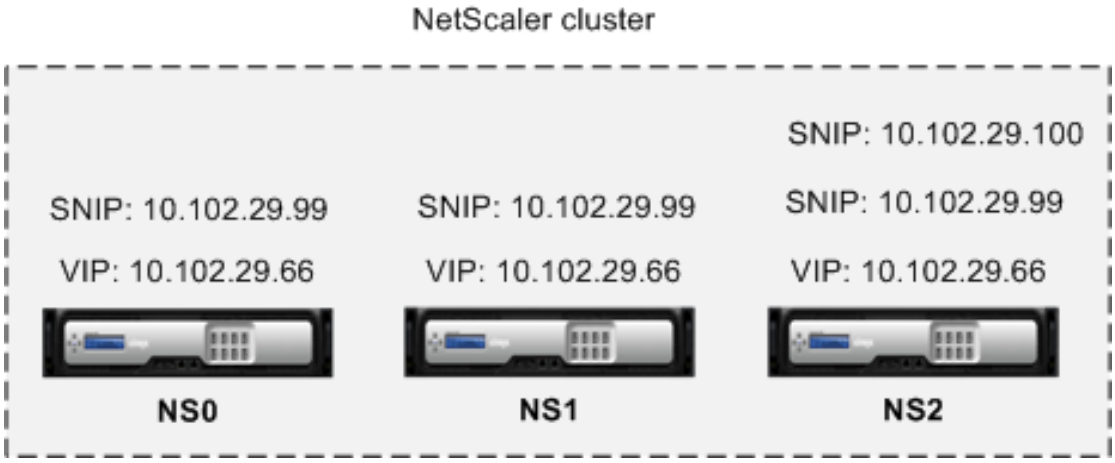


Figure 1. Three-node cluster with striped and spotted IP addresses

In the above figure, the VIP address 10.102.29.66 and SNIP address 10.102.29.99 is striped on all the cluster nodes. The SNIP address 10.102.29.100 is spotted on node NS2.

The following table shows the NetScaler-owned IP addresses that can be striped or spotted:

Table 1. Striped and Spotted IP addresses

NetScaler-owned IP addresses	Striped IP addresses	Spotted IP addresses
NSIP	No	Yes
Cluster IP address	No	No
VIP	Yes	No
SNIP	Yes	Yes (recommended)

Note:

- The cluster IP address is not a striped or spotted IP address. It is a floating IP address that is owned by the configuration coordinator, which is not a fixed node.

- Citrix recommends that you use only spotted IP addresses. You can use striped IP addresses only if there is a shortage of IP addresses. The use of striped IP addresses can result in ARP flux issues.

Communication in a Cluster Setup

The interfaces of NetScaler appliances that are added to a cluster, are prefixed with a node ID. This helps identify the cluster node to which the interface belongs. Therefore, the interface identifier c/u, where c is the controller number and u is the unit number, now becomes *n*/*c*/*u*, where n is the node ID. For example, in the following figure, interface 1/2 of node NS0 is represented as 0/1/2, interface 1/1 of node NS1 is represented as 1/1/1, and interface 1/4 of node NS2 is represented as 2/1/4.

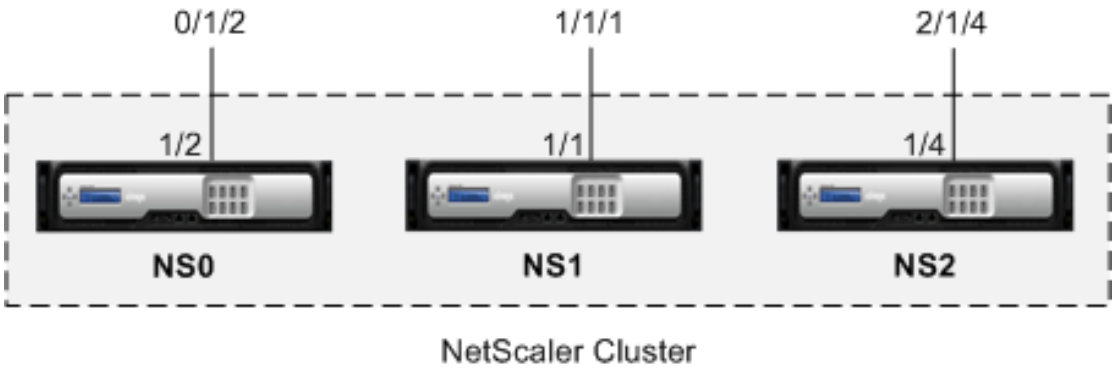


Figure 1. Interface naming convention in a cluster

Server communication

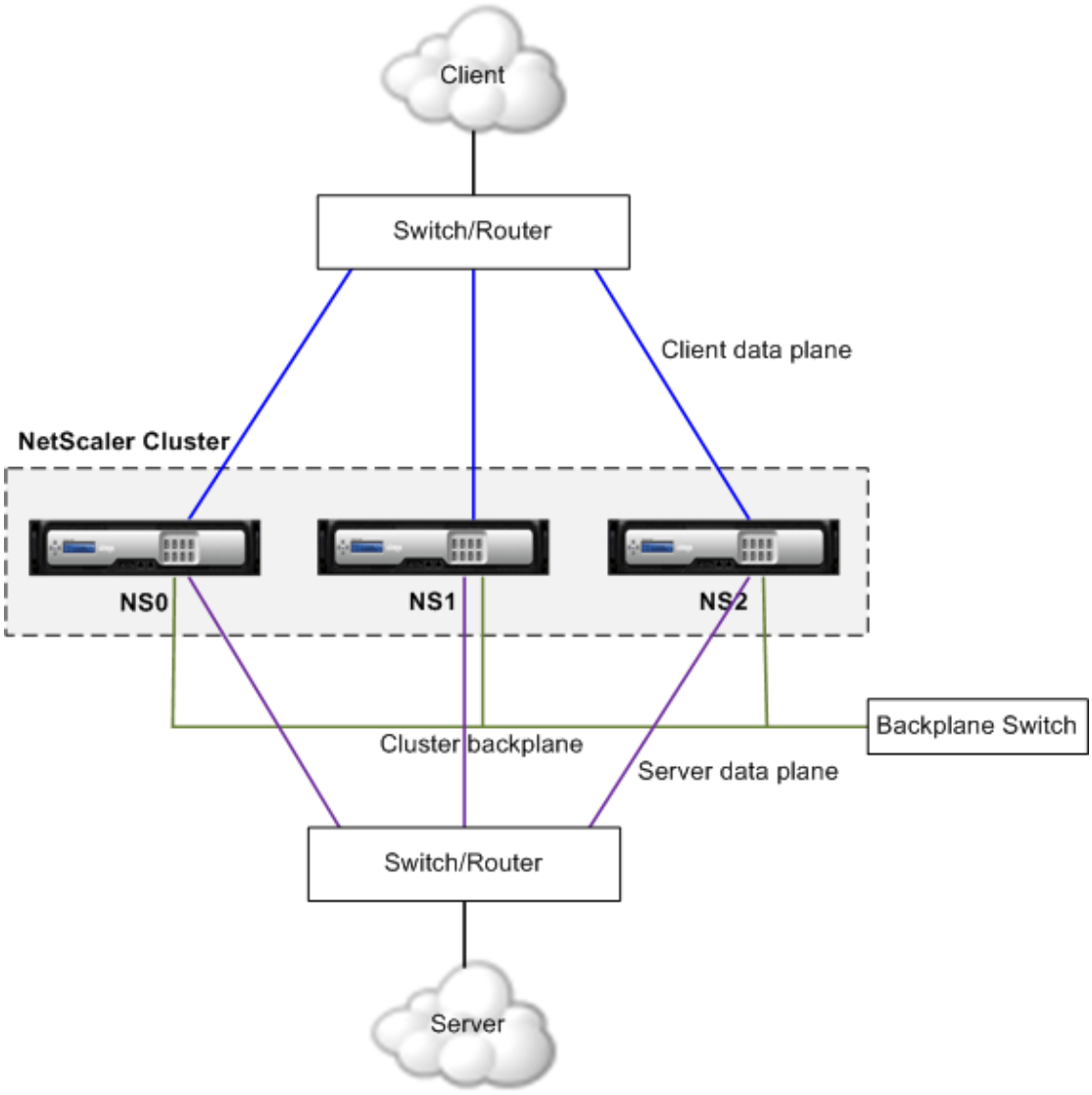
The cluster communicates with the server through the physical connections between the cluster node and the server-side connecting device. The logical grouping of these physical connections is called the *server data plane*.

Client communication

The cluster communicates with the client through the physical connections between the cluster node and the client-side connecting device. The logical grouping of these physical connections is called the *client data plane*.

Inter-node communication

The cluster nodes communicate with each other by using the *cluster backplane*. The backplane is a set of connections in which one interface of each node is connected to a common switch, which is called the *cluster backplane switch*. Each node of the cluster uses a special MAC address to communicate with other nodes through the backplane.



The following figure shows the logical grouping of the physical connections to form the client data plane, server data plane, and cluster backplane. Figure 2. Cluster communication interfaces

Traffic Distribution in a Cluster Setup

In a cluster setup, external networks view the collection of NetScaler appliances as a single entity. So, the cluster must select a single node that must receive the traffic. The cluster does this selection by using Equal Cost Multiple Path (ECMP) or cluster link aggregation traffic distribution mechanism. The selected node is called the *flow receiver*.

The flow receiver gets the traffic and then, using internal cluster logic determines the node that must process the traffic. This node is called the *flow processor*. The flow receiver steers the traffic to the flow processor over the backplane.

Note: The flow receiver and flow processor must be nodes capable of serving traffic.

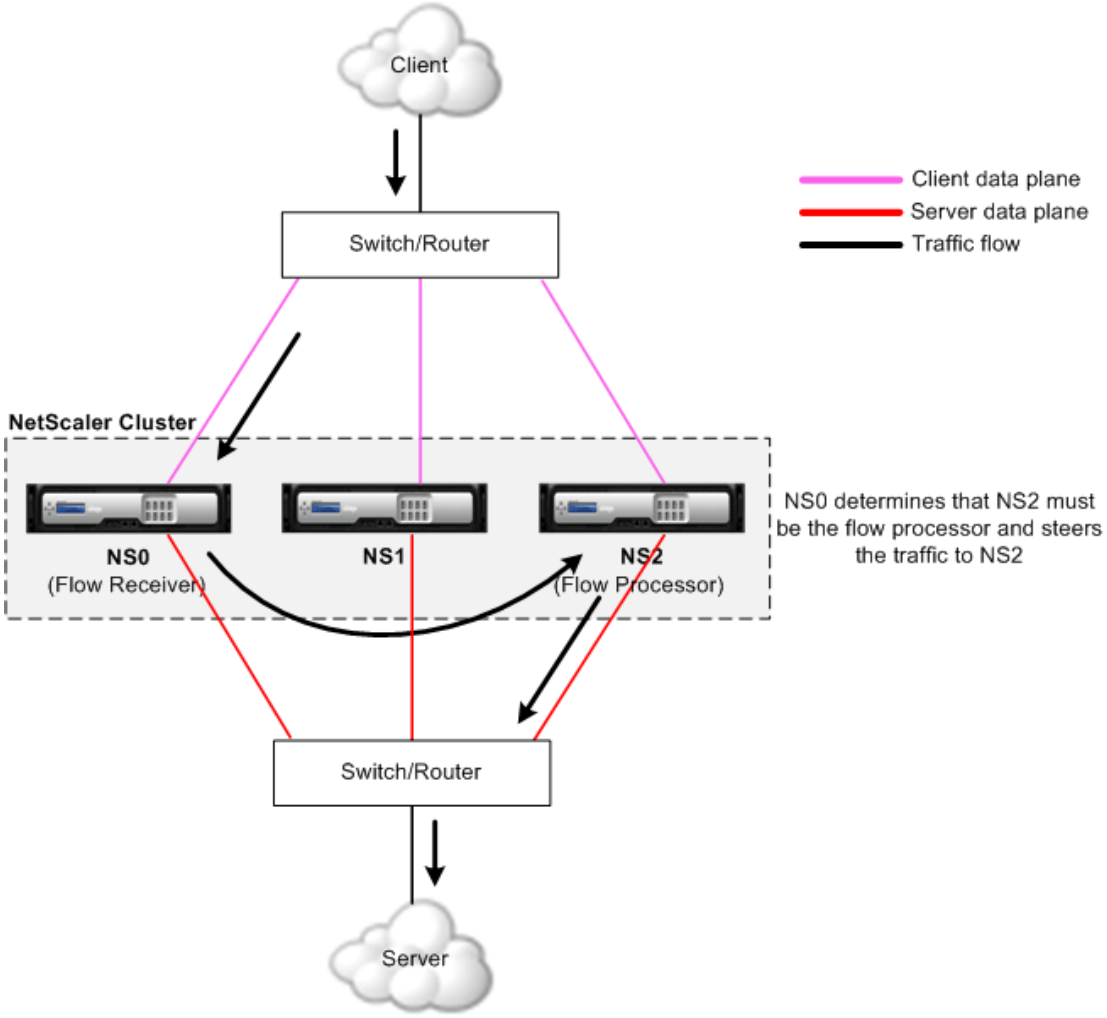


Figure 1. Traffic distribution in a cluster

The above figure shows a client request flowing through the cluster. The client sends a request to a virtual IP (VIP) address. A traffic distribution mechanism configured on the

client data plane selects one of the cluster nodes as the flow receiver. The flow receiver receives the traffic, determines the node that must process the traffic, and steers the request to that node (unless the flow receiver selects itself as the flow processor).

The flow processor establishes a connection with the server. The server processes the request and sends the response to the subnet IP (SNIP) address that sent the request to the server.

- If the SNIP address is a striped IP address, the traffic distribution mechanism configured on the server data plane selects one of the cluster nodes as the flow receiver. The flow receiver receives the traffic, determines the flow processor, and steers the request to the flow processor through the cluster backplane.
- If the SNIP address is a spotted IP address, the node that owns the SNIP address receives the response from the server.

In an asymmetric cluster topology (all cluster nodes are not connected to the external switch), you must use *linksets* either exclusively or combined with ECMP or cluster link aggregation. For more information, see Using Linksets.

Cluster and Node States

For a cluster to be functional, a majority of the nodes (n/2 + 1) must be online and be able to serve traffic by satisfying the following criteria:

- Admin state must be ACTIVE
- Operational state must be ACTIVE
- Health status must be UP

The following table describes the states of a cluster.

Type	Description
Admin	An admin state is configured when you add the node to the cluster. It indicates the purpose of the node, which can be in one of the following states: · **Active.** Nodes in this state serve traffic if they are operationally active and healthy. · **Passive.** Nodes in this state do not serve traffic but are in sync with the cluster. This is the default state of a cluster node. · **Spare.** Nodes in this state do not serve traffic but are in sync with the cluster. Spare nodes act as backup nodes for the cluster. If one of the nodes in the ACTIVE admin state becomes unavailable, a spare node becomes operationally active and starts serving traffic. **Note:** Whether the spare node remains operationally active depends on the preemption parameter of the add cluster instance command. If preemption is disabled, the spare node continues to serve traffic even if a node in ACTIVE admin state comes back online. If preemption is enabled, when a node in ACTIVE admin state comes back online, it preempts the spare node and starts serving traffic. The spare node goes back to inactive state.
Operational	When a node is part of a cluster, its operational state can change to ACTIVE, INACTIVE, or UNKNOWN. There are a number of reasons for a node being in INACTIVE or UNKNOWN state. Review the ns.log file or error counters to help determine the exact reason. **Note:** Passive nodes are always operationally INACTIVE. Spare nodes are ACTIVE only when they are serving traffic. Else, they are operationally INACTIVE.
Health	Depending on its health, a node can either be UP or NOT UP. To view the reasons for a node being in NOT UP state, run the show cluster node command for that node.

Routing in a Cluster

Routing in a cluster works in much the same way as routing in a standalone system. A few points to note:

- Routing runs only on spotted SNIP addresses and NSIP addresses.
- All routing configurations must be performed from the cluster IP address and the configurations are propagated to the other cluster nodes.
- Node-specific routing configurations must be performed by using the owner-node argument as follows:

```
!
interface vlan97
!
router ospf
 owner-node 0
  ospf router-id 97.131.0.1
 exit-owner-node
 owner-node 1
  ospf router-id 97.131.0.2
 exit-owner-node
 owner-node 2
  ospf router-id 97.131.0.3
 exit-owner-node
 redistribute kernel
 network 97.0.0.0/8 area 0
!
```

- Retrieve node-specific routing configurations by specifying the node(s) in the owner-node argument as follows:

```
> vtysh
ns# owner-node 0 1
ns(node-0 1)# show cluster state
ns(node-0 1)# exit-owner-node
```

- Clear node-specific routing configurations by specifying the node(s) in the owner-node argument as follows:

```
> vtysh
ns# owner-node 0 1
ns(node-0 1)# clear config
ns(node-0 1)# exit-owner-node
```

- Routing protocol daemons can run and adjacencies can be formed on active and inactive nodes of a cluster.
- Only active nodes advertise host routes to VIP addresses.

- Active and inactive nodes can learn dynamic routes and install them into the routing table.

- Routes learnt on a node are propagated to other nodes in the cluster only if route propagation is configured. This is mostly needed in asymmetric topologies where the unconnected nodes may not be able to form adjacencies.

  ns(config)# ns route-install propagate

  Note: Make sure that route propagation is not configured in a symmetric cluster topology as it can result in making the node unavailable to the cluster.

Setting up a NetScaler Cluster

To set up a cluster, begin by setting up the inter-node communication. Then, create the cluster by adding the first node to the cluster and by assigning a cluster IP address to that node. After you have created the cluster, you can add more nodes to the cluster.

Every appliance that you want to add to the cluster must:

- Be NetScaler nCore appliances. Clustering of NetScaler Classic appliances is not supported.
- Be of the same platform type (physical appliances or virtual appliances).
- Be of the same platform model type (for physical appliances).
- Be on the same subnet.
- Have the following licenses:

Till NetScaler 10.5 Build 51.10	For NetScaler 10.5 Build 52.11 and later releases
A separate cluster license file is required. This file must be copied to the /nsconfig/license/ directory of the configuration coordinator.	No separate cluster license is required.
Because of the separate cluster license file, cluster is available with Standard, Enterprise, and Platinum licenses.	Cluster is licensed with the Enterprise and Platinum licenses. Cluster is not available for Standard license.
All cluster nodes must have the same licenses.	All cluster nodes must have the same licenses.

- Be of the same software version and build.
- Be initially configured and connected to a common client-side and server-side network.

Setting up Inter-Node Communication

The nodes in a cluster communicate with each other through the cluster backplane.

To set up the cluster backplane, do the following for every node

1. Identify the network interface that you want to use for the backplane.
2. Connect an Ethernet or optical cable from the selected network interface to the cluster backplane switch.

For example, to use interface 1/2 as the backplane interface for node 4, connect a cable from the 1/2 interface of node 4 to the backplane switch.

Important points to note while setting up the cluster backplane

- Do not use the appliance's management interface (0/1) as the backplane interface.
- Interfaces used for the backplane must not be used for the client data plane or server data plane.
- You can configure a link aggregate (LA) channel to optimize the throughput of the cluster backplane.
- The backplane interfaces of all nodes of a cluster must be connected to the same switch and bound to the same L2 VLAN. The backplane interfaces, by default, have presence on all L3 VLANs configured on the cluster.
- If you have multiple clusters with the same cluster instance ID, make sure that the backplane interfaces of each cluster are bound to a different VLAN.
- It is recommended that you dedicate a separate switch only for the backplane, so that large amounts of traffic are handled seamlessly.
- The backplane interface is always monitored, regardless of the HA monitoring settings of that interface.
- In a cluster that is deployed on a XenServer and with MAC spoofing enabled, the NIC (XenServer Vswitch) can drop packets sent on the backplane. You must disable MAC spoofing on the XenServer.
- In a cluster that is deployed on a HyperV and with MAC spoofing disabled on the backplane interface, the steered packets are dropped. You must enable MAC spoofing to form a cluster on the HyperV.
- The Maximum Transmission Unit (MTU) for interfaces of the backplane switch must be greater than or equal to 1512 bytes, if features like MBF, L2 policies, ACLs, routing in CLAG deployments are configured. The MTU on the cluster backplane is automatically

updated.

Creating a NetScaler Cluster

To create a cluster, you must create a cluster instance and configure a cluster IP address on the first appliance that you add to the cluster. This node is called the configuration coordinator. As the name suggests, all cluster configurations are performed on this node, by accessing it through the cluster IP address. The role of a cluster configuration coordinator is not fixed to a specific cluster node. It can change over time. For example, if the current configuration coordinator fails, the cluster elects one of the other nodes as the new configuration coordinator, which then owns the cluster IP address.

The configurations of the appliance are cleared by implicitly executing the clear ns config `extended` command.

Note:

- The default VLAN and NSVLAN are not cleared from the appliance. Therefore, if you want the NSVLAN on the cluster, make sure it is created before the appliance is added to the cluster.
- The SNIP addresses and all VLAN configurations are cleared from the appliance.

To create a cluster by using the command line interface

1. Log on to an appliance (for example, appliance with NSIP address 10.102.29.60) that you want to add to the cluster.
2. Add a cluster instance.

   add cluster instance <clId>

   Note: Make sure that the cluster instance ID is unique within a LAN.
3. Add the appliance to the cluster.

   add cluster node <nodeId> <IPAddress> -state <state> -backplane <interface_name>

   Example

   Adding a node for a L2 cluster (all cluster nodes are in the same network).

   > add cluster node 0 10.102.29.60 -state PASSIVE -backplane 0/1/1
4. Add the cluster IP address (for example, 10.102.29.61) on this node.

   add ns ip <IPAddress> <netmask> -type `clip`

   Example

   > add ns ip 10.102.29.61 255.255.255.255 -type clip
5. Enable the cluster instance.

   enable cluster instance <clId>
6. Save the configuration.

   save ns config
7. Warm reboot the appliance.

   reboot -warm

   Verify the cluster configurations by using the show cluster instance command. Verify that the output of the command displays the NSIP address of the appliance as a node of the cluster.

To create a cluster by using the configuration utility

1. Log on to an appliance (for example, an appliance with NSIP address 10.102.29.60) that you intend to add to the cluster.
2. Navigate to System > Cluster.
3. In the details pane, click the Manage Cluster link.
4. In the Cluster Configuration dialog box, set the parameters required to create a cluster. For a description of a parameter, hover the mouse cursor over the corresponding text box.
5. Click Create.
6. In the Configure cluster instance dialog box, make sure that the Enable cluster instance check box is selected.
7. In the Cluster Nodes pane, select the node and click Open.
8. In the Configure Cluster Node dialog box, set the State.
9. Click OK, and then click Save.
10. Warm reboot the appliance.

Parameter Descriptions (of commands listed in the CLI procedure)

add cluster instance

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add cluster node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add ns ip

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

enable cluster instance

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

save ns config

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

reboot

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Adding a Node to the Cluster

You can seamlessly scale the size of a cluster to include a maximum of 32 nodes. When an appliance is added to the cluster, the licenses on that appliance are checked against the licenses available on the configuration coordinator. If the licenses match, the appliance is added to the cluster. The existing configurations of the appliance are cleared, and the cluster configurations are synchronized with the node.

There can be an intermittent drop in traffic while the synchronization is in progress.

Note: If you use the command line interface to add a node, the new node does not become a functional part of the cluster until you join it to the cluster. After logging on to the cluster IP address and adding the node, log on to that node and join the node to the cluster. Alternatively, you can add the node from the command line and use the configuration utility to join the node to the cluster. If you use the configuration utility, you need only log on to the cluster IP address and add the node. The newly added node is automatically joined to the cluster.

Important: Before you add the node, make sure that you have set up the backplane interface for that node. Additional considerations include the following:

- If you want the NSVLAN on the cluster, make sure that the NSVLAN is created on the appliance before it is added to the cluster.
- Citrix recommends that you add the node as a passive node. Then, after joining the node to the cluster, complete the node specific configuration from the cluster IP address. Run the force cluster sync command if the cluster has only spotted IP addresses, has L3 VLAN binding, or has static routes.
- When an appliance with a preconfigured link aggregate (LA) channel is added to a cluster, the LA channel continues to exist in the cluster environment. The LA channel is renamed from LA/x to nodeId/LA/x, where LA/x is the LA channel identifier.

To add a node to the cluster by using the command line interface

1. Log on to the cluster IP address and, at the command prompt, do the following:
   a. Add the appliance (for example, 10.102.29.70) to the cluster.

      add cluster node <nodeId> <IPAddress> -state <state> -backplane <interface_name>

      Example

      > add cluster node 1 10.102.29.70 -state PASSIVE -backplane 1/1/1

   b. Save the configuration.

      save ns config
2. Log on to the newly added node (for example, 10.102.29.70) and do the following:
   a. Join the node to the cluster.

      join cluster -clip <ip_addr> -password <password>

      Example

      > join cluster -clip 10.102.29.61 -password nsroot

   b. Save the configuration.

      save ns config

   c. Warm reboot the appliance.

      reboot -warm

To add a node to the cluster by using the configuration utility

1. Log on to the cluster IP address.
2. Navigate to System > Cluster > Nodes.
3. In the details pane, click Add to add the new node (for example, 10.102.29.70).
4. In the Create Cluster Node dialog box, configure the new node. For a description of a parameter, hover the mouse cursor over the corresponding text box.
5. Click Create. When prompted to perform a warm reboot, click Yes.

To join a previously added node to the cluster by using the configuration utility

If you have used the command line to add a node to the cluster, but have not joined the node to the cluster, you can use the following procedure.

1. Log on to the node that you want to join to the cluster (for example, 10.102.29.70).
2. Navigate to System > Cluster.
3. In the details pane, under Get Started, click the Join Cluster link.
4. In the Join to existing cluster dialog box, set the cluster IP address and the nsroot password of the configuration coordinator. For a description of a parameter, hover the mouse cursor over the corresponding text box.
5. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

add cluster node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

save ns config

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

join cluster

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

reboot

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Removing a Cluster Node

Removing a node from a cluster is a two-step process:

1. Remove the reference to the cluster instance from the node. The cluster configurations are cleared from the node by internally executing the clear ns config command with extended as the argument specifying the level of execution. The SNIP addresses and all VLAN configurations (except the default VLAN and NSVLAN) are also cleared from the appliance.

2. Remove the node from the cluster.

Note:

- When you remove a node that is the configuration coordinator, all current cluster IP address sessions are invalidated. Another cluster node is selected as the configuration coordinator, and the cluster IP address is assigned to that node. You must start a new cluster IP address session.

- To delete the cluster, you must remove each node individually. When you remove the last node, the cluster IP address(es) are deleted.

To remove a cluster node by using the command line interface

1. Log on to the node that you want to remove from the cluster and do the following:

   a. Remove the reference to the cluster instance.

      rm cluster instance <clId>

   b. Save the configuration.

      save ns config

   Note: To remove the last node of a cluster, you must only remove the cluster instance from that node. The node is automatically removed from the cluster.

2. Log on to the cluster IP address and do the following:

   a. Remove the node from which you removed the cluster instance.

      rm cluster node <nodeId>

   b. Save the configuration.

      save ns config

   Note: Make sure you do not run the rm cluster node command from the local node as this results in inconsistent configurations between the configuration coordinator and the node.

To remove a cluster node by using the configuration utility

1. Log on to the cluster IP address.
2. Navigate to System > Cluster > Nodes.
3. In the details pane, select the node that you want to remove, and click Remove.

Parameter Descriptions (of commands listed in the CLI procedure)

rm cluster instance

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

save ns config

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

rm cluster node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Removing a Node from a Cluster Deployed Using Cluster Link Aggregation

To remove a node from a cluster that uses cluster link aggregation as the traffic distribution mechanism, you must make sure that the node is made passive so that it does not receive any traffic and then, on the upstream switch, remove the corresponding interface from the channel.

For detailed information on cluster link aggregation, see Using Cluster Link Aggregation.

To remove a node from a cluster that uses cluster link aggregation as the traffic distribution mechanism

1. Log on to the cluster IP address.
2. Set the state of the cluster node that you want to remove to PASSIVE.

   set cluster node <nodeId> -state PASSIVE
3. On the upstream switch, remove the corresponding interface from the channel by using switch-specific commands.

   Note: You do not have to manually remove the nodes interface on the cluster link aggregation channel. It is automatically removed when the node is deleted in the next step.
4. Remove the node from the cluster.

   rm cluster node <nodeId>

Parameter Descriptions (of commands listed in the CLI procedure)

set cluster node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

rm cluster node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Viewing the Details of a Cluster

You can view the details of the cluster instance and the cluster nodes by logging on to the cluster IP address.

To view details of a cluster instance by using the command line interface

Log on to the cluster IP address and, at the command prompt, type:

show cluster instance <clId>

Note: When executed from the NSIP address of a cluster node that is not the configuration coordinator, this command displays the status of the cluster on this node.

To view details of a cluster node by using the command line interface

Log on to the cluster IP address and, at the command prompt, type:

show cluster node <nodeId>

To view details of a cluster instance by using the configuration utility

1. Log on to the cluster IP address.
2. Navigate to System > Cluster.
3. In the details pane, under Get Started, click the Manage Cluster link to view the details of the cluster.

To view details of a cluster node by using the configuration utility

1. Log on to the cluster IP address.
2. Navigate to System > Cluster > Nodes.
3. In the details pane, click the node for which you want to view the details.

Parameter Descriptions (of commands listed in the CLI procedure)

show cluster instance

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show cluster node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Distributing Traffic Across Cluster Nodes

After you have created the NetScaler cluster and performed the required configurations, you must deploy Equal Cost Multiple Path (ECMP) or cluster Link Aggregation (LA) on the client data plane (for client traffic) or server data plane (for server traffic). These mechanisms distribute external traffic across the cluster nodes.

Using Equal Cost Multiple Path (ECMP)

With the Equal Cost Multiple Path (ECMP) mechanism, the router has equal-cost routes to VIP addresses with the next hops as the active nodes of the cluster. The router uses a stateless hash-based mechanism to distribute traffic across the routes.

Note: Routes are limited to the maximum number of ECMP routes supported by the upstream router.

To use ECMP, you must first enable the required routing protocol (OSPF, RIP, BGP, or ISIS) on the cluster IP address. You must bind the interfaces and the spotted IP address (with dynamic routing enabled) to a VLAN. Configure the selected routing protocol and redistribute the kernel routes on the ZebOS by using the vtysh shell.

You must perform similar configurations on the cluster IP address and on the external connecting device.

Note:

- All routing configurations must be done through the cluster IP address. No configurations must be performed on individual cluster nodes.
- Make sure that the licenses on the cluster support dynamic routing, otherwise ECMP does not work.
- ECMP is not supported for wildcard virtual servers since RHI needs a VIP address to advertise to a router and wildcard virtual servers do not have associated VIP addresses.

You must have detailed knowledge of routing protocols to use ECMP. For more information, see "Configuring Dynamic Routes. For more information on routing in a cluster, see "Routing in a Cluster".

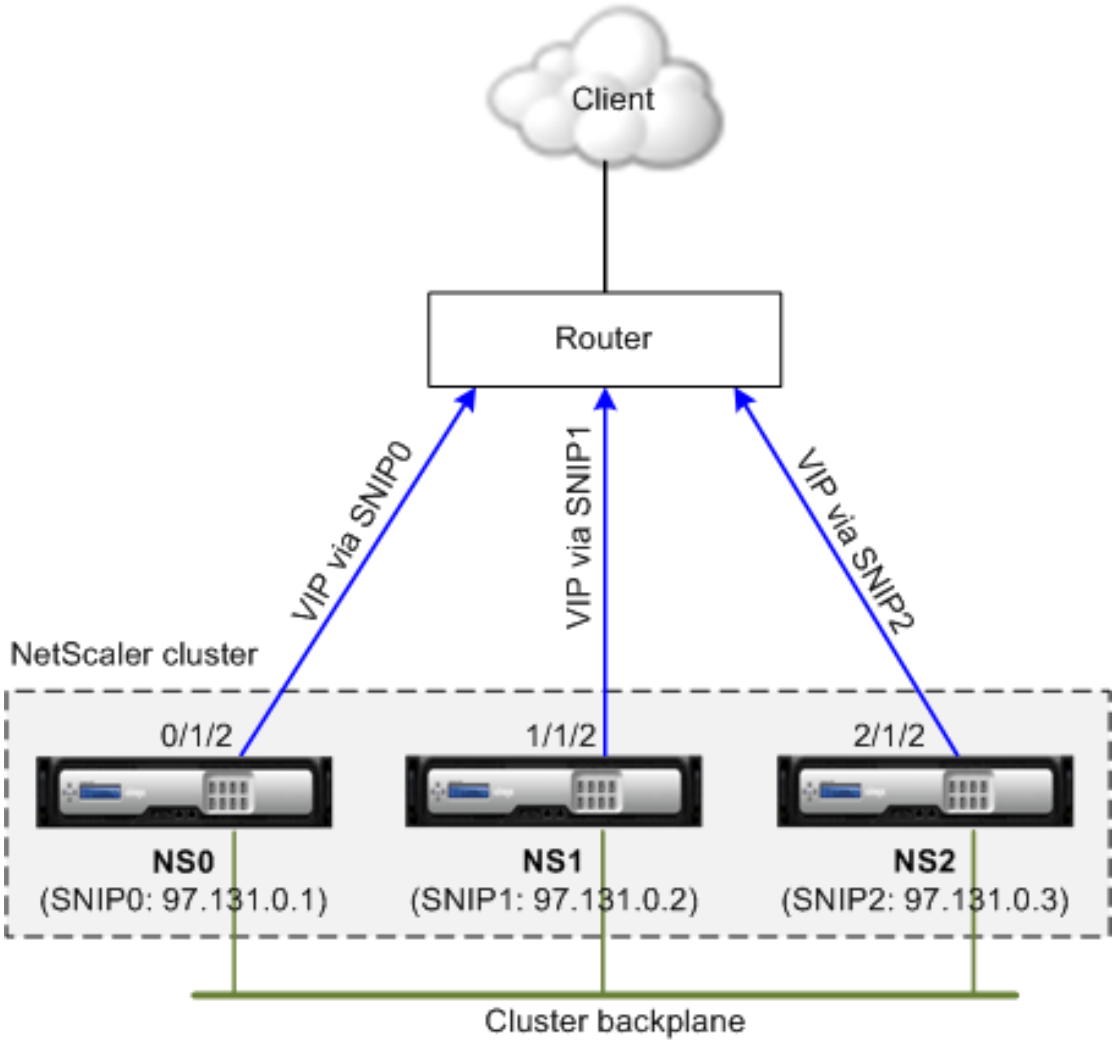


Figure 1. ECMP topology

As seen in the above figure, the ECMP router can reach the VIP address via SNIP0, SNIP1, or SNIP2.

To configure ECMP on the cluster by using the command line interface

1. Log on to the cluster IP address.
2. Enable the routing protocol.

   enable ns feature <feature>

   Example: To enable the OSPF routing protocol.

   > enable ns feature ospf

3. Add a VLAN.

   add vlan <id>

   Example

   > add vlan 97

4. Bind the interfaces of the cluster nodes to the VLAN.

   bind vlan <id> -ifnum <interface_name>

   Example

   > bind vlan 97 -ifnum 0/1/2 1/1/2 2/1/2

5. Add a spotted SNIP address for each node and enable dynamic routing on it.

   add ns ip <SNIP> <netmask> -ownerNode <positive_integer> -dynamicRouting ENABLED

   Example

   > add ns ip 97.131.0.1 255.0.0.0 -ownerNode 0 -dynamicRouting ENABLED -type SNIP
   > add ns ip 97.131.0.2 255.0.0.0 -ownerNode 1 -dynamicRouting ENABLED -type SNIP
   > add ns ip 97.131.0.3 255.0.0.0 -ownerNode 2 -dynamicRouting ENABLED -type SNIP

6. Bind one of the spotted SNIP addresses to the VLAN. When you bind one spotted SNIP address to a VLAN, all other spotted SNIP addresses defined on the cluster in that subnet are automatically bound to the VLAN.

   bind vlan <id> -IPAddress <SNIP> <netmask>

   Example

   > bind vlan 97 -ipAddress 97.131.0.1 255.0.0.0

   Note: You can use NSIP addresses of the cluster nodes instead of adding SNIP addresses. If so, you do not have to perform steps 3 - 6.

7. Configure the routing protocol on ZebOS using vtysh shell.

   Example: To configure OSPF routing protocol on node IDs 0, 1, and 2.

   ```
   > vtysh

   !
   interface vlan97
   !
   router ospf
    owner-node 0
     ospf router-id 97.131.0.1
    exit-owner-node
    owner-node 1
     ospf router-id 97.131.0.2
    exit-owner-node
    owner-node 2
     ospf router-id 97.131.0.3
    exit-owner-node
    redistribute kernel
    network 97.0.0.0/8 area 0
   !
   ```

   Note: For VIP addresses to be advertised, RHI setting must done by using the vserverRHILevel parameter as follows:

   add ns ip <IPAddress> <netmask> -type VIP -vserverRHILevel <vserverRHILevel>

   For OSPF specific RHI settings, there are additional settings that can be done as follows:

   add ns ip <IPAddress> <netmask> -type VIP -ospfLSAType (TYPE1 | TYPE5) -ospfArea <positive_integer>

   Use the add ns ip6 command to perform the above commands on IPv6 addresses.

8. Configure ECMP on the external switch. The following sample configurations are provided for the Cisco® Nexus 7000 C7010 Release 5.2(1) switch. Similar configurations must be performed on other switches.

   ```
   //For OSPF (IPv4 addresses)
   Global config:
   Configure terminal
   feature ospf

   Interface config:
   Configure terminal
   interface Vlan10
      no shutdown
      ip address 97.131.0.5/8

   Configure terminal
   router ospf 1
   network 97.0.0.0/8 area 0.0.0.0
   --------------------------------
   ```

```
//For OSPFv3 (IPv6 addresses)
Global config:
Configure terminal
feature ospfv3

Configure terminal
interface Vlan10
   no shutdown
   ipv6 address use-link-local-only
   ipv6 router ospfv3 1 area 0.0.0.0

Configure terminal
router ospfv3 1
```

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add vlan

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind vlan

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add ns ip

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Using Cluster Link Aggregation

Cluster link aggregation, as the name suggests, is a group of interfaces of cluster nodes. It is an extension of NetScaler link aggregation. The only difference is that, while link aggregation requires the interfaces to be from the same device, in cluster link aggregation, the interfaces are from different nodes of the cluster.

For more information about link aggregation, see "Configuring Link Aggregation".

Cluster link aggregation can be either static or dynamic.

For example, consider a three-node cluster where all three nodes are connected to the upstream switch. A cluster LA channel (CLA/1) is formed by binding interfaces 0/1/2, 1/1/2, and 2/1/2.

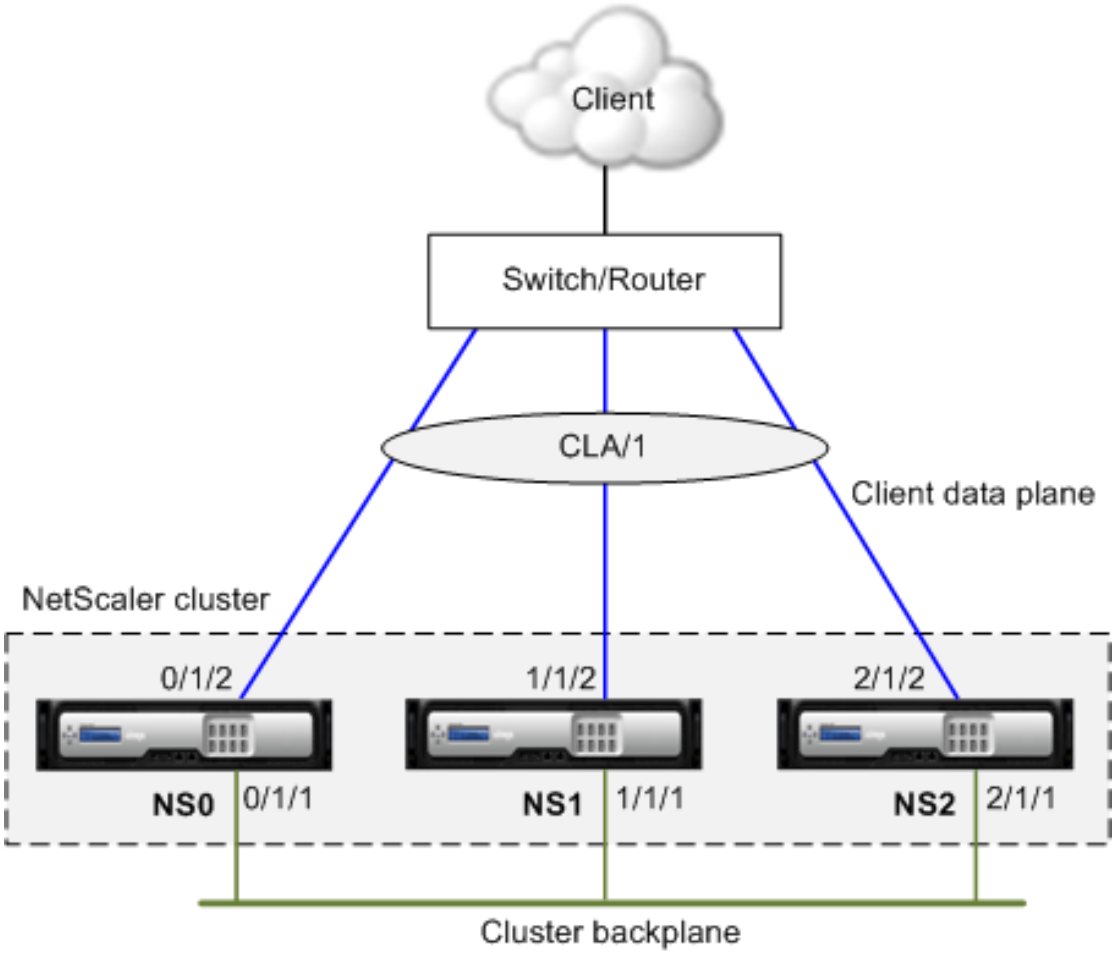


Figure 1. Cluster Link Aggregation topology

A cluster LA channel has the following attributes:

- Each channel has a unique MAC agreed upon by cluster nodes.

- The channel can bind both local and remote nodes' interfaces.
- A maximum of four cluster LA channels are supported in a cluster.
- Backplane interfaces cannot be part of a cluster LA channel.
- When an interface is bound to a cluster LA channel, the channel parameters have precedence over the network interface parameters. A network interface can be bound to one channel only.

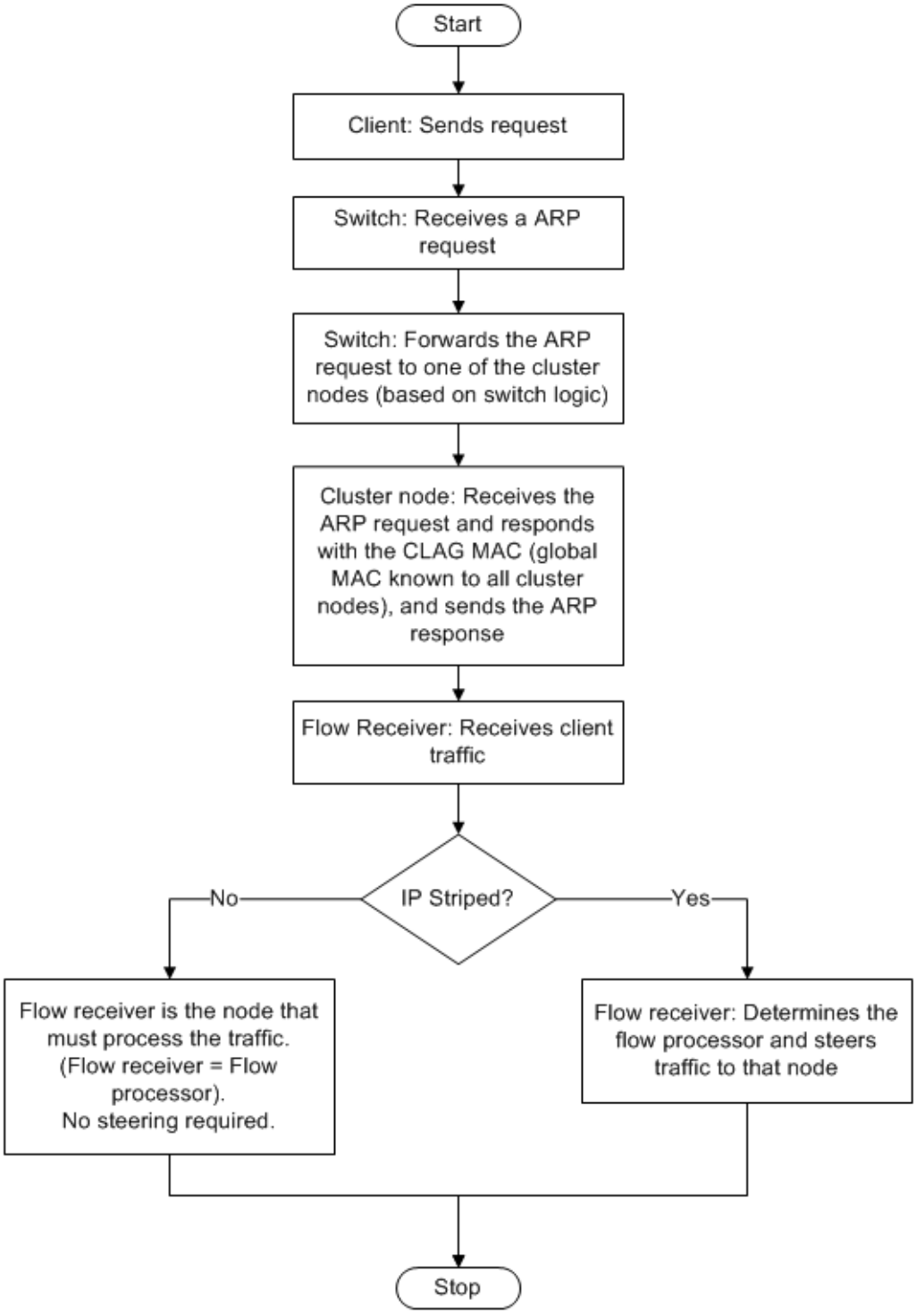


Figure 2. Traffic distribution flow using cluster LA

Static Cluster Link Aggregation

You must configure a static cluster LA channel on the cluster IP address and on the external connecting device. If possible, configure the upstream switch to distribute traffic based on IP address or port instead of MAC address.

For more information about configuring a static LA channel, see "Configuring Link Aggregation Manually".

To configure a static cluster LA channel by using the command line interface

1. Log on to the cluster IP address.

   Note: Make sure that you configure the cluster LA channel on the cluster IP address before configuring link aggregation on the external switch. Otherwise, the switch will forward traffic to the cluster even though the cluster LA channel is not configured. This can lead to loss of traffic.

2. Create a cluster LA channel.

   add channel <id> -speed <speed>

   Example

   > add channel CLA/1 -speed 1000

   Note: You must not specify the speed as AUTO. Rather, you must explicitly specify the speed as 10, 100, 1000, or 10000. Only interfaces that have the speed matching the <speed> attribute in the cluster LA channel are added to the active distribution list.

3. Bind the required interfaces to the cluster LA channel. Make sure that the interfaces are not used for the cluster backplane.

   bind channel <id> <ifnum>

   Example

   > bind channel CLA/1 0/1/2 1/1/2 2/1/2

4. Verify the configurations.

   show channel <id>

   Example

   > show channel CLA/1

   Note: You can bind the cluster LA channel to a VLAN by using the bind vlan command. The interfaces of the channel are automatically bound to the VLAN.

5. Configure static LA on the external switch. The following sample configurations are provided for the Cisco® Nexus 7000 C7010 Release 5.2(1). Similar configurations must be performed on other switches.

   Global config:
   Configure terminal

   Interface level config:

   interface Ethernet2/47

```
    switchport
    switchport access vlan 10
    channel-group 7 mode on
    no shutdown

interface Ethernet2/48
    switchport
    switchport access vlan 10
    channel-group 7 mode on
    no shutdown
```

Parameter Descriptions (of commands listed in the CLI procedure)

add channel

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind channel

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show channel

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Dynamic Cluster Link Aggregation

Dynamic cluster LA channel uses Link Aggregation Control Protocol (LACP). For more information about configuring a dynamic LA channel, see "Configuring Link Aggregation by Using the Link Aggregation Control Protocol".

You must perform similar configurations on the cluster IP address and on the external connecting device. If possible, configure the upstream switch to distribute traffic based on IP address or port instead of MAC address.

Points to remember:

- Enable LACP (by specifying the LACP mode as either ACTIVE or PASSIVE).

  Note: Make sure the LACP mode is not set as PASSIVE on both the NetScaler cluster and the external connecting device.

- Specify the same LACP key on each interface that you want to be the part of the channel. For creating a cluster LA channel, the LACP key can have a value from 5 through 8. For example, if you set the LACP key on interfaces 0/1/2, 1/1/2, and 2/1/2 to 5, CLA/1 is created. The interfaces 0/1/2, 1/1/2, and 2/1/2 are automatically bound to CLA/1. Similarly, if you set the LACP key to 6, CLA/2 channel is created.

- Specify the LAG type as Cluster.

To configure a dynamic cluster LA channel by using the command line interface

On the cluster IP address, for each interface that you want to add to the cluster LA channel, type:

```
set interface <id> -lacpMode <lacpMode> -lacpKey <positive_integer> -lagType CLUSTER
```

Example: To configure a cluster LA channel for 3 interfaces.

```
> set interface 0/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 1/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 2/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
```

Note: Optionally, you can enable link redundancy support on the dynamic LA interface or channel as follows:

- set interface CLA/1 -lr ON

- set channel CLA/2 -lr ON

Similarly, configure dynamic LA on the external switch. The following sample configurations are provided for the Cisco® Nexus 7000 C7010 Release 5.2(1). Similar configurations must be performed on other switches.

Global config:
Configure terminal
feature lacp
Interface level config:

```
interface Ethernet2/47
   switchport
   switchport access vlan 10
   channel-group 7 mode active
   no shutdown

interface Ethernet2/48
   switchport
   switchport access vlan 10
   channel-group 7 mode active
   no shutdown
```

Parameter Descriptions (of commands listed in the CLI procedure)

set interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

set channel

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Using Linksets

Linksets must be used when some cluster nodes are not physically connected to the external network. In such a cluster topology, the unconnected cluster nodes use the interfaces specified in the linkset to communicate with the external network through the cluster backplane. Linksets are typically used in scenarios when the connecting devices have insufficient ports to connect the cluster nodes.

Additionally, linksets must be used in the following scenarios:

- For topologies that require MAC-based Forwarding (MBF).
- To improve manageability of ACL and L2 policies involving interfaces. You must define a linkset of the interfaces and add ACL and L2 policies based on linksets.

Linksets must be configured only through the cluster IP address.

For example, consider a three node cluster where the upstream switch has only two ports available. Using linksets, you can connect two nodes to the switch and leave the third node unconnected. In the following figure, a linkset (LS/1) is formed by binding the interfaces 0/1/2 and 1/1/2. NS2 is the unconnected node of the cluster.

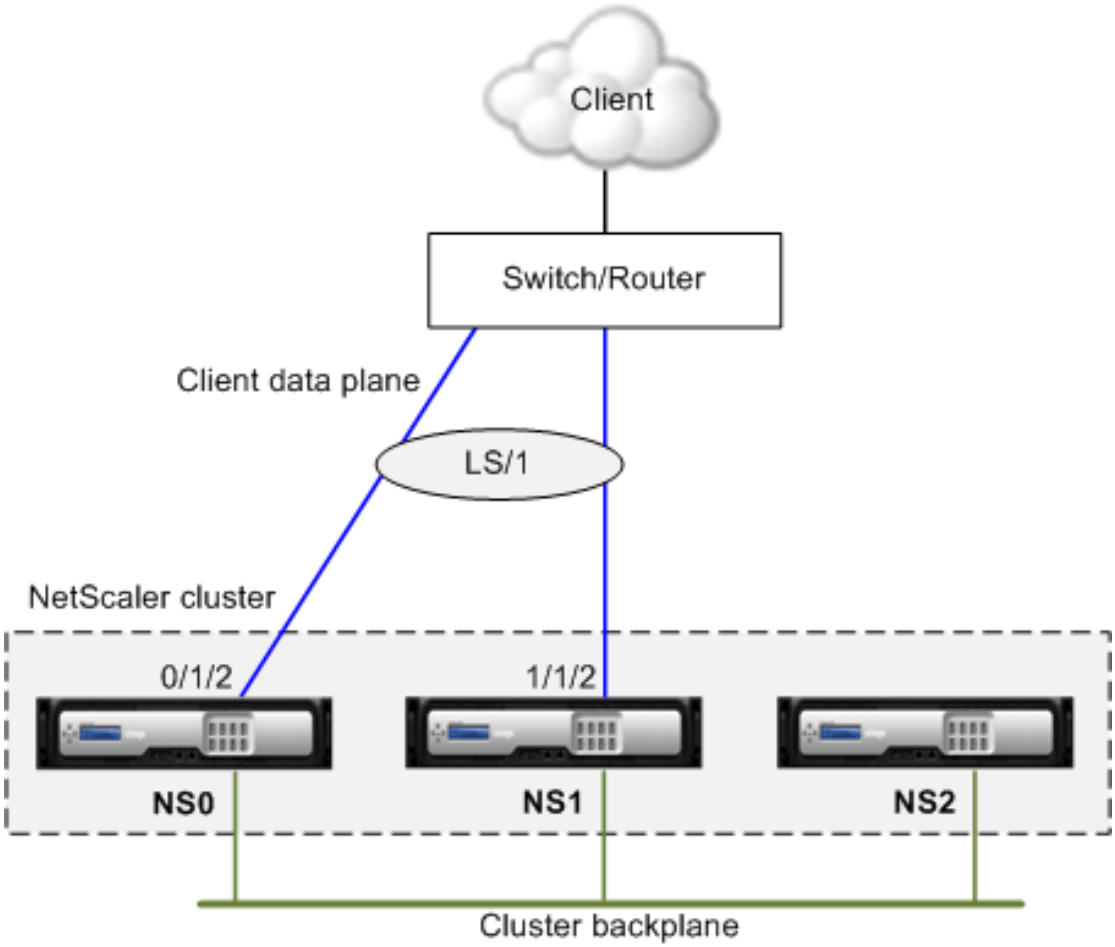


Figure 1. Linksets topology

The linkset informs NS2 that it can use interfaces 0/1/2 and 1/1/2 to communicate with the network devices. All traffic to and from NS2 is now routed through interfaces 0/1/2 or 1/1/2.

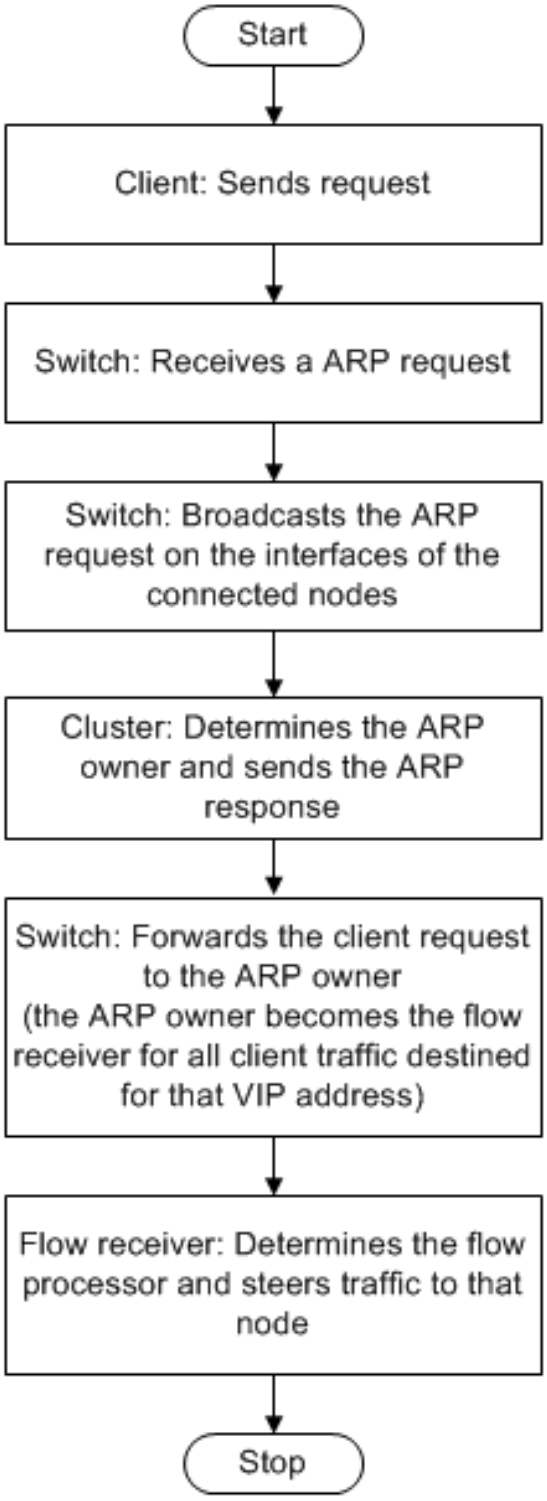


Figure 2. Traffic distribution flow using linksets

To configure a linkset by using the command line interface

1. Log on to the cluster IP address.
2. Create a linkset.

   add linkset <id>

   Example

   > add linkset LS/1

3. Bind the required interfaces to the linkset. Make sure the interfaces are not used for the cluster backplane.

   bind linkset <id> -ifnum <interface_name> ...

   Example

   > bind linkset LS/1 -ifnum 0/1/2 1/1/2

4. Verify the linkset configurations.

   show linkset <id>

   Example

   > show linkset LS/1

   Note: You can bind the linkset to a VLAN by using the bind vlan command. The interfaces of the linkset are automatically bound to the VLAN.

To configure a linkset by using the configuration utility

1. Log on to the cluster IP address.
2. Navigate to Network > Linkset.
3. In the details pane, click Add.
4. In the Create Linkset dialog box:
   a. Specify the name of the linkset by setting the Linkset parameter.
   b. Specify the Interfaces to be added to the linkset and click Add. Repeat this step for each interface you want to add to the linkset.
5. Click Create, and then click Close.

Parameter Descriptions (of commands listed in the CLI procedure)

add linkset

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind linkset

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show linkset

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Managing the NetScaler Cluster

After you have created a cluster and configured the required traffic distribution mechanism, the cluster is able to serve traffic. During the lifetime of the cluster, you can perform cluster tasks such as configuring nodegroups, disabling nodes of a cluster, discovering NetScaler appliances, viewing statistics, synchronizing cluster configurations, cluster files, and the time across the nodes, and upgrading or downgrading the software of cluster nodes.

Configuring Nodegroups for Datacenter Redundancy

As described in Cluster Nodegroups, a nodegroup can be used for two purposes. Here, we describe the procedure to create a nodegroup that can be used for providing datacenter redundancy. To understand the configurations for defining such a nodegroup, let us use an example of a 12 node cluster, where you define 3 nodegroups each of 3 nodes.

In this setup, one nodegroup must be defined as active and the others will be defined as spare nodegroups.

Configuring a nodegroup for datacenter redundancy by using the command line interface

1. Log on to the cluster IP address.
2. Create the active nodegroup and bind the required cluster nodes.

   To create the active nodegroup

   add cluster nodegroup ng1 -state ACTIVE

   To bind the three cluster nodes to the nodegroup

   bind cluster nodegroup ng1 -node n1

   bind cluster nodegroup ng1 -node n2

   bind cluster nodegroup ng1 -node n3
3. Create the spare nodegroup and bind the requisite nodes.

   To create the active nodegroup

   add cluster nodegroup ng2 -state SPARE -priority <integer>

   To bind the three cluster nodes to the nodegroup

   bind cluster nodegroup ng2 -node n4

   bind cluster nodegroup ng2 -node n5

   bind cluster nodegroup ng2 -node n6
4. Create another spare nodegroup and bind the requisite nodes.

   To create the active nodegroup

   add cluster nodegroup ng3 -state SPARE -priority <integer>

To bind the three cluster nodes to the nodegroup

bind cluster nodegroup ng3 -node n7

bind cluster nodegroup ng3 -node n8

bind cluster nodegroup ng3 -node n9

Disabling a Cluster Node

You can temporarily remove a node from a cluster by disabling the cluster instance on that node. A disabled node is not synchronized with the cluster configurations and is unable to serve traffic. When the node is enabled again, it is automatically synchronized with the cluster configurations. For more information, see Cluster Synchronization.

Note: If the configurations of a non-configuration coordinator node are modified (through the NSIP address of the node) after it is disabled, the configurations are not automatically synchronized on that node. You must manually synchronize the configurations as described in Synchronizing Cluster Configurations.

To disable a cluster node by using the command line interface

At the command prompt of the node that you want to disable, type:

disable cluster instance <clId>

Note: To disable the cluster, run the disable cluster instance command on the cluster IP address.

To disable a cluster node by using the configuration utility

1. Log on to the node that you want to disable.
2. Navigate to System > Cluster.
3. In the details pane, under Get Started, click Manage Cluster.
4. In the Configure cluster instance dialog box, unselect the Enable cluster instance check box.
5. Click OK.

   Note: To disable the cluster instance on all the nodes, perform the above procedure on the cluster IP address.

Parameter Descriptions (of commands listed in the CLI procedure)

disable cluster instance

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Discovering NetScaler Appliances

You can discover NetScaler appliances present in the same subnet as the NSIP address of the configuration coordinator. The discovered appliances can then be added to the cluster.

Note: This operation is available only through the configuration utility.

To discover appliances by using the configuration utility

1. Log on to the cluster IP address.
2. Navigate to System > Cluster > Nodes.
3. In the details pane, at the bottom of the page, click Discover NetScalers.
4. In the Discover NetScalers dialog box, set the following parameters:
   - IP address range - Specify the range of IP addresses within which you want to discover appliances. For example, you can search for all NSIP addresses between 10.102.29.4 to 10.102.29.15 by specifying this option as 10.102.29.4 - 15.
   - Backplane interface - Specify the interfaces to be used as the backplane interface. This is an optional parameter. If you do not specify this parameter, you must update it after the node is added to the cluster.
5. Click OK.
6. Select the appliances that you want to add to the cluster.
7. Click OK.

Viewing the Statistics of a Cluster

You can view the statistics of a cluster instance and cluster nodes to evaluate the performance or to troubleshoot the operation of the cluster.

To view the statistics of a cluster instance by using the command line interface

At the command prompt of the cluster IP address, type:

stat cluster instance <clId>

To view the statistics of a cluster node by using the command line interface

At the command prompt of the cluster IP address, type:

stat cluster node <nodeid>

Note: When executed from the cluster IP address, this command displays the cluster level statistics. However, when executed from the NSIP address of a cluster node, the command displays node level statistics.

To view the statistics of a cluster instance by using the configuration utility

1. Log on to the cluster IP address.
2. Navigate to System > Cluster.
3. In the details pane, in the center of the page, click Statistics.

To view the statistics of a cluster node by using the configuration utility

1. Log on to the cluster IP address.
2. Navigate to System > Cluster > Nodes.
3. In the details pane, select a node and click Statistics to view the statistics of the node. To view the statistics of all the nodes, click Statistics without selecting a specific node.

Parameter Descriptions (of commands listed in the CLI procedure)

stat cluster instance

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

stat cluster node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Synchronizing Cluster Configurations

NetScaler configurations that are available on the configuration coordinator are synchronized to the other nodes of the cluster when:

- A node joins the cluster
- A node rejoins the cluster
- A new command is executed through the cluster IP address.

Additionally, you can forcefully synchronize the configurations that are available on the configuration coordinator (full synchronization) to a specific cluster node. Make sure you synchronize one cluster node at a time, otherwise the cluster can get affected.

To synchronize cluster configurations by using the command line interface

At the command prompt of the appliance on which you want to synchronize the configurations, type:

force cluster sync

To synchronize cluster configurations by using the configuration utility

1. Log on to the appliance on which you want to synchronize the configurations.
2. Navigate to System > Cluster.
3. In the details pane, under Utilities, click Force cluster sync.
4. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

force cluster sync

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Synchronizing Cluster Files

The files available on the configuration coordinator are called cluster files. These files are automatically synchronized on the other cluster nodes when the node is added to the cluster and periodically, during the lifetime of the cluster. Additionally, you can manually synchronize the cluster files.

The directories and files from the configuration coordinator that are synchronized are:

- /nsconfig/ssl/
- /var/netscaler/ssl/
- /var/vpn/bookmark/
- /nsconfig/dns/
- /nsconfig/htmlinjection/
- /netscaler/htmlinjection/ens/
- /nsconfig/monitors/
- /nsconfig/nstemplates/
- /nsconfig/ssh/
- /nsconfig/rc.netscaler
- /nsconfig/resolv.conf
- /nsconfig/inetd.conf
- /nsconfig/syslog.conf
- /nsconfig/snmpd.conf
- /nsconfig/ntp.conf
- /nsconfig/httpd.conf
- /nsconfig/sshd_config
- /nsconfig/hosts
- /nsconfig/enckey
- /var/nslw.bin/etc/krb5.conf
- /var/nslw.bin/etc/krb5.keytab

- /var/lib/likewise/db/
- /var/download/
- /var/wi/tomcat/webapps/
- /var/wi/tomcat/conf/Catalina/localhost/
- /var/wi/java_home/lib/security/cacerts
- /var/wi/java_home/jre/lib/security/cacerts
- /nsconfig/license/
- /nsconfig/rc.conf

To synchronize cluster files by using the command line interface

At the command prompt of the cluster IP address, type:

sync cluster files <mode>

To synchronize cluster files by using the configuration utility

1. Log on to the cluster IP address.
2. Navigate to System > Cluster.
3. In the details pane, under Utilities, click Synchronize cluster files.
4. In the Synchronize cluster files dialog box, select the files to be synchronized in the Mode drop-down box.
5. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

sync cluster files

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Synchronizing Time on Cluster Nodes

The cluster uses Precision Time Protocol (PTP) to synchronize the time across cluster nodes. PTP uses multicast packets to synchronize the time. If there are some issues in time synchronization, you must disable PTP and configure Network Time Protocol (NTP) on the cluster.

To enable/disable PTP by using the command line interface

At the command prompt of the cluster IP address, type:

set ptp -state disable

To enable/disable PTP by using the configuration utility

1. Log on to the cluster IP address.
2. Navigate to System > Cluster.
3. In the details pane, under Utilities, click Configure PTP Settings.
4. In the Enable/Disable PTP dialog box, select whether you want to enable or disable PTP.
5. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

set ptp

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Upgrading or Downgrading the Cluster Software

All cluster nodes must be running the same software version. To upgrade or downgrade the software of a cluster, you must upgrade or downgrade the software on each node, one node at a time.

When the software on a node is upgraded or downgraded, the node is not removed from the cluster. The node continues to be a part of the cluster and serves client traffic uninterrupted, except for the down-time when the node reboots after it is upgraded or downgraded. However, due to software version mismatch among the cluster nodes, configuration propagation is disabled and is enabled only after all the cluster nodes are of the same version.

Since configuration propagation is disabled during upgrading on downgrading a cluster, you cannot perform any configurations through the cluster IP address during this time. However, you can perform node-level configurations through the NSIP address of individual nodes, but you must make sure that you perform the same configurations on all the nodes to maintain them in synch.

Note:

- You cannot add cluster nodes while upgrading or downgrading the cluster software version.
- You cannot execute the start nstrace command from the cluster IP address when the cluster is being upgraded. However, you can get the trace of individual nodes by performing this operation on individual cluster nodes through their NetScaler IP (NSIP) address.
- Configurations can be lost during the downgrade of the cluster.

To upgrade or downgrade the software of the cluster nodes

1. Make sure the cluster is stable and the configurations are synchronized on all the nodes.
2. Upgrade or downgrade the software of the cluster.
    a. Upgrade or downgrade the software of a cluster node. For detailed information about upgrading and downgrading the software of an appliance, see "Upgrading or Downgrading the System Software".
    b. Save the configurations.
    c. Reboot the appliance.
    d. Repeat the above two steps for each of the other cluster nodes.

        Note:

        - Citrix recommends that you wait for the previous node to become active before upgrading or downgrading the next node.
        - If you have configured a cluster before NetScaler 10.5 Build 52.11, the cluster will work with the separate cluster license file. No changes are required.
        - When you configure a new cluster in Build 52.11 and then downgrade, the cluster will not work as it now expects the separate cluster license file.

Use Cases

Some scenarios in which a cluster can be deployed:

- Creating a Two-Node Cluster
- Migrating an HA Setup to a Cluster Setup
- Migrating an HA Setup to a Cluster Setup without Downtime
- Setting Up GSLB in a Cluster
- Using Cache Redirection in a Cluster
- Using Cluster LA Channel with Linksets
- Backplane on LA Channel
- Common Interface for Client and Server and Dedicated Interfaces for Backplane
- Common Switch for Client, Server, and Backplane
- Common Switch for Client and Server and Dedicated Switch for Backplane
- Different Switch for Every Node
- Sample Cluster Configurations

Creating a Two-Node Cluster

A two-node cluster is an exception to the rule that a cluster is functional only when a minimum of (n/2 +1) nodes, where n is the number of cluster nodes, are able to serve traffic. If that formula were applied to a two-node cluster, the cluster would fail if one node went down (n/2 +1=2).

A two-node cluster is functional even if only one node is able to serve traffic.

Creating a two node cluster is the same as creating any other cluster. You must add one node as the configuration coordinator and the other node as the other cluster node.

Note: Incremental configuration synchronization is not supported in a two-node cluster. Only full synchronization is supported.

Migrating an HA Setup to a Cluster Setup

An existing high availability (HA) setup can be migrated to a cluster setup by first removing the appliances from the HA setup and then creating the NetScaler cluster. This approach will result in a downtime for the application.

Consider an HA setup with appliances NS0 (10.102.97.131) and NS1 (10.102.97.132). NS0 is the primary and NS1 is the secondary appliance of the HA setup.

To convert a HA setup to cluster setup by using the NetScaler command line

1. Log on to each HA node and remove it from the HA setup.

   rm HA node <id>

   Example

   rm HA node 1

2. Go to the shell on one of the HA nodes and copy the ns.conf file to another .conf file (for example, ns_backup.conf).

3. On both the nodes, identify the network interfaces to be used for the cluster backplane. Make sure to configure the backplane switch appropriately.

4. Create the cluster on one of the appliances (for example, 10.102.97.131).

   ```
   //On the NSIP address of the first appliance
   add cluster instance 1
   add cluster node 0 10.102.97.131 -state ACTIVE -backplane 0/1/1
   add ns ip 10.102.97.133 255.255.255.255 -type CLIP
   enable cluster instance 1
   save ns config
   reboot -warm
   ```

5. Add the other appliance to the cluster.

   ```
   //On the cluster IP address
   add cluster node 1 10.102.97.132 -state ACTIVE -backplane 1/1/1

   //On the NSIP address of the appliance
   join cluster -clip 10.102.97.133 -password nsroot
   save ns config
   reboot -warm
   ```

6. After the two nodes are up and active, log on to the cluster IP address and modify the backed-up configuration file as follows:

   a. Remove the features that are not supported on a cluster. For the list of unsupported features, see NetScaler Features Supported by a Cluster. This is an optional step. If you do not perform this step, the execution of unsupported commands will fail.

   b. Remove the configurations that have interfaces, or update the interface names from the c/u convention to the n/c/u convention.

      Example

      add vlan 10 -ifnum 0/1

      should be changed to

add vlan 10 -ifnum 0/0/1 1/0/1

c. The backup configuration file can have SNIP addresses or MIP addresses. These addresses are striped on all the cluster nodes. It is recommended that you add spotted IP addresses for each node.

Example

```
add ns ip 1.1.1.1 255.255.255.0 -ownerNode 0
add ns ip 1.1.1.2 255.255.255.0 -ownerNode 1
```

d. Update the hostname to specify the owner node.

Example

```
set ns hostname ns0 -ownerNode 0
set ns hostname ns1 -ownerNode 1
```

e. Change all other relevant networking configuration that depend on spotted IPs. For example, L3 VLAN, RNAT configuration which uses SNIPs as NATIP, INAT rules that refers to SNIPs/MIPs).

7. Apply configurations from the backup configuration file to the configuration coordinator through the cluster IP address.

   batch -fileName <input_filename>

   Example

   batch -f ns_backup.conf

8. Configure appropriate client traffic distribution mechanism (ECMP, cluster LA or linksets).

9. Save the configuration.

   save ns config

The appliances of the HA setup are migrated to a cluster setup.

Parameter Descriptions (of commands listed in the CLI procedure)

rm HA node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

batch

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

save ns config

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Migrating an HA Setup to a Cluster Setup without Downtime

An existing high availability (HA) setup can be migrated to a cluster setup by first removing the secondary appliance from the HA setup and using that appliance to create a single-node cluster. Then, after the cluster becomes operational and serves traffic, the primary appliance of the HA setup is added to the cluster. This approach will not result in a downtime for the application.

Consider an HA setup with appliances NS0 (10.102.97.131) and NS1 (10.102.97.132). NS0 is the primary and NS1 is the secondary appliance of the HA setup.

To convert a HA setup to cluster setup (without downtime) by using the NetScaler command line

1. Go to the shell on one of the HA nodes and copy the ns.conf file to another .conf file (for example, ns_backup.conf).

   Note: Make sure HA pair is stable with respect to configurations.

2. Log on to the secondary appliance NS1 and clear all the configurations. This removes the secondary appliance from the HA setup and makes it a standalone appliance.

   clear ns config full

   Note:

   - The configurations are cleared to make sure that NS1 does not start owning the VIPs once it becomes a standalone appliance.

   - At this stage, NS0 is still active and continues to serve traffic.

3. Create a cluster on appliance NS1 and configure it as a PASSIVE node.

   ```
   //On the NSIP address of node NS1
   add cluster instance 1
   add cluster node 0 10.102.97.131 -state PASSIVE -backplane 0/1/1
   add ns ip 10.102.97.133 255.255.255.255 -type CLIP
   enable cluster instance 1
   save ns config
   reboot -warm
   ```

4. Modify the backed-up configuration file.

   a. Remove the features that are not supported on a cluster. For the list of unsupported features, see NetScaler Features Supported by a Cluster. This is an optional step. If you do not perform this step, the execution of unsupported commands will fail.

   b. Remove the configurations that have interfaces, or update the interface names from the c/u convention to the n/c/u convention.

      Example

      add vlan 10 -ifnum 0/1

      should be changed to

      add vlan 10 -ifnum 0/0/1 1/0/1

   c. The backup configuration file can have SNIP addresses or MIP addresses. These addresses are striped on all the cluster nodes. It is recommended that you add spotted IP addresses for each node.

      Example

```
add ns ip 1.1.1.1 255.255.255.0 -ownerNode 0
add ns ip 1.1.1.2 255.255.255.0 -ownerNode 1
```

d. Update the hostname to specify the owner node.

Example

```
set ns hostname ns0 -ownerNode 0
set ns hostname ns1 -ownerNode 1
```

e. Change all other relevant networking configuration that depend on spotted IPs. For example, L3 VLAN, RNAT configuration which uses SNIPs as NATIP, INAT rules that refers to SNIPs/MIPs).

5. On the cluster, do the following:

a. Make the topological changes to the cluster by connecting the cluster backplane, the cluster link aggregation channel, and so on.

b. Apply configurations from the backup configuration file to the configuration coordinator through the cluster IP address.

```
batch -f ns_backup.conf
```

c. Configure external traffic distribution mechanisms like ECMP or cluster link aggregation.

6. Switch-over the traffic from the HA setup to the single-node cluster setup.

a. Disable all interfaces on the primary appliance NS0.

```
disable interface <interface id>
```

b. Configure the cluster node as an ACTIVE node.

```
set cluster node 0 -state ACTIVE
```

Note: There can be a small amount (in the order of seconds) of downtime between disabling the interfaces and making the cluster node active.

7. On the primary appliance NS0, do the following:

a. Clear all the configurations.

```
clear ns config full
```

b. Enable all the interfaces.

```
enable interface <interface id>
```

c. Add the appliance to the cluster.

```
//On the cluster IP address (in this sample, 10.102.97.133)
add cluster node 1 10.102.97.132 -state PASSIVE -backplane 1/1/1
```

```
//On the NSIP address of the appliance
join cluster -clip 10.102.97.133 -password nsroot
save ns config
reboot -warm
```

d. Perform the required topological and configuration changes.

e. Configure NS0 as an ACTIVE node.

```
set cluster node 1 -state ACTIVE
```

The appliances of the HA setup are migrated to a cluster setup without any downtime for the application.

Setting Up GSLB in a Cluster

Note: Supported from NetScaler 10.5 Build 52.11 onwards.

To set up GSLB in a cluster you must bind the different GSLB entities to a node group. The node group must have a single member node.

Note:

- The parent-child topology of GSLB is not supported in a cluster.
- If you have configured the static proximity GSLB method, make sure that the static proximity database is present on all the cluster nodes. This happens by default if the database file is available at the default location. However, if the database file is maintained in a directory other than /var/netscaler/locdb/, you must manually synch the file to all the cluster nodes.

To set up GSLB in a cluster by using the command line interface

Log on to the cluster IP address and perform the following operations at the command prompt:

1. Configure the different GSLB entities. For information, see Configuring Global Server Load Balancing.

   Note: When creating the GSLB site, make sure that you specify the cluster IP address and public cluster IP address (needed only when the cluster is deployed behind a NAT device). These parameters are required to ensure the availability of the GSLB auto-sync functionality.

   add gslb site <siteName> <siteType> <siteIPAddress> -publicIP <ip_addr> -clip <ip_addr> <publicCLIP>

2. Create a cluster node group.

   add cluster nodegroup <name> [-sticky (YES | NO)]

   Note: Enable the sticky option if you want to set up GSLB based on VPN users.

3. Bind a single cluster node to the node group.

   bind cluster nodegroup <name> -node <nodeId>

4. Bind the local GSLB site to the nodegroup.

   bind cluster nodegroup <name> -gslbSite <string>

   Note: Make sure that the IP address of the local GSLB site IP address is striped (available across all cluster nodes).

5. Bind the ADNS (or ADNS-TCP) service or the DNS (or DNS-TCP) load balancing virtual server to the node group.

   To bind the ADNS service:

   bind cluster nodegroup <name> -service <string>

   To bind the DNS load balancing virtual server:

   bind cluster nodegroup <name> -vServer <string>

6. Bind the GSLB virtual server to the node group.

   bind cluster nodegroup <name> -vServer <string>

7. [Optional] To setup GSLB based on VPN users, bind the VPN virtual vserver to the GSLB node group.

   bind cluster nodegroup <name> -vServer <string>

8. Verify the configurations.

   show gslb runningConfig

To set up GSLB in a cluster by using the graphical user interface

Log on to the cluster IP address and perform the following operations in the Configuration tab:

1. Configure the GSLB entities.

   Navigate to Traffic Management > GSLB to perform the required configurations.

2. Create a node group and perform other node group related configurations.

   Navigate to System > Cluster > Node Groups to perform the required configurations.

For the detailed configurations to be performed, see the description provided in the CLI procedure mentioned above.

Parameter Descriptions (of commands listed in the CLI procedure)

add gslb site

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show gslb runningConfig

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Using Cache Redirection in a Cluster

Cache redirection in a cluster works in the same way as it does on a standalone NetScaler appliance. The only difference is that the configurations are done on the cluster IP address. For more information on cache redirection, see "Cache Redirection."

Points to remember when using cache redirection in transparent mode on a cluster:

- Before configuring cache redirection, make sure that you have connected all nodes to the external switch and that you have linksets configured. Otherwise, client requests will be dropped.
- When MAC mode is enabled on a load balancing virtual server, make sure MBF mode is enabled on the cluster by using the enable ns mode `MBF` command. Otherwise, the requests are sent to origin server directly instead of being sent to the cache server.

Using L2 Mode in a Cluster Setup

Note: Supported from NetScaler 10.5 and later releases.

To use L2 mode in a cluster setup, you must make sure of the following:

- Spotted IP addresses must be available on all the nodes as required.
- Linksets must be used to communicate with the external network.
- Asymmetric topologies or asymmetric cluster LA groups are not supported.
- Cluster LA group is recommended.
- Traffic is distributed between the cluster nodes only for deployments where services exist.

Using Cluster LA Channel with Linksets

In an asymmetric cluster topology, some cluster nodes are not connected to the upstream network. In such a case, you must use linksets. To optimize the performance, you can bind the interfaces that are connected to the switch as a cluster LA channel and then bind the channel to a linkset.

To understand how a combination of cluster LA channel and linksets can be used, consider a three-node cluster for which the upstream switch has only two ports available. You can connect two of the cluster nodes to the switch and leave the other node unconnected.

Note: Similarly, you can also use a combination of ECMP and linksets in an asymmetric topology.

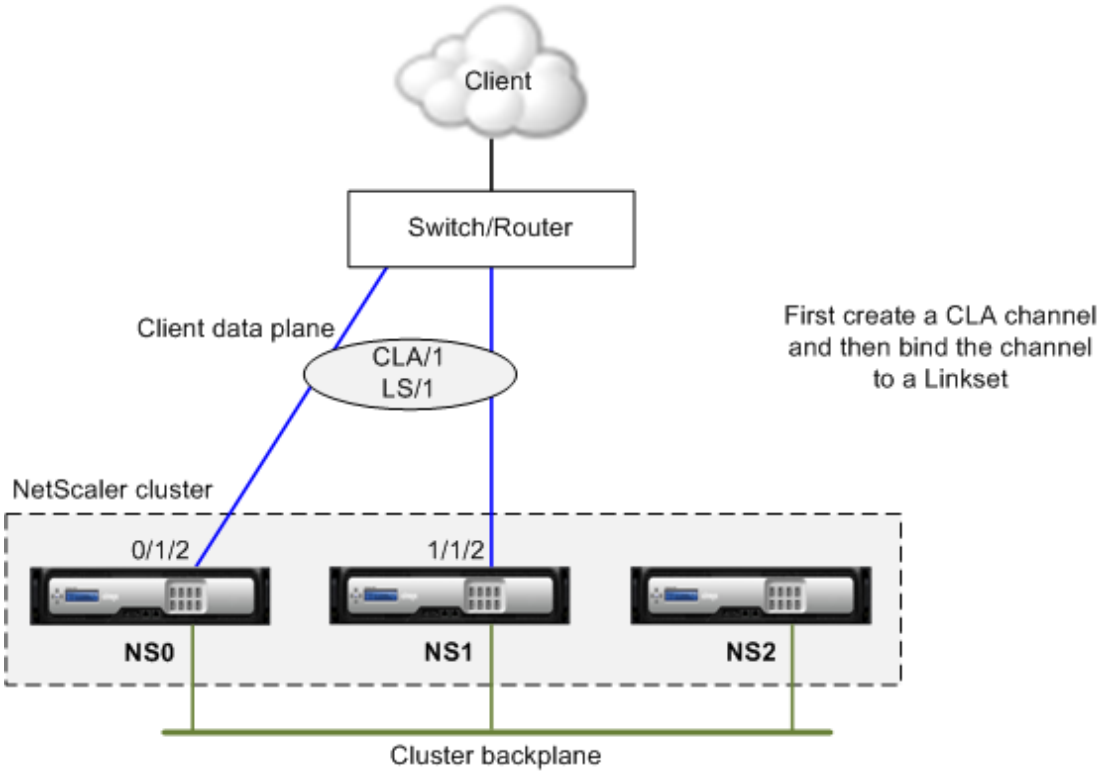


Figure 1. Linksets and cluster LA channel topology

To configure cluster LA channel and linksets by using the NetScaler command line

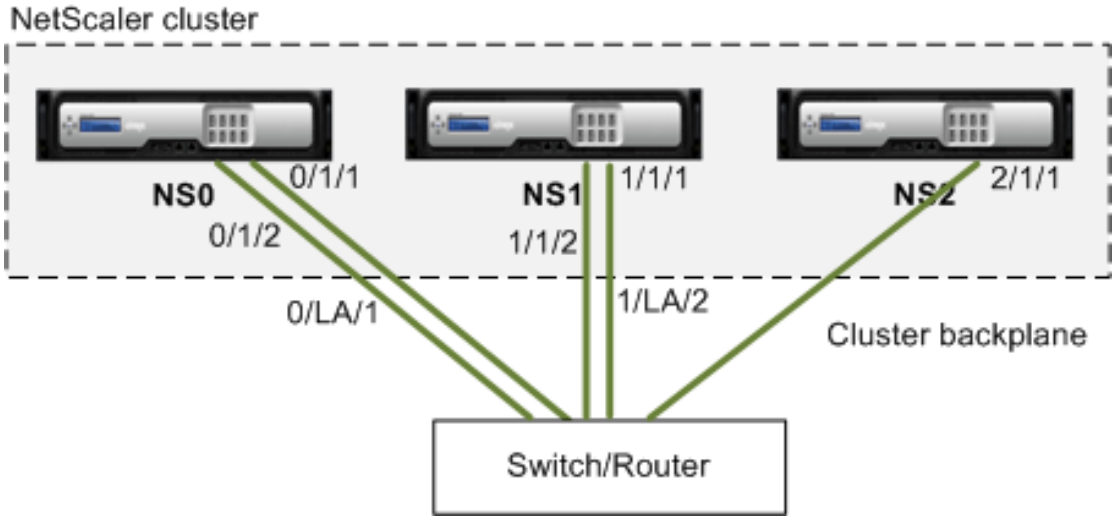
1. Log on to the cluster IP address.
2. Bind the connected interfaces to a cluster LA channel.

   add channel CLA/1 –ifnum 0/1/2 1/1/2
3. Bind the cluster LA channel to the linkset.

   add linkset LS/1 -ifnum CLA/1

Backplane on LA Channel

In this deployment, LA channels are used for the cluster backplane.



NS0 - nodeId: 0, NSIP: 10.102.29.60

NS1 - nodeId: 1, NSIP: 10.102.29.70

NS2 - nodeId: 2, NSIP: 10.102.29.80

To deploy a cluster with the backplane interfaces as LA channels

1. Create a cluster of nodes NS0, NS1, and NS2.

    a. Log on to the first node that you want to add to the cluster and do the following:

    ```
    create cluster instance 1
    add cluster node 0 10.102.29.60 -state ACTIVE
    enable cluster instance 1
    add ns ip 10.102.29.61 255.255.255.255 -type CLIP
    save ns config
    reboot -warm
    ```

    b. Log on to the cluster IP address and do the following:

    ```
    add cluster node 1 10.102.29.70 -state ACTIVE
    add cluster node 2 10.102.29.80 -state ACTIVE
    ```

    c. Log on to the nodes 10.102.29.70 and 10.102.29.80 to join the nodes to the cluster.

    ```
    join cluster -clip 10.102.29.61 -password nsroot
    save ns config
    reboot -warm
    ```

As seen in the above commands the interfaces 0/1/1, 1/1/1, and 2/1/1 are configured as the backplane interfaces of the three cluster nodes.

2. Log on to the cluster IP address and do the following:

   a. Create the LA channels for nodes NS0 and NS1.

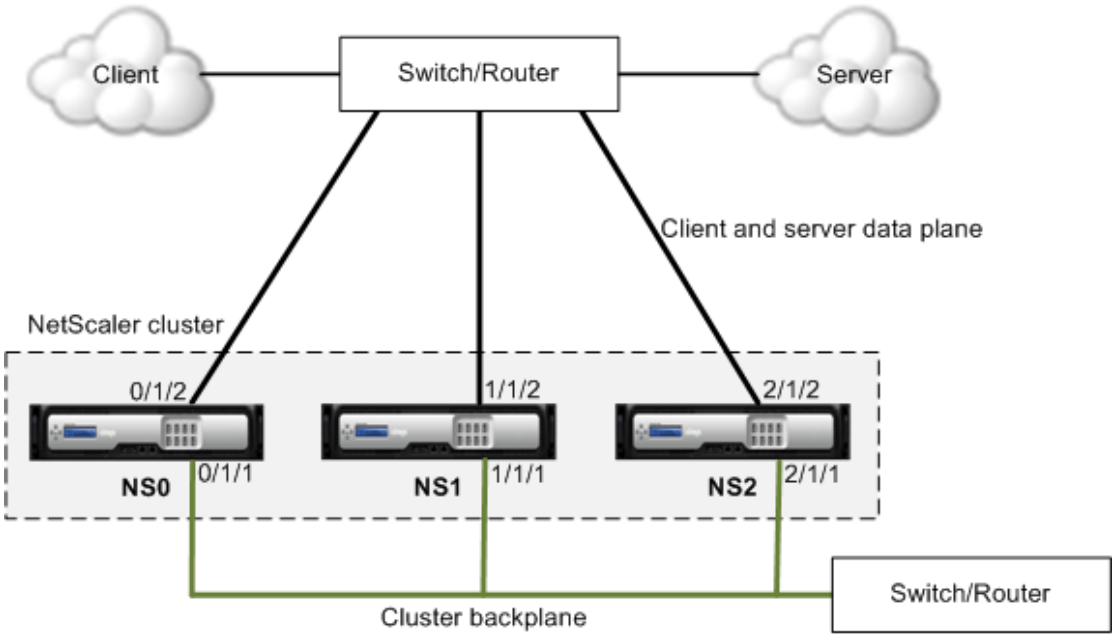
      ```
      add channel 0/LA/1 -ifnum 0/1/1 0/1/2
      add channel 1/LA/2 -ifnum 1/1/1 1/1/2
      ```

   b. Configure the backplane for the cluster nodes.

      ```
      set cluster node 0 -backplane 0/LA/1
      set cluster node 1 -backplane 1/LA/2
      set cluster node 2 -backplane 2/1/1
      ```

Common Interfaces for Client and Server and Dedicated Interfaces for Backplane

This is a one-arm deployment of the NetScaler cluster. In this deployment, the client and server networks use the same interfaces to communicate with the cluster. The cluster backplane uses dedicated interfaces for inter-node communication.



NS0 - nodeId: 0, NSIP: 10.102.29.60

NS1 - nodeId: 1, NSIP: 10.102.29.70

NS2 - nodeId: 2, NSIP: 10.102.29.80

To deploy a cluster with a common interface for the client and server and a different interface for the cluster backplane

1. Create a cluster of nodes NS0, NS1, and NS2.

    a. Log on to the first node that you want to add to the cluster and do the following:

```
create cluster instance 1
add cluster node 0 10.102.29.60 -state ACTIVE -backplane 0/1/1
enable cluster instance 1
add ns ip 10.102.29.61 255.255.255.255 -type CLIP
save ns config
```

```
reboot -warm
```

b. Log on to the cluster IP address and do the following:

```
add cluster node 1 10.102.29.70 -state ACTIVE -backplane 1/1/1
add cluster node 2 10.102.29.80 -state ACTIVE -backplane 2/1/1
```

c. Log on to the nodes 10.102.29.70 and 10.102.29.80 to join the nodes to the cluster.

```
join cluster -clip 10.102.29.61 -password nsroot
save ns config
reboot -warm
```

As seen in the above commands the interfaces 0/1/1, 1/1/1, and 2/1/1 are configured as the backplane interfaces of the three cluster nodes.

2. On the cluster IP address, create VLANs for the backplane interfaces and for the client and server interfaces.

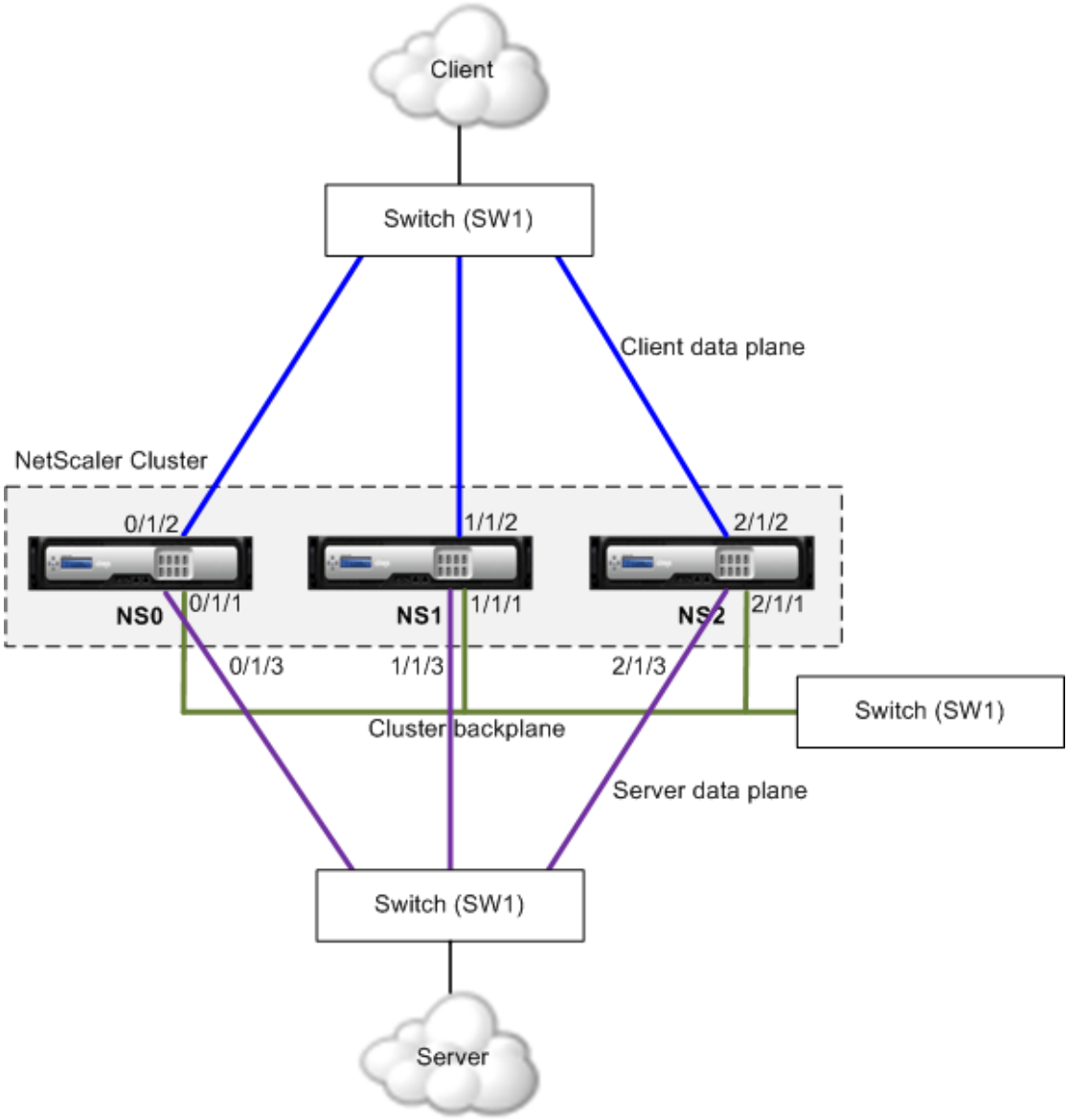
```
//For the backplane interfaces
add vlan 10
bind vlan 10 0/1/1 1/1/1 2/1/1

//For the interfaces that are connected to the client and server networks.
add vlan 20
bind vlan 20 0/1/2 1/1/2 2/1/2
```

3. On the switch, create VLANs for the interfaces corresponding to the backplane interfaces and the client and server interfaces. The following sample configurations are provided for the Cisco® Nexus 7000 C7010 Release 5.2(1) switch. Similar configurations must be performed on other switches.

```
//For the backplane interfaces. Repeat for each interface...
interface Ethernet2/47
switchport access vlan 100
switchport mode access
end

//For the interfaces connected to the client and server networks. Repeat for each interface...
interface Ethernet2/47
switchport access vlan 200
switchport mode access
end
```

Common Switch for Client, Server, and Backplane

In this deployment, the client, server, and backplane use dedicated interfaces on the same switch to communicate with the NetScaler cluster.



NS0 - nodeId: 0, NSIP: 10.102.29.60

NS1 - nodeId: 1, NSIP: 10.102.29.70

NS2 - nodeId: 2, NSIP: 10.102.29.80

To deploy a cluster with a common switch for the client, server, and backplane

1. Create a cluster of nodes NS0, NS1, and NS2.

   a. Log on to the first node that you want to add to the cluster and do the following:

      ```
      create cluster instance 1
      add cluster node 0 10.102.29.60 -state ACTIVE -backplane 0/1/1
      enable cluster instance 1
      add ns ip 10.102.29.61 255.255.255.255 -type CLIP
      save ns config
      reboot -warm
      ```

   b. Log on to the cluster IP address and do the following:

      ```
      add cluster node 1 10.102.29.70 -state ACTIVE -backplane 1/1/1
      add cluster node 2 10.102.29.80 -state ACTIVE -backplane 2/1/1
      ```

   c. Log on to the nodes 10.102.29.70 and 10.102.29.80 to join the nodes to the cluster.

      ```
      join cluster -clip 10.102.29.61 -password nsroot
      save ns config
      reboot -warm
      ```

   As seen in the above commands the interfaces 0/1/1, 1/1/1, and 2/1/1 are configured as the backplane interfaces of the three cluster nodes.

2. On the cluster IP address, create VLANs for the backplane, client, and server interfaces.

   ```
   //For the backplane interfaces
   add vlan 10
   bind vlan 10 0/1/1 1/1/1 2/1/1

   //For the client-side interfaces
   add vlan 20
   bind vlan 20 0/1/2 1/1/2 2/1/2

   //For the server-side interfaces
   add vlan 30
   bind vlan 30 0/1/3 1/1/3 2/1/3
   ```

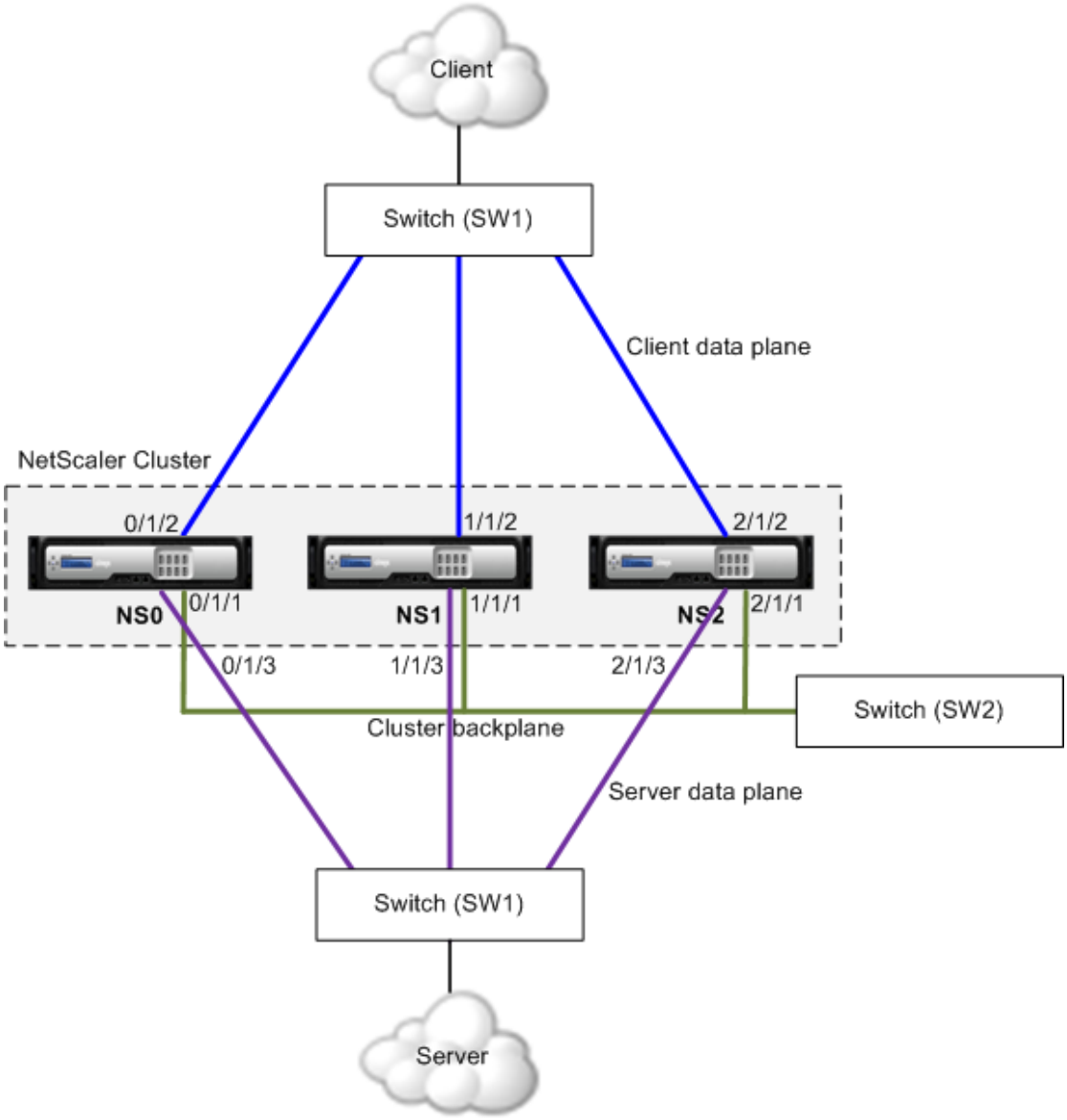
3. On the switch, create VLANs for the interfaces corresponding to the backplane interfaces and the client and server interfaces. The following sample configurations are provided for the Cisco® Nexus 7000 C7010 Release 5.2(1) switch. Similar configurations must be performed on other switches.

   ```
   //For the backplane interfaces. Repeat for each interface...
   interface Ethernet2/47
   switchport access vlan 100
   switchport mode access
   end
   ```

```
//For the client interfaces. Repeat for each interface...
interface Ethernet2/48
switchport access vlan 200
switchport mode access
end

//For the server interfaces. Repeat for each interface...
interface Ethernet2/49
switchport access vlan 300
switchport mode access
end
```

Common Switch for Client and Server and Dedicated Switch for Backplane

In this deployment, the clients and servers use different interfaces on the same switch to communicate with the NetScaler cluster. The cluster backplane uses a dedicated switch for inter-node communication.



NS0 - nodeId: 0, NSIP: 10.102.29.60

NS1 - nodeId: 1, NSIP: 10.102.29.70

NS2 - nodeId: 2, NSIP: 10.102.29.80

To deploy a cluster with the same switch for the clients and servers and a different switch for the cluster backplane

1. Create a cluster of nodes NS0, NS1, and NS2.

   a. Log on to the first node that you want to add to the cluster and do the following:

      ```
      create cluster instance 1
      add cluster node 0 10.102.29.60 -state ACTIVE -backplane 0/1/1
      enable cluster instance 1
      add ns ip 10.102.29.61 255.255.255.255 -type CLIP
      save ns config
      reboot -warm
      ```

   b. Log on to the cluster IP address and do the following:

      ```
      add cluster node 1 10.102.29.70 -state ACTIVE -backplane 1/1/1
      add cluster node 2 10.102.29.80 -state ACTIVE -backplane 2/1/1
      ```

   c. Log on to the nodes 10.102.29.70 and 10.102.29.80 to join the nodes to the cluster.

      ```
      join cluster -clip 10.102.29.61 -password nsroot
      save ns config
      reboot -warm
      ```

   As seen in the above commands the interfaces 0/1/1, 1/1/1, and 2/1/1 are configured as the backplane interfaces of the three cluster nodes.

2. On the cluster IP address, create VLANs for the backplane, client, and server interfaces.

   ```
   //For the backplane interfaces
   add vlan 10
   bind vlan 10 0/1/1 1/1/1 2/1/1

   //For the client-side interfaces
   add vlan 20
   bind vlan 20 0/1/2 1/1/2 2/1/2

   //For the server-side interfaces
   add vlan 30
   bind vlan 30 0/1/3 1/1/3 2/1/3
   ```

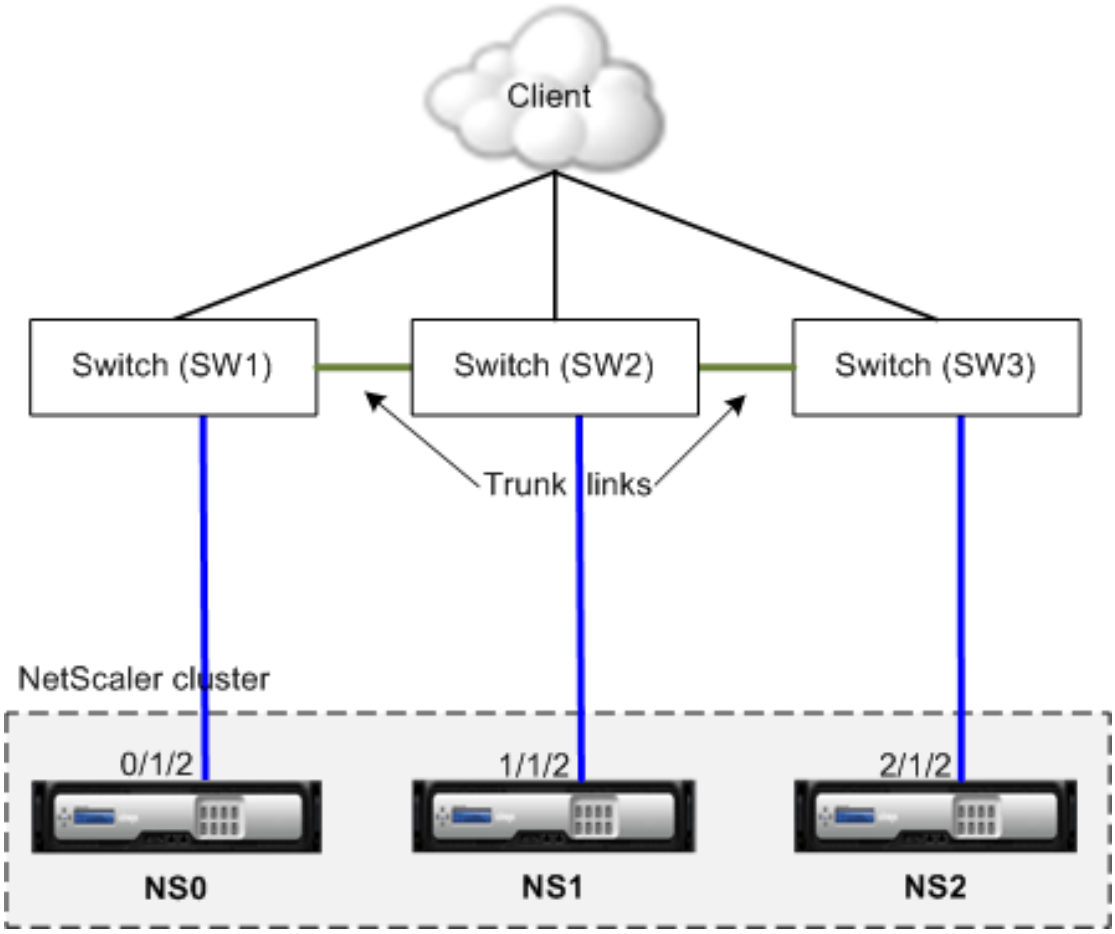
3. On the switch, create VLANs for the interfaces corresponding to the backplane interfaces and the client and server interfaces. The following sample configurations are provided for the Cisco® Nexus 7000 C7010 Release 5.2(1) switch. Similar configurations must be performed on other switches.

   ```
   //For the backplane interfaces. Repeat for each interface...
   interface Ethernet2/47
   switchport access vlan 100
   switchport mode access
   ```

```
end

//For the client interfaces. Repeat for each interface...
interface Ethernet2/48
switchport access vlan 200
switchport mode access
end

//For the server interfaces. Repeat for each interface...
interface Ethernet2/49
switchport access vlan 300
switchport mode access
end
```

Different Switch for Every Node

In this deployment, each cluster node is connected to a different switch and trunk links are configured between the switches.



The cluster configurations will be the same as the other deployments scenarios. Most of the client-side configurations will be done on the client-side switches.

Sample Cluster Configurations

The following example can be used to configure a four-node cluster with ECMP, cluster LA, or Linksets.

1. Create the cluster.
    a. Log on to first node.
    b. Add the cluster instance.

        add cluster instance 1

    c. Add the first node to the cluster.

        add cluster node 0 10.102.33.184 -backplane 0/1/1

    d. Enable the cluster instance.

        enable cluster instance 1

    e. Add the cluster IP address.

        add ns ip 10.102.33.185 255.255.255.255 -type CLIP

    f. Save the configurations.

        save ns config

    g. Warm reboot the appliance.

        reboot -warm
2. Add the other three nodes to the cluster.
    a. Log on to cluster IP address.
    b. Add the second node to the cluster.

        add cluster node 1 10.102.33.187 -backplane 1/1/1

    c. Add the third node to the cluster.

        add cluster node 2 10.102.33.188 -backplane 2/1/1

    d. Add the fourth node to the cluster.

        add cluster node 3 10.102.33.189 -backplane 3/1/1
3. Join the added nodes to the cluster. This step is not applicable for the first node.
    a. Log on to each newly added node.

b. Join the node to the cluster.

```
join cluster -clip 10.102.33.185 -password nsroot
```

c. Save the configuration.

```
save ns config
```

d. Warm reboot the appliance.

```
reboot -warm
```

4. Configure the NetScaler cluster through the cluster IP address.

```
// Enable load balancing feature
enable ns feature lb

// Add a load balancing virtual server
add lb vserver first_lbvserver http
....
....
```

5. Configure any one of the following (ECMP, cluster LA, or Linkset) traffic distribution mechanisms for the cluster.

- **ECMP**

a. Log on to the cluster IP address.

b. Enable the OSPF routing protocol.

```
enable ns feature ospf
```

c. Add a VLAN.

```
add vlan 97
```

d. Bind the interfaces of the cluster nodes to the VLAN.

```
bind vlan 97 -ifnum 0/1/4 1/1/4 2/1/4 3/1/4
```

e. Add a spotted SNIP on each node and enable dynamic routing on it.

```
add ns ip 1.1.1.10 255.255.255.0 -ownerNode 0 -dynamicRouting ENABLED
add ns ip 1.1.1.11 255.255.255.0 -ownerNode 1 -dynamicRouting ENABLED
add ns ip 1.1.1.12 255.255.255.0 -ownerNode 2 -dynamicRouting ENABLED
add ns ip 1.1.1.13 255.255.255.0 -ownerNode 3 -dynamicRouting ENABLED
```

f. Bind one of the SNIP addresses to the VLAN.

```
bind vlan 97 -ipAddress 1.1.1.10 255.255.255.0
```

g. Configure the routing protocol on ZebOS by using vtysh shell.

- **Static cluster LA**

a. Log on to the cluster IP address.

b. Add a cluster LA channel.

```
add channel CLA/1 -speed 1000
```

c. Bind the interfaces to the cluster LA channel.

```
bind channel CLA/1 0/1/5 1/1/5 2/1/5 3/1/5
```

d. Perform equivalent configuration on the switch.

- **Dynamic cluster LA**

a. Log on to the cluster IP address.

b. Add the interfaces to the cluster LA channel.

```
set interface 0/1/5 -lacpmode active -lacpkey 5 -lagtype cluster
set interface 1/1/5 -lacpmode active -lacpkey 5 -lagtype cluster
set interface 2/1/5 -lacpmode active -lacpkey 5 -lagtype cluster
set interface 3/1/5 -lacpmode active -lacpkey 5 -lagtype cluster
```

c. Perform equivalent configuration on the switch.

- **Linksets.** Assume that the node with nodeId 3 is not connected to the switch. You must configure a linkset so that the unconnected node can use the other node interfaces to communicate with the switch.

a. Log on to the cluster IP address.

b. Add a linkset.

```
add linkset LS/1
```

c. Bind the connected interfaces to the linkset.

```
bind linkset LS/1 -ifnum 0/1/6 1/1/6 2/1/6
```

6. Update the state of the cluster nodes to ACTIVE.

```
set cluster node 0 -state ACTIVE
set cluster node 1 -state ACTIVE
set cluster node 2 -state ACTIVE
set cluster node 3 -state ACTIVE
```

Troubleshooting the NetScaler Cluster

If a failure occurs in a NetScaler cluster, the first step in troubleshooting is to get information on the cluster instance and the cluster nodes by running the `show cluster instance <clId>` and `show cluster node <nodeId>` commands respectively.

If you are not able to find the issue by using the above two approaches, you can use one of the following:

- **Isolate the source of the failure.** Try bypassing the cluster to reach the server. If the attempt is successful, the problem is probably with the cluster setup.
- **Check the commands recently executed.** Run the history command to check the recent configurations performed on the cluster. You can also review the ns.conf file to verify the configurations that have been implemented.
- **Check the ns.log files.** Use the log files, available in the /var/log/ directory of each node, to identify the commands executed, status of commands, and the state changes.
- **Check the newnslog files.** Use the newnslog files, available in the /var/nslog/ directory of each node, to identify the events that have occurred on the cluster nodes. You can view multiple newnslog files as a single file, by copying the files to a single directory, and then running the following command:

  nsconmsg -K newnslog-node<id> -K newnslog.node<id> -d current

If you still cannot resolve the issue, you can try tracing the packets on the cluster or use the `show techsupport -scope cluster` command to send the report to the technical support team.

Parameter Descriptions (of commands listed in the CLI procedure)

show cluster instance

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show cluster node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show techsupport

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Tracing the Packets of a NetScaler Cluster

The NetScaler operating system provides a utility called *nstrace* to get a dump of the packets that are received and sent out by an appliance. The utility stores the packets in trace files. You can use these files to debug problems in the flow of packets to the cluster nodes. The trace files must be viewed with the *Wireshark* application. For traces collected in native (.cap) mode, it is important to use the internal version of Wireshark, which can understand native packets.

Some salient aspects of the nstrace utility are:

- Can be configured to trace packets selectively by using classic expressions and default expressions.
- Can capture the trace in multiple formats: nstrace format (.cap) and TCP dump format (.pcap).
- Can aggregate the trace files of all cluster nodes on the configuration coordinator.
- Can merge multiple trace files into a single trace file (only for .cap files).

You can use the nstrace utility from the NetScaler command line or the NetScaler shell.

To trace packets of a standalone appliance

Run the start nstrace command on the appliance. The command creates trace files in the /var/nstrace/<date-timestamp> directory. The trace file names are of the form nstrace<id>.cap.

You can view the status by executing the show nstrace command. You can stop tracing the packets by executing the stop nstrace command.

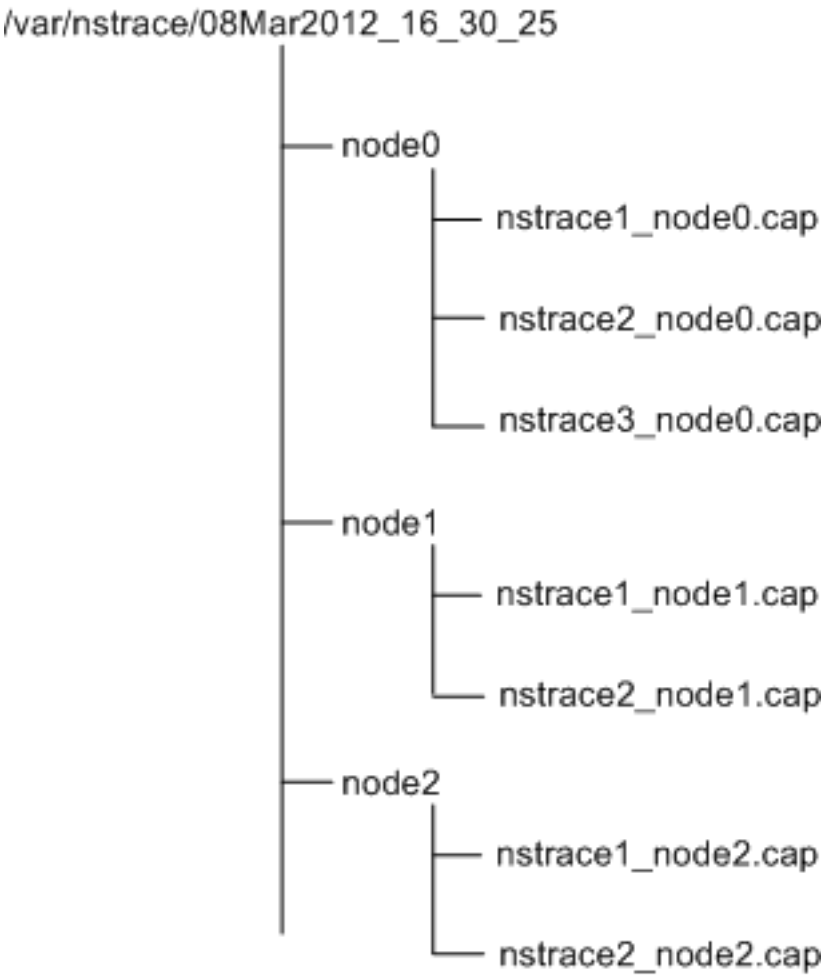
Note: You can also run the nstrace utility from the NetScaler shell by executing the nstrace.sh file. However, it is recommended that you use the nstrace utility through the NetScaler command line interface.

To trace packets of a cluster

You can trace the packets on all the cluster nodes and obtain all the trace files on the configuration coordinator.

Run the start nstrace command on the cluster IP address. The command is propagated and executed on all the cluster nodes. The trace files are stored in individual cluster nodes in the /var/nstrace/<date-timestamp> directory. The trace file names are of the form nstrace<id>_node<id>.cap.

You can use the trace files of each node to debug the nodes operations. But if you want the trace files of all cluster nodes in one location, you must run the stop nstrace command on the cluster IP address. The trace files of all the nodes are downloaded on the cluster configuration coordinator in the /var/nstrace/<date-timestamp> directory as follows:



Merge multiple trace files

You can prepare a single file from the trace files (supported only for .cap files) obtained from the cluster nodes. The single trace files gives you a cumulative view of the trace of the cluster packets. The trace entries in the single trace file are sorted based on the time the packets were received on the cluster.

To merge the trace files, at the NetScaler shell, type:

`nstracemerge.sh` -srcdir <DIR> -dstdir <DIR> -filename <name> -filesize <num>

where,

- srcdir is the directory from which the trace files are merged. All trace files within this directory are merged into a single file.
- dstdir is the directory where the merged trace file are created.

- filename is the name of the trace file that is created.
- filesize is the size of the trace file.

Examples

Following are some examples of using the nstrace utility to filter packets.

- To trace the packets on the backplane interfaces of three nodes:

  Using classic expressions:

  start nstrace -filter "INTF == 0/1/1 && INTF == 1/1/1 && INTF == 2/1/1"

  Using default expressions:

  start nstrace -filter "CONNECTION.INTF.EQ("0/1/1") && CONNECTION.INTF.EQ("1/1/1") && CONNECTION.

- To trace the packets from a source IP address 10.102.34.201 or from a system whose source port is greater than 80 and the service name is not "s1":

  Using classic expressions

  start nstrace -filter "SOURCEIP == 10.102.34.201 || (SVCNAME != s1 && SOURCEPORT > 80)"

  Using default expressions

  start nstrace -filter "CONNECTION.SRCIP.EQ(10.102.34.201) || (CONNECTION.SVCNAME.NE("s1") && CONN

Troubleshooting Common Issues

While joining a node to the cluster, I get the following message, "ERROR: Invalid interface name/number." What must I do to resolve this error?

This error occurs if you provided an invalid or incorrect backplane interface while using the add cluster node command to add the node. To resolve this error, verify the interface you provided while adding the node. Make sure that you have not specified the appliance's management interface as the backplane interface, and that the <nodeId> bit of the interface is the same as the node's Id. For example, if the nodeId is 3, the backplane interface must be 3/<c>/<u>.

While joining a node to the cluster, I get the following message, "ERROR: Clustering cannot be enabled, because the local node is not a member of the cluster." What must I do to resolve this error?

This error occurs when you try to join a node without adding the node's NSIP to the cluster. To resolve this error, you must first add the node's NSIP address to the cluster by using the add cluster node command and then execute the join cluster command.

While joining a node to the cluster, I get the following message, "ERROR: Connection refused." What must I do to resolve this error?

This error can occur due to the following reasons:

- **Connectivity problems.** The node cannot connect to the cluster IP address. Try pinging the cluster IP address from the node that you are trying to join.
- **Duplicate cluster IP address.** Check to see if the cluster IP address exists on some non-cluster node. If it does, create a new cluster IP address and try re-joining the cluster.

While joining a node to the cluster, I get the following message, "ERROR: License mismatch between the configuration coordinator and the local node." What must I do to resolve this error?

The appliance that you are joining to the cluster must have the same licenses as the configuration coordinator. This error occurs when the licenses on the node you are joining do not match the licenses on the configuration coordinator. To resolve this error, run the following commands on both the nodes and compare the outputs.

From the command line:

- show ns hardware
- show ns license

From the shell:

- nsconmsg -g feature -d stats
- ls /nsconfig/license

- View the contents of the /var/log/license.log file

What must I do when the configurations of a cluster node are not in synch with the cluster configurations?

In most cases, the configurations are automatically synchronized between all the cluster nodes. However, if you feel that the configurations are not synchronized on a specific node, you must force the synchronization by executing the force cluster sync command from the node that you want to synchronize. For more information, see " Synchronizing Cluster Configurations".

When configuring a cluster node, I get the following message, "ERROR: Session is read-only; connect to the cluster IP address to modify the configuration."

All configurations on a cluster must be done through the cluster IP address and the configurations are propagated to the other cluster nodes. All sessions established through the NetScaler IP (NSIP) address of individual nodes are read-only.

Why does the node state show "INACTIVE" when the node health shows "UP"?

A healthy node can be in the INACTIVE state for a number of reasons. A scan of ns.log or error counters can help you determine the exact reason.

How can I resolve the health of a node when its health shows "NOT UP"?

Node health " **Not UP**" indicates that there are some issues with the node. To know the root cause, you must run the show cluster node command. This command displays the node properties and the reason for the node failure.

What must I do when the health of a node shows as "NOT UP" and the reason indicates that configuration commands have failed on a node?

This issue arises when some commands are not executed on the cluster nodes. In such cases, you must make sure that the configurations are synchronized using one of the following options:

- If some of the cluster nodes are in this state, you must perform the force cluster synchronization operation on those nodes. For more information, see "Synchronizing Cluster Configurations".

- If all cluster nodes are in this state, you must disable and then enable the cluster instance on all the cluster nodes.

When I run the set vserver command, I get the following message, "No such resource." What must I do to resolve this issue?

The `set vserver` command is not supported in clustering. The `unset vserver`, `enable vserver`, `disable vserver`, and `rm vserver` commands are also not supported. However, the `show vserver` command is supported.

I cannot configure the cluster over a Telnet session. What must I do?

Over a telnet session, the cluster IP address can be accessed only in read-only mode. Therefore, you cannot configure a cluster over a telnet session.

I notice a significant time difference across the cluster nodes. What must I do to resolve this issue?

When PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment, the time will not get synchronized.

To synchronize the times, you must do the following on the cluster IP address:

1. Disable PTP.

   set ptp -state `disable`

2. Configure Network Time Protocol (NTP) for the cluster. For more information, see "Setting up Clock Synchronization".

What must I do, if there is no connectivity to the cluster IP address and the NSIP address of a cluster node?

If you cannot access to the cluster IP address or the NSIP of a cluster node, you must access the appliance through the serial console. For more information, see "Using the Command Line Interface".

If the NSIP address is reachable, you can SSH to the cluster IP address from the shell by executing the following command at the shell prompt:

ssh nsroot@<cluster IP address>

What must I do to recover a cluster node that has connectivity issues?

To recover a node that has connectivity issues:

1. Disable the cluster instance on that node (since you cannot execute commands from the NSIP of a cluster node).

2. Execute the commands required to recover the node.

3. Enable the cluster instance on that node.

Some nodes of the cluster have two default routes. How can I remove the second default route from the cluster node?

To delete the additional default route, do the following on each node that has the extra route:

1. Disable the cluster instance.

   disable cluster instance <clId>

2. Remove the route.

   rm route <network> <netmask> <gateway>

3. Enable the cluster instance.

   enable cluster instance <clId>

Parameter Descriptions (of commands listed in the CLI procedure)

set ptp

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable cluster instance

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

rm route

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

enable cluster instance

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Clustering FAQs

How many NetScaler appliances can I have in a cluster?

A NetScaler cluster can include as few as 2 or as many as 32 NetScaler nCore hardware or virtual appliances.

Can a cluster have NetScaler appliances from different networks?

No. The current cluster implementation requires that all cluster nodes be in the same network.

Can a NetScaler appliance be a part of multiple clusters?

No. An appliance can belong to only one cluster.

How can I set the hostname for a cluster node?

The hostname of a cluster node must be specified by executing the set ns hostname command through the cluster IP address. For example, to set the hostname of the cluster node with ID 2, the command is:

> set ns hostname hostName1 -ownerNode 2

What is a cluster IP address? What is its subnet mask?

The cluster IP address is the management address of a NetScaler cluster. All cluster configurations must be performed by accessing the cluster through this address. The subnet mask of the cluster IP address is fixed at 255.255.255.255.

Can I automatically detect NetScaler appliances so that I can add them to a cluster?

Yes. The configuration utility allows you to discover appliances that are present in the same subnet as the NSIP address of the configuration coordinator. For more information, see "Discovering NetScaler Appliances".

Why are the network interfaces of a cluster represented in 3-tuple (n/u/c) notation instead of the regular 2-tuple (u/c) notation?

When an appliance is part of a cluster, you must be able to identify the node to which the network interface belongs. Therefore, the network interface naming convention for cluster nodes is modified from u/c to n/u/c, where n denotes the node Id.

I have multiple standalone appliances, each of which has different configurations. Can I add them to a single cluster?

Yes. You can add appliances that have different configurations to a single cluster. However, when the appliance is added to the cluster, the existing configurations are cleared. To use the configurations that are available on each of the individual appliances, you must:

1. Create a single *.conf file for all the configurations.

2. Edit the configuration file to remove features that are not supported in a cluster environment.

3. Update the naming convention of interfaces from 2-tuple (u/c) format to 3-tuple (n/u/c) format.

4. Apply the configurations to the configuration coordinator node of the cluster by using the batch command.

Can I migrate the configurations of a standalone NetScaler appliance or an HA setup to the clustered setup?

No. When a node is added to a clustered setup, its configurations are implicitly cleared by using the clear ns config command (with the extended option). In addition, the SNIP addresses and all VLAN configurations (except default VLAN and NSVLAN) are cleared. Therefore, it is recommended that you back up the configurations before adding the appliance to a cluster. Before using the backed-up configuration file for the cluster, you must:

1. Edit the configuration file to remove features that are not supported in a cluster environment.

2. Update the naming convention of interfaces from two-tuple (x/y) format to three-tuple (x/y/z) format.

3. Apply the configurations to the configuration coordinator node of the cluster by using the batch command.

How can I configure/unconfigure the NSVLAN on a cluster?

- To make the NSVLAN available in a cluster, make sure that each appliance has the same NSVLAN configured before it is added to cluster.

- To remove the NSVLAN from a cluster node, first remove the node from the cluster and then delete the NSVLAN from the appliance.

Can a cluster node that is not connected to the client or server network still serve traffic?

Yes. The cluster supports a traffic distribution mechanism called linksets, which allows unconnected nodes to serve traffic by using the interfaces of connected nodes. The unconnected nodes communicate with the connected nodes through the cluster backplane. For more information, see "Using Linksets".

Can I execute commands from the NSIP address of a cluster node?

No. Access to individual cluster nodes through the NetScaler IP (NSIP) addresses is read-only. Therefore, when you log on to the NSIP address of a cluster node you can only view the configurations and the statistics. You cannot configure anything. However, there are some operations you can execute from the NSIP address of a cluster node. For more information, see "Operations Supported on Individual Nodes".

Can I disable configuration propagation among cluster nodes?

No, you cannot explicitly disable the propagation of cluster configurations among cluster nodes. However, during a software upgrade or downgrade, a version mismatch can

automatically disable configuration propagation.

Can I change the NSIP address or change the NSVLAN of a NetScaler appliance when it is a part of the cluster?

No. To make such changes you must first remove the appliance from the cluster, perform the changes, and then add the appliance to the cluster.

Does the NetScaler cluster support L2 and L3 Virtual Local Area Networks (VLANs)?

Yes. A cluster supports VLANs between cluster nodes. The VLANs must be configured on the cluster IP address.

- **L2 VLAN.** You can create a layer2 VLAN by binding interfaces that belong to different nodes of the cluster.

- **L3 VLAN.** You can create a layer3 VLAN by binding IP addresses that belong to different nodes of the cluster. The IP addresses must belong to the same subnet. Make sure that one of the following criteria is satisfied. Otherwise, the L3 VLAN bindings can fail.

  - All nodes have an IP address on the same subnet as the one bound to the VLAN.

  - The cluster has a striped IP address and the subnet of that IP address is bound to the VLAN.

  When you add a new node to a cluster that has only spotted IPs, the sync happens before spotted IP addresses are assigned to that node. In such cases, L3 VLAN bindings can be lost. To avoid this loss, either add a striped IP or add the L3 VLAN bindings on the NSIP of the newly added node.

How can I configure SNMP on a NetScaler cluster?

SNMP monitors the cluster, and all the nodes of the cluster, in the same way that it monitors a standalone appliance. The only difference is that SNMP on a cluster must be configured through the cluster IP address. When generating hardware specific traps, two additional varbinds are included to identify the node of the cluster: node ID and NSIP address of the node.

For detailed information about configuring SNMP, see "SNMP".

What details must I have available when I contact technical support for cluster-related issues?

The NetScaler provides a `show techsupport -scope cluster` command that extracts configuration data, statistical information, and logs of all the cluster nodes. You must run this command on the cluster IP address.

The output of this command is saved in a file named collector_cluster_<nsip_CCO>_P_<date-timestamp>.tar.gz which is available in the /var/tmp/support/cluster/ directory of the configuration coordinator.

Send this archive to the technical support team to debug the issue.

Can I use striped IP addresses as the default gateway of servers?

In case of cluster deployments, make sure the default gateway of the server points to a striped IP address (if you are using a NetScaler-owned IP address). For example, in case

of LB deployments with USIP enabled, the default gateway must be a striped SNIP address.

Can I view routing configurations of a specific cluster node from the cluster IP address?

Yes. You can view and clear the configurations specific to a node by specifying the owner node while entering the vtysh shell.

For example, to view the output of a command on nodes 0 and 1, the command is as follows:

```
> vtysh
ns# owner-node 0 1
ns(node-0 1)# show cluster state
ns(node-0 1)# exit-cluster-node
ns#
```

How can I specify the node for which I want to set the LACP system priority?

Applicable for NetScaler 10.1 and later releases.

In a cluster, you must set that node as the owner node by using the set lacp command.

For example: To set the LACP system priority for node with ID 2:

```
> set lacp -sysPriority 5 -ownerNode 2
```

How can I configure IP tunnels in a cluster?

Applicable for NetScaler 10.1 and later releases.

Configuring IP tunnels in a cluster is the same as on a standalone appliance. The only difference is that in a cluster setup, the local IP address must be a striped SNIP or MIP address. For more information, see "Configuring IP Tunnels".

How can I add a failover interface set (FIS) on the nodes of a NetScaler cluster?

Applicable for NetScaler 10.5 and later releases.

On the cluster IP address, specify the ID of the cluster node on which the FIS must be added.

add fis <name> -ownerNode <nodeId>

Note:

- The FIS name for each cluster node must be unique.
- A cluster LA channel can be added to a FIS. You must make sure that the cluster LA channel has a local interface as a member interface.

For more information on FIS, see "Configuring FIS".

Are Net Profiles supported on a cluster?

Applicable for NetScaler 10.5 and later releases.

Net profiles are now supported on a NetScaler cluster. You can bind spotted IP addresses to a net profile which can then be bound to spotted lbvserver or service (defined using a node group) with the following recommendations:

Note:

- If the "strict" parameter of the node group is "Yes", the net profile must contain a minimum of one IP address from each node of the node group member.
- If the "strict" parameter of the node group is "No", the net profile must include at least one IP address from each of the cluster nodes.
- If the above recommendations are not followed, the net profile configurations will not be honored and the USIP/USNIP settings will be used.

Parameter Descriptions (of commands listed in the CLI procedure)

add fis

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Operations Not Propagated to Cluster Nodes

Unless specified otherwise, all operations performed on the cluster IP address, are propagated to other cluster nodes. The exceptions to this rule are:

shutdown

Shuts down only the configuration coordinator.

reboot

Reboots only the configuration coordinator.

rm cluster instance

Removes the cluster instance from the node that you are executing the command on.

Operations Supported on Individual Cluster Nodes

Access to cluster nodes through their NSIP addresses, is read-only. However, NetScaler allows you to perform the following operations on individual cluster nodes by accessing their NSIP address. These operations, when executed from the NSIP address, are not propagated to other cluster nodes.

Note: All the show and statistics commands are allowed as they do not involve any change in configurations.

- cluster instance (set | rm | enable | disable)
- cluster node (set | rm)
- nstrace (start | show | stop)
- interface (set | enable | disable)
- force cluster sync
- sync cluster files
- disable ntp sync
- save ns config
- reboot
- shutdown

For example, when you execute the command disable interface `1/1/1` from the NSIP address of a cluster node, the interface is disabled only on that node. Since the command is not propagated, the interface 1/1/1 remains enabled on all the other cluster nodes.

CloudBridge

As a tool for building a cloud-extended data center, the Citrix NetScaler® CloudBridge™ feature is a fundamental part of the Citrix® Cloud framework. This feature can reduce the cost of moving your applications to the cloud, reduce the risk of application failure, and increase network efficiency in your cloud environment.

With the CloudBridge feature, you can create a network bridge (or more than one) connecting one or more cloud computing instances-virtual servers in the cloud-to your network without reconfiguring your network. Cloud-hosted applications appear as though they are running on one contiguous enterprise network.

Setting up a network bridge involves configuring two NetScaler appliances or virtual appliances, one on each side of the bridge. On each appliance, you configure one or more GRE tunnels and configure IPSec on the tunnel or tunnels. You then assign a name to the network bridge and bind the GRE tunnel(s) to it. Optionally, you can bind VLANs and IP addresses to the network bridge.

If you need only one GRE tunnel, you can use an alternative configuration method in which you configure all of the network bridge elements in one dialog box in the configuration utility. You can add more tunnels later.

CloudBridge is a complete network solution - **available as a standalone physical or virtual appliance, or integrated into NetScaler Platinum edition** - enabling enterprises to transparently shift web and application servers to the cloud while keeping the database safely within the enterprise datacenter.

Terminology

The Citrix CloudBridge VPX™ product is a virtual instance that can be hosted on Amazon Web Services (AWS), Citrix XenServer®, VMware ESX or ESXi, and Microsoft Hyper-V virtualization platforms. The Citrix CloudBridge MPX™ product is a physical appliance that you can install in your private enterprise network.

Note: These topics focuses primarily on CloudBridge VPX.

The term CloudBridge can also refer to the connection that you create between the two private networks by using CloudBridge appliances or instances. Networks connected by a CloudBridge function like a single network. The CloudBridge is transparent to the user. To configure a CloudBridge, you:

1. Create a network bridge
2. Create an IPSec profile
3. Create a GRE tunnel with the IPSec profile
4. Bind the tunnel to the network bridge.

CloudBridge VPX License

After the initial instance launch, CloudBridge VPX for AWS requires a license. If you are bringing your own license (BYOL), see the VPX Licensing Guide at: http://support.citrix.com/article/CTX122426.

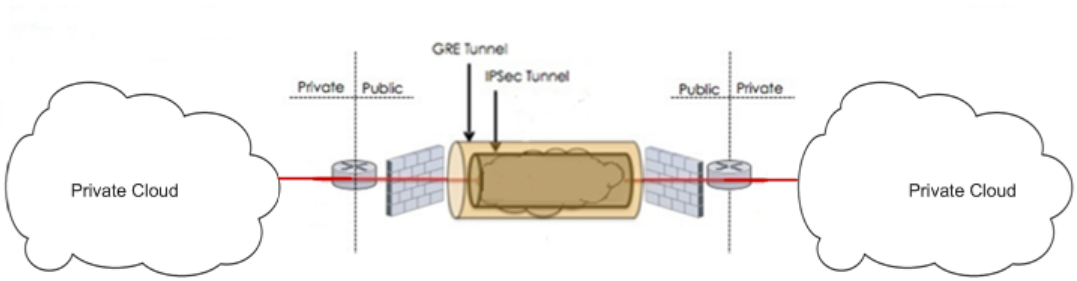
You have to:

1. Use the licensing portal within MyCitrix to generate a valid license.
2. Upload the license to the instance.

If this is a **paid** marketplace instance, then you do not need to install a license. The correct feature set and performance will activate automatically.

CloudBridge Architecture

You can configure a CloudBridge between a data center and AWS, between a data center and a data center, or between two VPCs in AWS clouds. Setting up a CloudBridge involves configuring a CloudBridge appliance or instance on each side of the bridge. On each appliance or instance, you configure a network bridge and one or more GRE tunnels with IPSec enabled. You then assign a name to the network bridge and bind the IPSec tunnel(s) to it. Optionally, with CloudBridge MPX, you can bind VLANs and IP addresses to the network bridge.



The following figure illustrates the topology of a seamless network with a secure tunnel.
Figure 1. CloudBridge Architecture

CloudBridge VPX and MPX support all the features of a NetScaler appliance, except the virtual MAC (vMAC) addresses, Layer 2 (L2) mode, and link aggregation control protocol (LACP). VLAN tagging is supported on the CloudBridge VPX virtual appliances hosted on the XenServer and VMware ESX platforms.

Generic Routing Encapsulation

The network bridge extends layer 2 bridging to connect a CloudBridge virtual appliance residing in a cloud to a CloudBridge virtual appliance on your LAN or in your cloud. The connection is established by using a Generic Routing Encapsulation (GRE) tunnel. The GRE protocol provides a mechanism for encapsulating packets from a wide variety of network protocols. The GRE protocol encapsulates packets by adding a GRE header and a GRE IP header to the packets.

Internet Protocol Security

CloudBridge supports the use of the open-standard Internet Protocol security (IPSec) protocol suite to secure the communication between the connected peers.

In a CloudBridge, IPSec ensures:

- Data integrity

- Data origin authentication
- Data confidentiality (encryption)
- Protection against anti-replay attacks

CloudBridge uses IPSec transport mode to:

- Protect data exchanged between the two hosts
- Secure the IP packet using Encapsulating Security Payload (ESP).
- Encapsulate the IPSec/ESP packet over the GRE tunnel

The IPSec/ESP header is inserted after the GRE header, and an ESP trailer is inserted at the end of the encrypted payload.

CloudBridge also supports the NAT implementation defined in RFCs 3947 and 3948, for the CloudBridge peers to communicate with peers behind NAT devices.

To secure the communication across the network bridge, the two peers use Internet Key Exchange (IKE) and IPSec to:

- Authenticate each other, using one of the following authentication methods:
    - **Pre-shared key authentication**. A text string called a pre-shared key is manually configured on each peer. The pre-shared keys of the peers are matched against each other for authentication. Therefore, for the authentication to be successful, you must configure the same pre-shared key on each of the peers.
    - **Digital certificates authentication**. The initiator (sender) peer signs message interchange data by using its private key and the other receiver peer uses the sender's public key to verify the signature. Typically, the public key is exchanged in messages containing an X.509v3 certificate. This certificate provides a level of assurance that a peer's identity as represented in the certificate is associated with a particular public key.
- Negotiate to reach agreement on:
    - ESP security protocol
    - Encryption algorithm
    - Cryptographic algorithms for data authentication

This agreement upon the ESP, encryption algorithm and authentication algorithm is called a security association (SA). SAs function in the simplex communication mode. SA is used to encrypt the outgoing packets and decrypt the incoming packets.

SAs expire after a specified length of time, which is called the *lifetime*. The two peers use the Internet Key Exchange (IKE) protocol to negotiate new cryptographic keys and establish new SAs. The purpose of the limited lifetime is to prevent attackers from cracking a key.

Branch Repeater

Citrix Branch Repeater accelerates Wide Area Networks, providing LAN-like performance for applications running across enterprise data centers and public clouds. Branch Repeaters offer a broad base of protocol acceleration support and market-leading VDI acceleration for Citrix XenDesktop. Branch Repeater appliances work in pair at either side of the WAN.

For more information about Branch Repeater appliances, see Branch Repeaters.

Consider an example of a CloudBridge setup where CloudBridge appliances CB1 and CB2 are CloudBridge peers. To enable WAN optimization in the CloudBridge set up, Branch Repeater appliances BR1 and BR2 are paired with CloudBridge appliances CB1 and CB2, respectively.

Following is the traffic flow in this example:

1. The CloudBridge CB1 at one end sends the data to Branch Repeater appliance BR1.
2. BR1 compresses the data and sends it to CloudBridge CB1.
3. CB1 sends the compressed data to its peer, CloudBridge CB2.
4. CB2 sends the compressed data to Branch Repeater BR2 for decompression.
5. BR2 decompresses the data and sends it to CloudBridge CB2.
6. CloudBridge CB2 forwards the data.

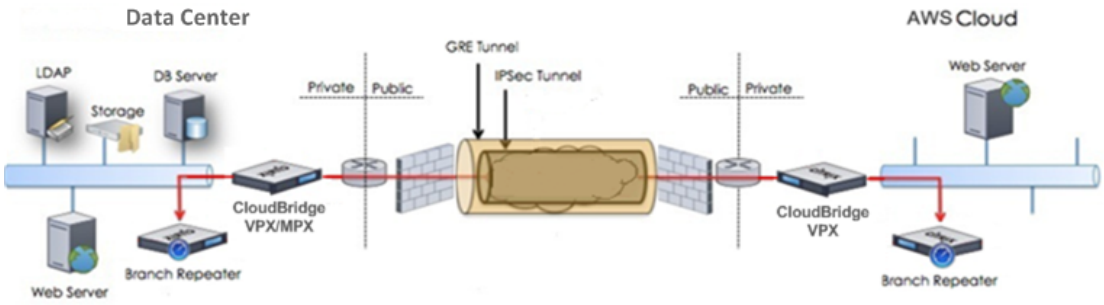
CloudBridge Topologies

You can deploy CloudBridge for seamless connectivity between CloudBridge VPX instances in the data center and in an AWS cloud, between two CloudBridge VPX instances in two different VPCs in AWS clouds, or between two CloudBridge instances in two different data centers. The advantage of CloudBridge is that you can leverage the resources between two locations for optimal use and performance.

Amazon Web Services provides a highly reliable, scalable, secure, low-cost infrastructure platform in the cloud. You can leverage AWS to run and deploy applications without having to wait for the infrastructure to be set up. AWS provides flexibility in your choice of a platform and development language. You can install any platform and programming model that meets your business requirement. Once the deployment is complete, all the applications and services hosted on the cloud appear local to the user.

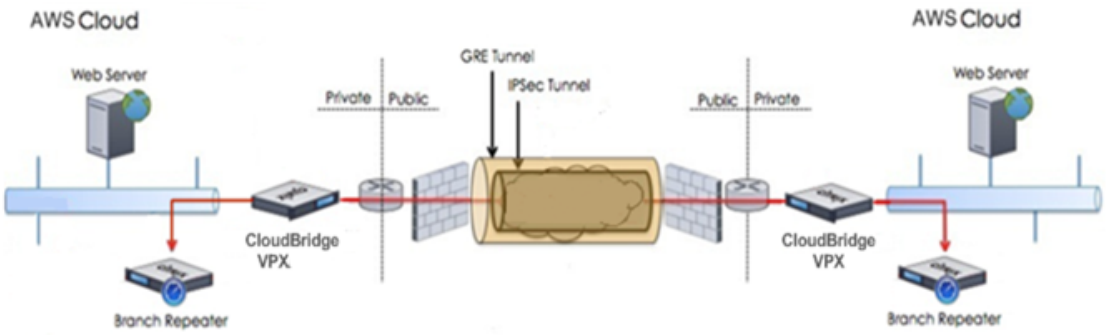
Between Data Center and AWS

You can connect your data center to AWS or AWS to data center by using CloudBridge to leverage the infrastructure and computing capabilities of the data center and the AWS cloud. With AWS, you can extend your network without initial capital investment or the cost of maintaining the extended network infrastructure. You can scale your infrastructure up or down, as required. For example, you can lease more server capabilities when the demand increases.



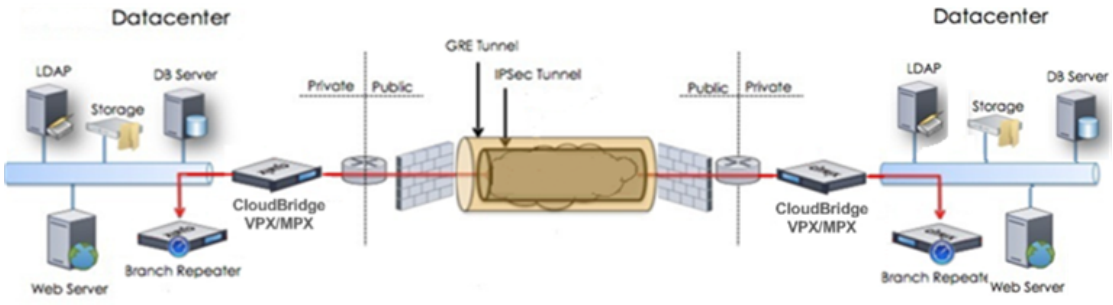
AWS to AWS

You can deploy a CloudBridge between two CloudBridge VPX instances/MPX appliances in two different VPCs in AWS cloud to implement redundancy and failure protection. This setup helps in optimal utilization of infrastructure and resources across the two AWS clouds. This deployment is primarily used to provide backup for the applications and services running in one cloud instance.



Data Center to Data Center

You can deploy a CloudBridge between two CloudBridge VPX instances/MPX appliances in two different data centers to implement redundancy and failure protection. This setup helps achieve optimal utilization of infrastructure and resources across two data centers. This deployment is primarily used to provide backup for the applications and services running in one data center.



Installing NetScaler VPX on AWS

You can now launch an instance of Citrix® NetScaler VPX within Amazon Web Services (AWS). NetScaler VPX is available as an Amazon Machine Image (AMI) in AWS marketplace. NetScaler VPX on AWS enables customers to leverage AWS Cloud computing capabilities and use NetScaler load balancing and traffic management features for their business needs. NetScaler on AWS supports all the traffic management features of a physical NetScaler appliance. NetScaler instances running in AWS can be deployed as standalone instances or in HA pairs.

How NetScaler VPX on AWS Works

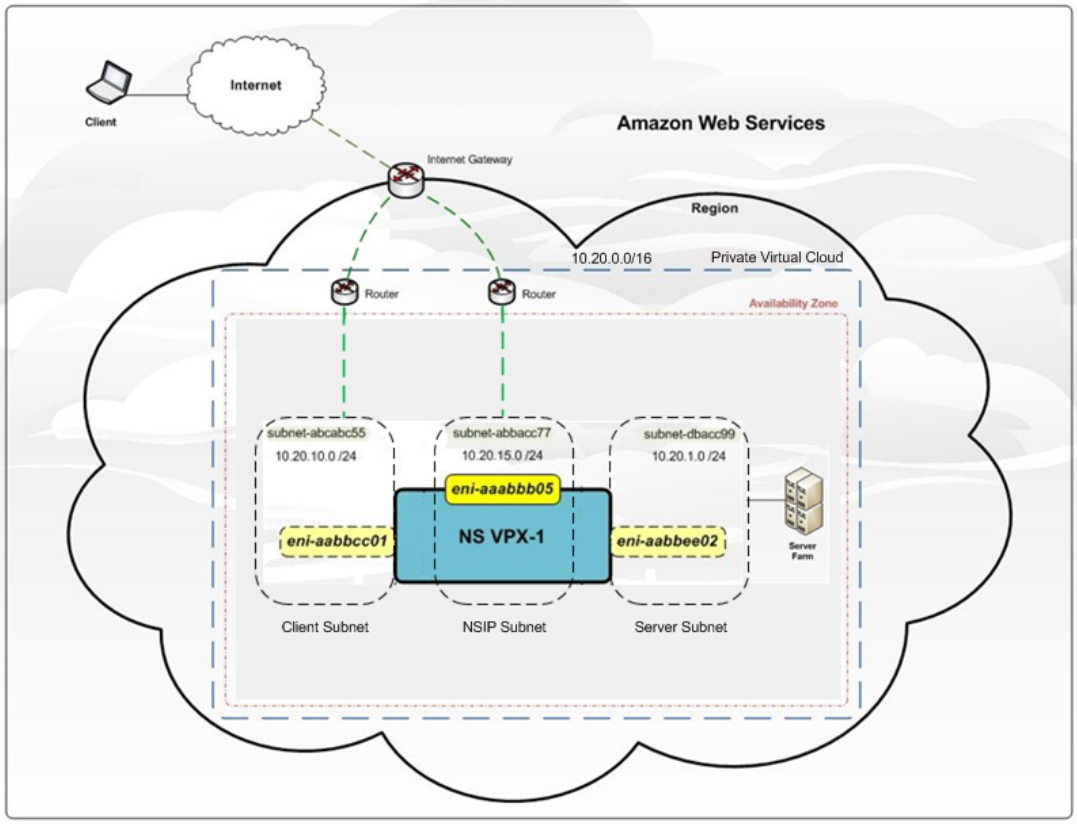
AWS offers different types of web services, such as Amazon Simple Storage Services (S3), Amazon Elastic Cloud Compute (EC2), and Amazon Virtual Private Cloud (VPC). Amazon VPC allows you to run AWS resources (for example, EC2 instances) in a private, virtual network. Amazon EC2 instances are available as instance types that map to hardware archetypes on the basis of factors such as number of EC2 Compute Units (ECU), number of virtual cores, and memory size.

The NetScaler VPX AMI is packaged as an EC2 instance that is launched within an AWS VPC. The VPX AMI instance requires a minimum of 2 virtual CPUs and 2 GB of memory. An EC2 instance launched within an AWS VPC can also provide the multiple interfaces, multiple IP addresses per interface, and public and private IP addresses needed for VPX configuration. Currently, on Amazon AWS, VPX can be launched only within a VPC, because each VPX instance requires at least three IP addresses. (Although VPX on AWS can be implemented with one or two elastic network interfaces, Citrix recommends three network interfaces for a standard VPX on AWS installation.) AWS currently makes multi-IP functionality available only to instances running within an AWS VPC. A VPX instance in a VPC can be used to load balance servers running in EC2 instances.

An Amazon VPC allows you to create and control a virtual networking environment, including your own IP address range, subnets, route tables, and network gateways.

Note: By default, you can create up to 5 VPC instances per AWS region for each AWS account. You can request higher VPC limits by submitting Amazon's request form (http://aws.amazon.com/contact-us/vpc-request/).

VPX on AWS Architecture



An EC2 instance of NetScaler VPX (AMI image) is launched within the AWS VPC. The following figure shows a typical VPX on AWS deployment.Figure 1. VPX on AWS Architecture

The figure shows a simple topology of an AWS VPC with a NetScalerVPX deployment. The AWS VPC has:

1. A single Internet gateway to route traffic in and out of the VPC.
2. Network connectivity between the Internet gateway and the Internet.
3. Three subnets, one each for management, client, and server.
4. Network connectivity between the Internet gateway and the two subnets (management and client).
5. A single NetScaler VPX deployed within the VPC. The VPX instance has three Elastic Network Interfaces (ENIs), one attached to each subnet.

Supported EC2 instances

The NetScaler AMI can be launched on any of the following EC2 instance types:

- m1.large

- m1.xlarge

For more information about Amazon EC2 instances, see:
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/instance-types.html

ENI Support

The following table lists the EC2 instance types and corresponding number of supported ENIs and number of private IP addresses per ENI.

Table 1. EC2 Support for ENIs and IP Addresses

Instance Name	Number of ENIs	Private IP Addresses per ENI
m1.large	3	10
m1.xlarge	4	15

Limitations and Usage Guidelines

- The clustering feature is not supported for VPX.
- For HA to work as expected, associate a dedicated NATing device to management Interface or associate EIP to NSIP. For more information on NAT, in the AWS documentation, see NAT Instances.
- Data traffic and management traffic should be segregated by using ENIs belonging to different subnets.
- Only the NSIP address should be present on the management ENI.
- If a NAT instance is used for security instead of assigning an EIP to the NSIP, appropriate VPC level routing changes are required. For instructions on making VPC level routing changes, in the AWS documentation, see "Scenario 2: VPC with Public and Private Subnets."
- A VPX instance can be moved from one EC2 instance type to another (for example, from m1.large to an m1.xlarge).
- For storage options for VPX on AWS, Citrix recommends EBS, because it is durable and the data is available even after it is detached from instance.
- Dynamic addition of ENIs to VPX is not supported. You have to restart the VPX instance to apply the update. Citrix recommends you to stop the standalone or HA instance, attach the new ENI, and then restart the instance.
- You can assign multiple IP addresses to an ENI. The maximum number of IP addresses per ENI is determined by the EC2 instance type, see EC2 Support for ENIs and IP Addresses.
- Citrix recommends that you avoid using the enable and disable interface commands on NetScaler VPX interfaces.
- Due to Amazon AWS limitations, these features are not supported:
  - IPV6
  - Gratuitous ARP(GARP)
  - L2 mode
  - Tagged VLAN
  - Dynamic Routing
  - Virtual MAC (VMAC)

Launching the NetScaler VPX for AWS AMI

You can launch a Citrix NetScaler VPX AMI within an Amazon Web Services (AWS) Virtual Private Cloud (VPC) in one of two ways:

1. Using the Amazon GUI and CLI toolkit.
2. Using a Citrix authored CloudFormation template.
3. Using the Amazon 1-Click launch.

Launching NetScaler VPX for AWS by Using the Amazon GUI and CLI toolkit

To launch a NetScaler VPX AMI within an Amazon Web Services (AWS) Virtual Private Cloud (VPC) by using the Amazon GUI and CLI toolkit, you need:

- An AWS account
- An AWS Virtual Private cloud (VPC)
- The AWS API toolkit (if creating a VPX instance with three or more ENIs).
- An IAM account

Creating an AWS Account

To launch a NetScaler VPX AMI in an Amazon Web Services (AWS) Virtual Private Cloud (VPC), you need an AWS account. You can create an AWS account for free at www.aws.amazon.com.

Creating an AWS Virtual Private Cloud (VPC)

Citrix recommends at least three IP addresses for a NetScaler instance. Currently, the only support that AWS provides for instances with multiple IP addresses is for instances within an AWS VPC.

To create an AWS VPC, first launch the AWS GUI console. For instructions for using the AWS GUI console, see http://docs.amazonwebservices.com/AmazonVPC/latest/GettingStartedGuide/GetStarted.html?r=2900.

To create an AWS VPC

1. Use the VPC with a Single Public Subnet Only option to create a new AWS VPC in an AWS availability zone.
2. Create additional subnets within the AWS VPC. Citrix recommends that you create at least three subnets, of the following types:
   - One subnet for NetScaler management traffic. You place the NetScaler management IP(NSIP) on this subnet.
   - One or more subnets for client-access (user-to-NetScaler) traffic, through which clients connect to one or more virtual IP (VIP) addresses assigned to NetScaler load balancing virtual servers.

- One or more subnets for the server-access (NetScaler-to-server) traffic, through which your servers connect to NetScaler-owned subnet IP (SNIP) addresses.

  For more information about NetScaler load balancing and virtual servers, virtual IP addresses (VIPs), and subnet IP addresses (SNIPs), see: .

Note:

- All subnets should be in the same availability zone.
- You can launch a NetScaler AMI in an AWS VPC with a single subnet. In this configuration, the management traffic, client-side traffic, and server-side traffic all use the same subnet, and high availability (HA) cannot be configured.
- You can launch the NetScaler AMI into an AWS VPC with two subnets. In this configuration, one subnet is used for management traffic, and the other subnet is used for both client-side and server-side traffic. This topology supports NetScaler HA.

3. Create an Internet gateway and attach it to the VPC instance.
4. Create routing tables for all traffic flowing into or out of the VPC. You need routes for access to the NSIP and to any client-facing VIP addresses. Traffic leaving the VPC must be routed through the Internet Gateway of the AWS VPC.

   Note:

   - Make sure that you associate management and client subnets with the routing table.
   - Add a default route to the routing table for the traffic flowing out of the VPC. Set the Destination to 0.0.0.0/0, and the Target as the Internet gateway address.
5. Create a security group and open the required ports.

Setting-up the AWS API Toolkit

The AWS GUI console does not allow you to launch instances with more than two ENIs. For a standard deployment, you have to create at least three ENIs for a VPC instance (though it is possible to launch a NetScaler AMI with one or two ENIs). To create three or more ENIs for a NetScaler instance, you must use the AWS CLI. To use the AWS CLI, you must install the AWS API toolkit.

The AWS API toolkit is available for download at http://aws.amazon.com/developertools/351/. To install the AWS API toolkit, complete the following tasks on a Windows or Linux machine:

1. Download the AWS API Toolkit.
2. Download X.509 certificate files and X.509 private key file.
3. Download the private key.
4. Convert the downloaded private key (.pem file) for SSH connectivity.
5. Configure the AWS API Toolkit environment on your Windows or Linux computer.

To download the AWS API toolkit

1. In a web browser, open the following website: http://aws.amazon.com/developertools/351/.
2. On the Amazon EC2 API Tools page, in the Download section, click Download the Amazon EC2 API Tools.
3. Save the file, ec2-api-tools.zip, to a local disk and use a file compression utility (for example, WinZip) to extract the files.

To download the X.509 certificate file and X.509 private key file

1. In your browser, open the following website: http://aws.amazon.com/.
2. Click My Account/Console, and then click Security Credentials.
3. On the Amazon Web Services Sign in page, use your Amazon account credentials to sign in.
4. On the Security Credentials page, in the Access Credentials section, on the X.509 Certificates tab, click Create a New Certificate.
5. In the X509 Certificate Created dialog box, Click Download Private Key File and save the private key file to a secure folder on your local drive.
6. Click Download X.509 Certificate and save the certificate to a secure folder on your local drive.
7. Click Close.

Note: The Private Key File can be downloaded only at the time of creating a certificate. However, you can download the certificate at any time after creating it.

To download private key for SSH connectivity

1. In your browser, open the following website:http://aws.amazon.com/ .
2. Click **My Account/Console.**
3. On the **Amazon Web Services Sign in** page, use your Amazon account credentials to sign in.
4. In the **Service** pane, in **Amazon Web Services**, click **EC2**.
5. In the **Navigation** section, in **Network and Security**, click **Key Pairs**.
6. In the **Key Pairs** pane, click **Create Key Pair**.
7. In the **Create Key Pair** dialog box, type the name for key pair and click **Create**.
8. Download the Key Pair to the local disk and click **Close**.

To convert the downloaded private key for SSH connectivity

For SSH connections from a management machine using Putty, you must convert the .pem file (Private Key) into .ppk file. The .ppk file is the private key for SSH connections to the NetScaler VPX instance hosted in the AWS environment. To convert the .pem file

to a .ppk file, use the Putty application's PuttyGen utility. Make sure that the key pairs and certificate files are stored in an unshared and secured directory. After the conversion, you can use SSH to securely connect to the management address of the VPX on AWS instance.

To configure the AWS API Toolkit environment on a Windows machine

1. Move the certificate files to an unshared folder (for example, aws-ec2-api-tools).

2. Move the extracted AWS API toolkit folder to the unshared folder (for example, the aws-ec2-api-tools folder created in example in Step 1).

3. Create a batch file to configure the specific AWS environment in the unshared folder (aws-ec2-api-tools if you used the example in the preceding two steps). Following is an example of the batch file. The file location used in this example is C:\aws-vpc-config\ and the file name is set-aws-environment.bat.

   ```
   rem Setup Amazon EC2 Command-Line Tools

   set JAVA_HOME="C:\Program Files\Java\jre7\"

   set EC2_HOME="C:\aws-ec2-api-tools\"

   set PATH=%PATH%;%EC2_HOME%\bin

   set EC2_PRIVATE_KEY=C:\aws-ec2-security-files\pk-3T6ACCLBEDGD3O3
   SMAM7YDI76VP5HXSU.pem

   set EC2_CERT=C:\aws-ec2-security-files\cert-3T6ACCLBEDGD3O3SMAM7
   YDI76VP5HXSU.pem

   set EC2_URL=https://<aws-region>.ec2.amazonaws.com
   ```

4. Open the command prompt and run the batch file. For the file in the above example, type:

   ```
   C:\aws-vpc-config> set-aws-environment.bat
   ```

5. Run the ec2ver command to verify that the AWS toolkit is installed properly. For example:

   ```
   C:\aws-vpc-config>ec2ver 1.5.6.1 2012-06-15
   ```

To configure the AWS API Toolkit on a Linux machine

1. Move the certificate files to an unshared folder (for example, aws-ec2-api-tools).

2. Move the extracted AWS API toolkit folder to the unshared folder (for example, the aws-ec2-api-tools folder created in example in Step 1).

3. Create a shell script to configure the specific AWS environment in the unshared folder (aws-ec2-api-tools if you used the example in the preceding two steps). Following is an example of the batch file. In this example, the file location used is C:\aws-vpc-config\ and the file name used is set-aws-environment.bat.

   ```
   # Setup Amazon EC2 Command-Line Tools
   ```

```
export EC2_HOME=~/ec2-api-tools-1.5.6.0

export EC2_URL= https://us-east-1.ec2.amazonaws.com

export
PATH=$EC2_HOME/bin:/usr/bin:$/usr/sbin:/usr/local/sbin:/sbin

export EC2_PRIVATE_KEY=~/pk-XOX3NS2UPZL6BGLFO7PM5OGLYBDPBUCB.pem

export EC2_CERT=~/cert-XOX3NS2UPZL6BGLFO7PM5OGLYBDPBUCB.pem

export JAVA_HOME=/usr

export PS1="AWS PROMPT >"
```

4. Run the ec2ver command to verify that the AWS toolkit is installed properly. For example:

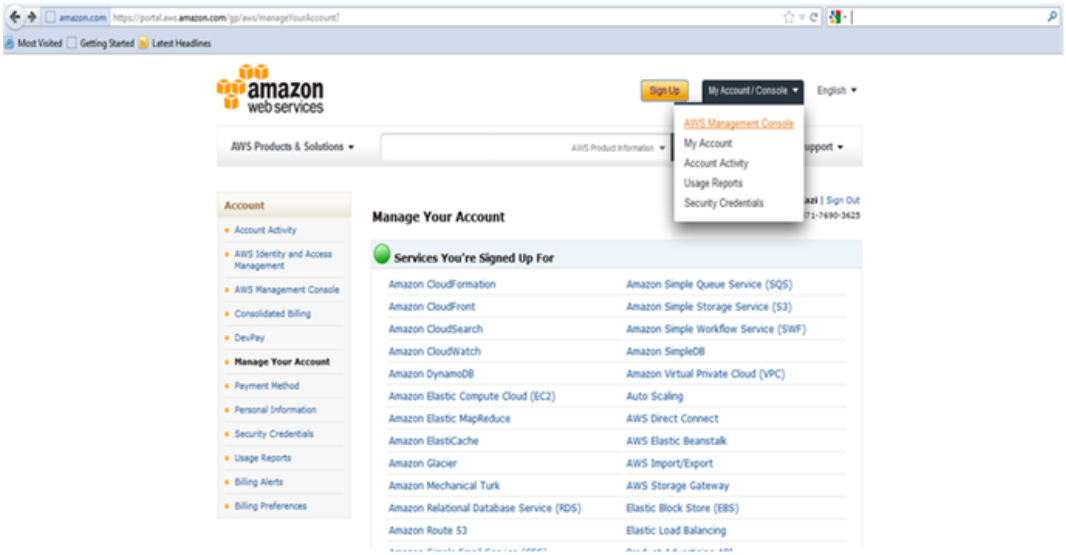
```
AWS PROMPT >ec2ver

1.5.6.1 2012-06-15
```

Creating an IAM Account

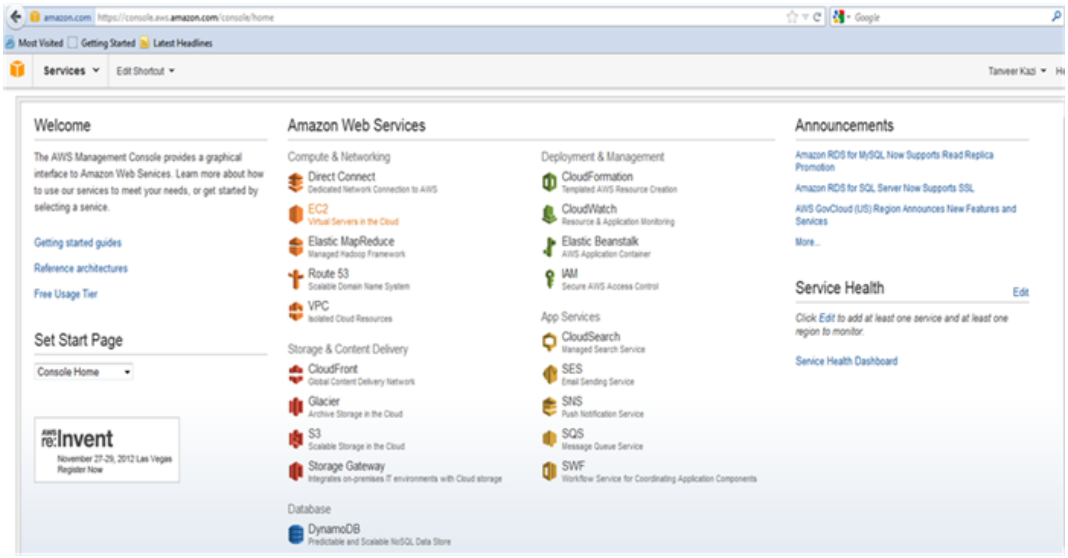
Before you launch the VPX AMI instance, you have to create a new IAM user account with the Access and Secret keys. The Access and Secret key credentials from the new IAM user are required for launching the NetScaler AMI instance. To create a new IAM user for NetScaler, complete the following steps.

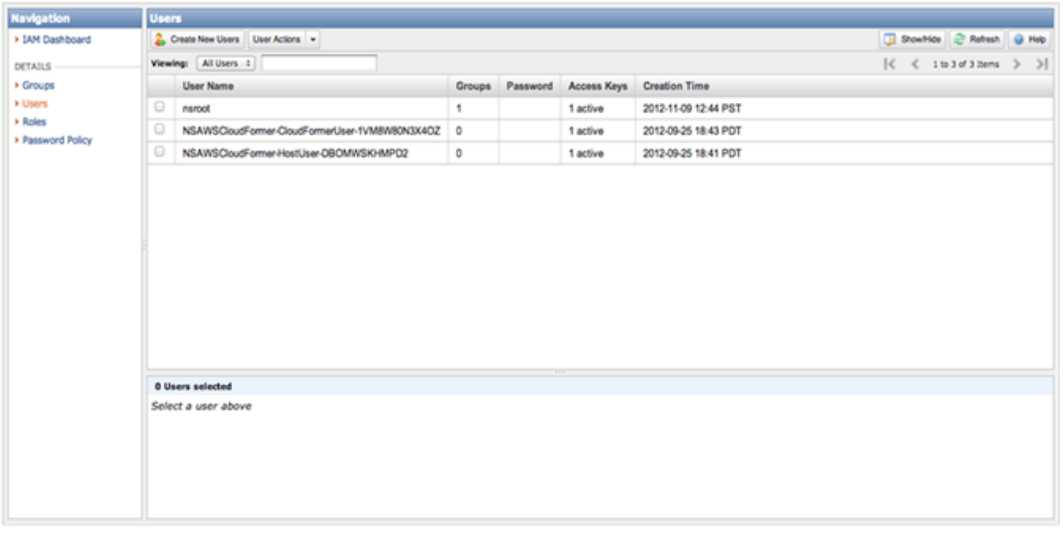
1. 

   In a web browser, open the website at www.aws.amazon.com and log on with AWS credentials.
2. Click My Account/Console, and then click AWS Management Console.



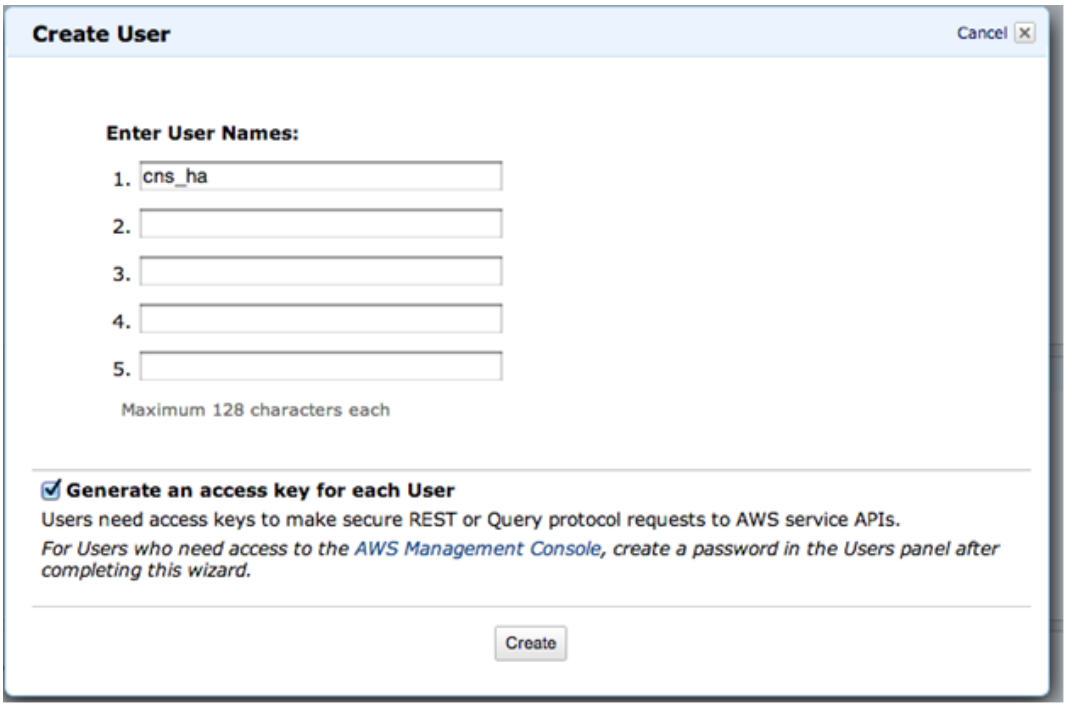
3. On the Amazon Web Services page, click IAM.



4. 

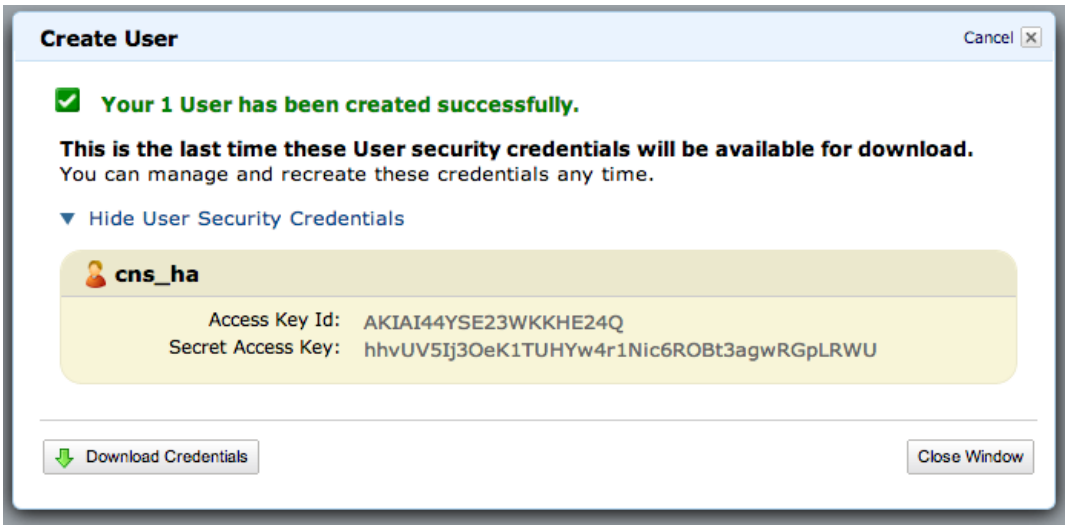
In the Navigation pane, click Users, and then click Create New Users.

5. In the Create User dialog box, in one of the Enter User Names text boxes, type a user name (for example, cns_ha). Also select the Generate an access key for each User check box, and then click Create.

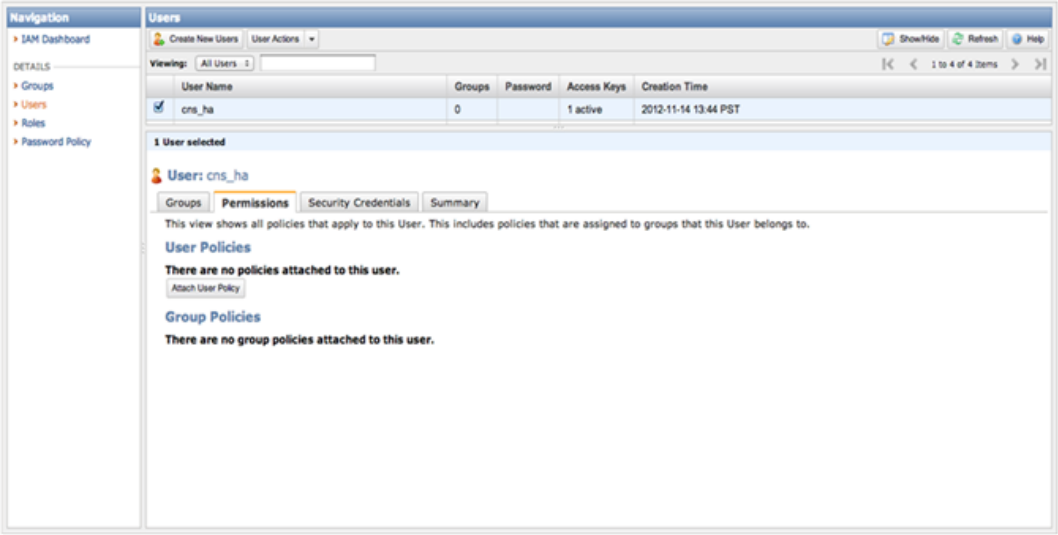


6. After a new IAM user is created, click Download Credentials to download the Access and Secret Keys to a safe location. These keys are required for launching NetScaler AMI. Click Close.

   Note: The Access Key ID and Secret Access Key values are used to create the key-pair file and to launch an instance.

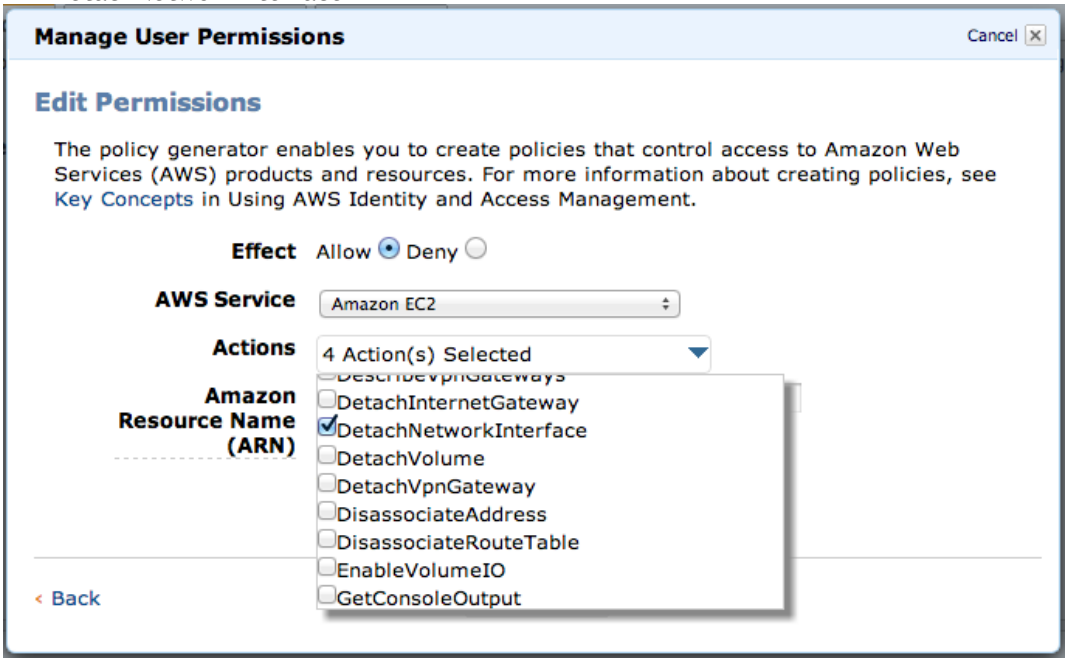


7. In the Users pane, select the newly created IAM user and click the Permissions tab. Then, click Attach User Policy to set policies for the user.

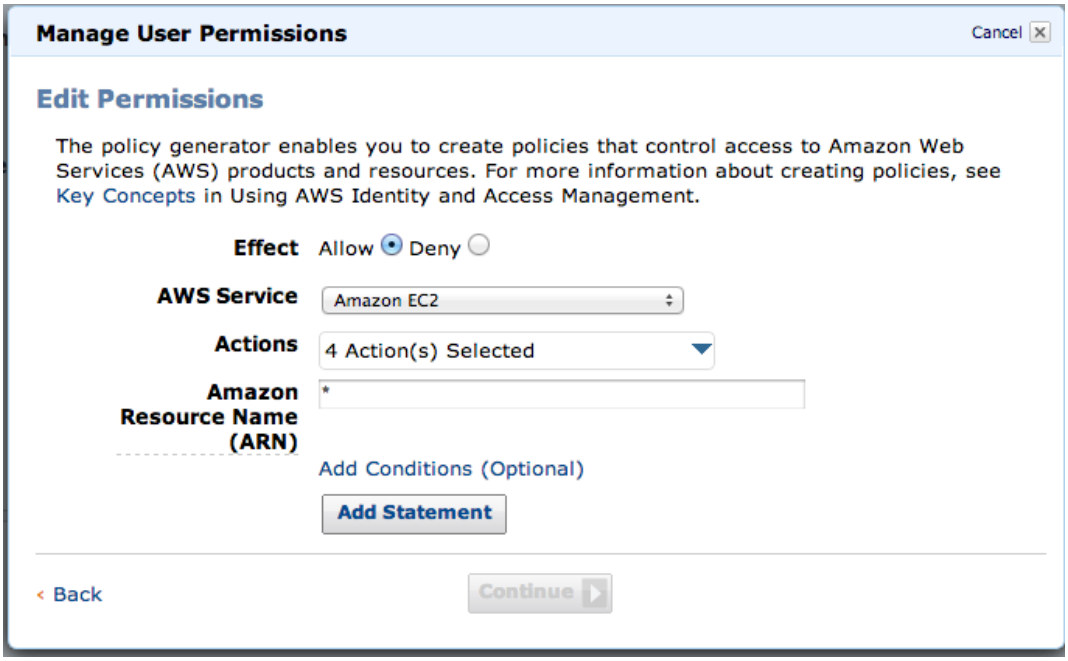


8. In the Manage User Permissions dialog box, next to Effect, select the Allow option. For AWS Service, select Amazon EC2. From the Actions drop-down list, select the following four actions:

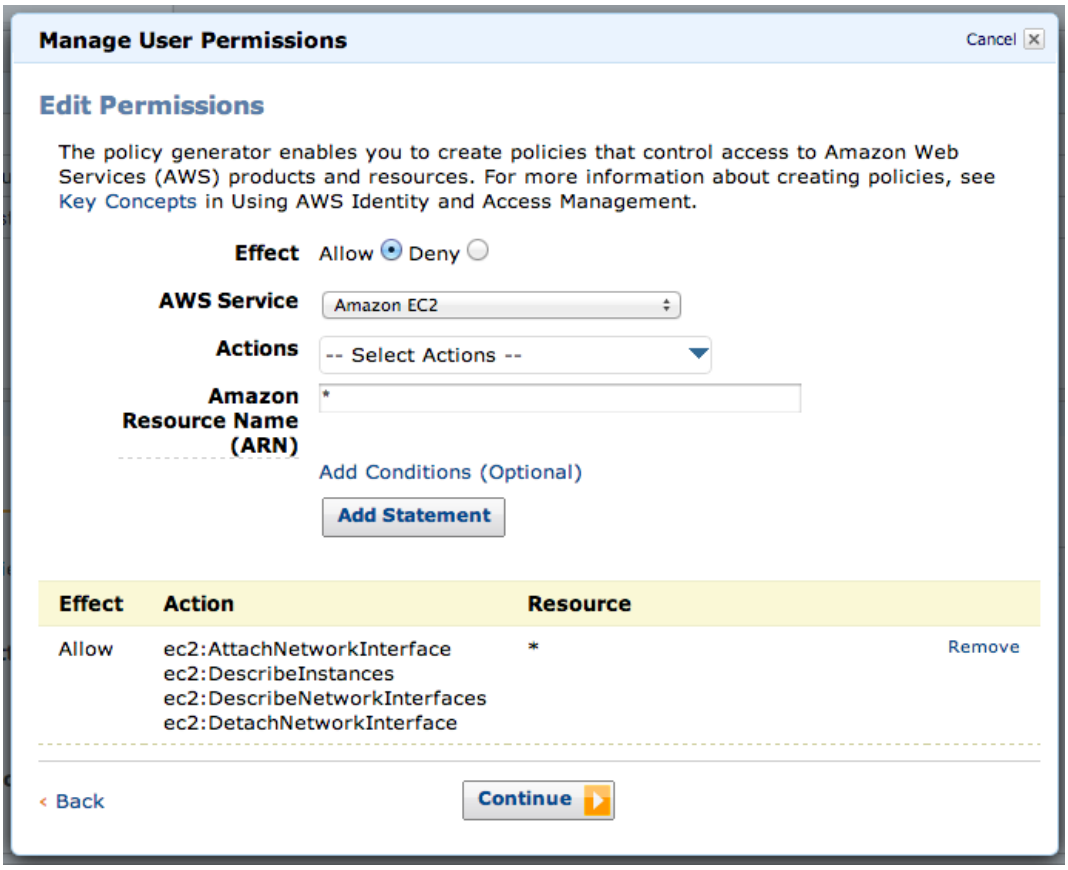
   - AttachNetworkInterface
   - DescribeInstances
   - DescribeNetworkInterfaces
   - DetachNetworkInterface



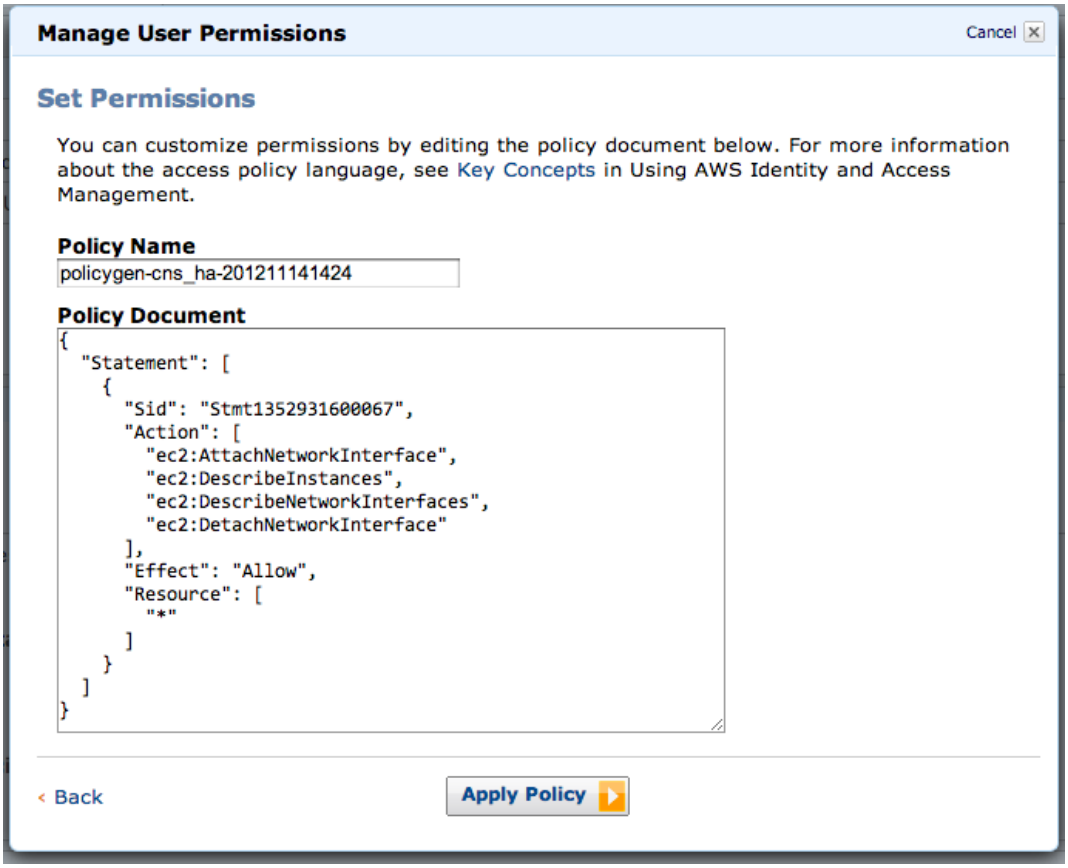
9. Click Add Statement.



10. Click Continue.



11. Click Apply Policy to set the new permissions for the selected user.



Launching the NetScaler AMI

Use the AWS CLI to launch the NetScaler AMI in an AWS VPC. Use the ec2-run-instances command. For information about the ec2-run-instances command, see http://docs.amazonwebservices.com/AWSEC2/latest/CommandLineReference/ApiReference-cmd-RunInstances.html.

Following are Windows and Linux examples of running the command to launch a single NetScaler instance. The EC2 instance type is m1.large. It is configured with the following entities:

- NetScaler AMI named ami-bd2986d4.
- Three ENIs (named NSIP, CLIENT-SIDE, and SERVER-SIDE) associated with the three subnets (15fa057e, 1547ba7e, and 1547ba7e) within the VPC.
- A single IP address for the NSIP ENI.
- Multiple private IP addresses (for multiple VIPs) on the CLIENT-SIDE ENI.
- Multiple private IPs (for multiple SNIPs) on the SERVER-SIDE ENI.

On a Windows platform:

```
C:\aws-vpc-config>ec2-run-instances ami-bd2986d4 -n 1 -t m1.large -k keyPairName -f
keyPairFile -a :0:subnet-15fa057e:"NSIP":10.20.15.21 -a :1:subnet-1547ba7e:"CLIENT-SIDE
```

":10.20.10.21::::"10.20.10.22,10.20.10.23,10.20.10.24,10.20.10.25,10.20.10.26,10.20.10.27,10.20.10.28,10.20.10.29,10.20.10.30" -a :2:subnet-cc47baa7:"SERVER-SIDE":10.20.1.21::::"10.20.1.22,10.20.1.23,10.20.1.24,10.20.1.25,10.20.1.26,10.20.1.27,10.20.1.28,10.20.1.29,10.20.1.30"

Note: The keyPairFile file contains the access and secret keys.

On a Linux platform:

AWS PROMPT > ec2-run-instances ami-bd2986d4 -n 1 -t m1.large -k keyPairName -f keyPairFile -a :0:subnet-15fa057e:"NSIP":10.20.15.21 -a :1:subnet-1547ba7e:"CLIENT-SIDE":10.20.10.21::::10.20.10.22,10.20.10.23,10.20.10.24,10.20.10.25,10.20.10.26,10.20.10.27,10.20.10.28,10.20.10.29,10.20.10.30 -a :2:subnet-cc47baa7:"SERVER-SIDE":10.20.1.21::::10.20.1.22,10.20.1.23,10.20.1.24,10.20.1.25,10.20.1.26,10.20.1.27,10.20.1.28,10.20.1.29,10.20.1.30

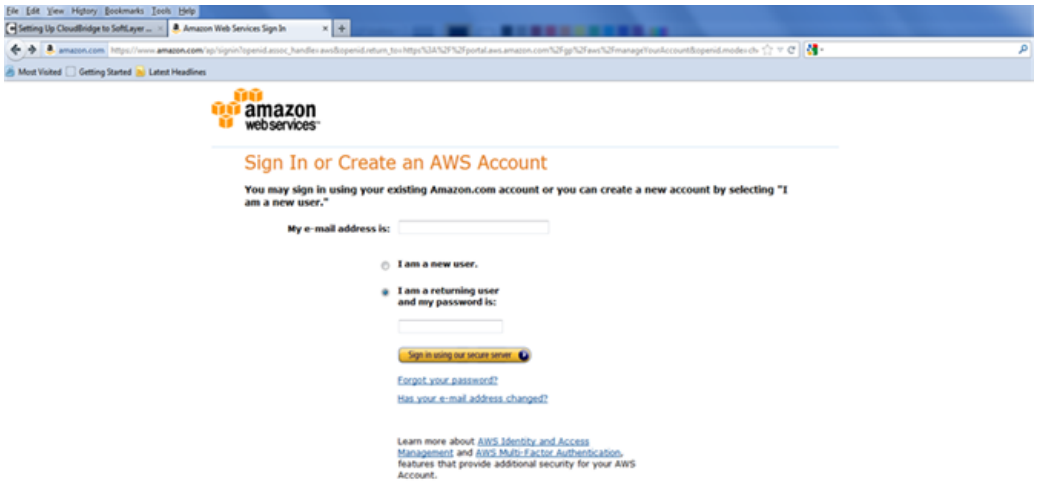
Note: The keyPairFile file contains the access and secret keys.

The command returns the instance ID and the associated information. You can see the instance running within your AWS GUI Console.

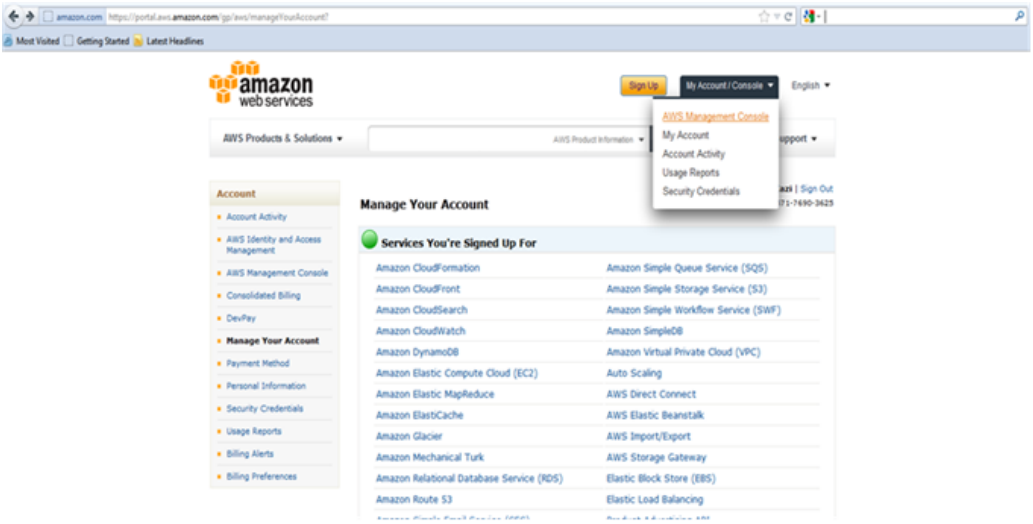
Note: Make sure that the environment variable EC2_URL points to the region where you want to launch the VPX instance.

To access the EC2 instance

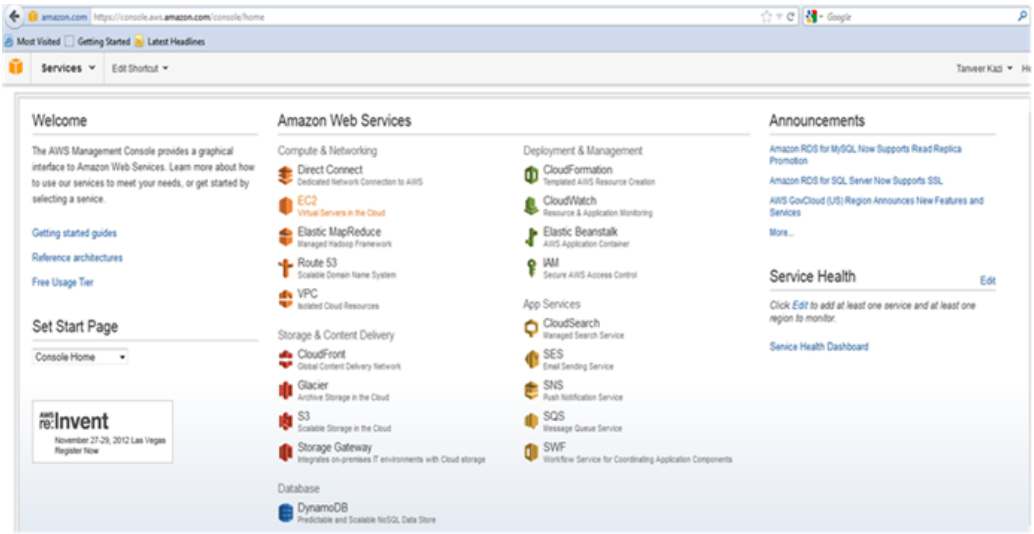
1. In a web browser, open the website at www.aws.amazon.com and log on with AWS credentials.



2. Click My Account/Console, and then click AWS Management Console.

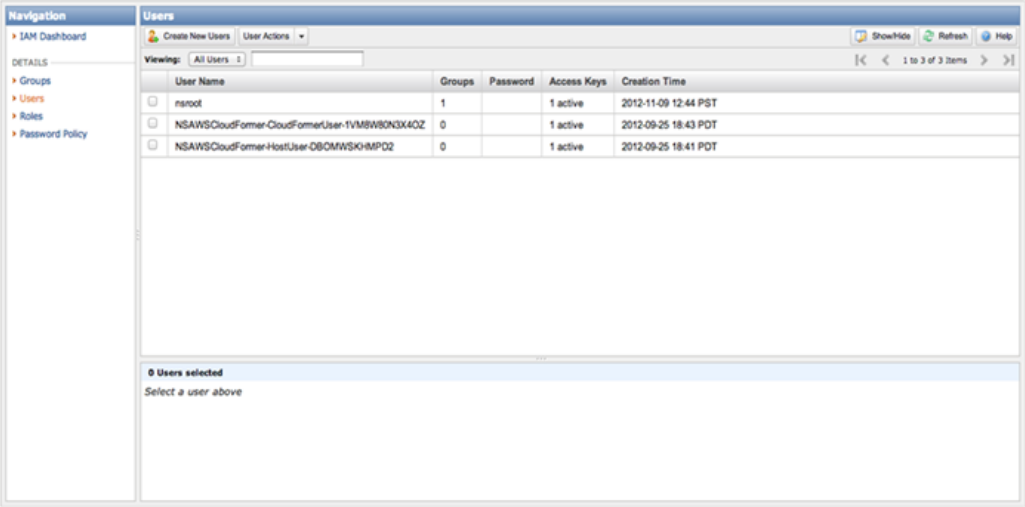


3. On the Amazon Web Services page, click EC2.



4. On the Amazon EC2 Console Dashboard page, in the Navigation pane, click Instances and verify that all of the NetScaler VPX instances are configured with the IP addresses that you specified when you used the ec2-run-instances command.

   Note: The VPX instance or instances can take from five to ten minutes to start running.



The ec2-run-instances command does not allow associating AWS elastic IP with an ENI. To associate one or more EIPs with an ENI in the Navigation pane, in the NETWORK & SECURITY area, click Elastic IPs and associate EIPs with Private IP addresses for any of the VIPs that need to be externally routable.

You must also associate the instance ENIs with appropriate security groups. Go to the Network Interfaces section, right-click on the individual ENI, and select the Change Security Groups option. You can then associate a proper VPC security group.

Using the Citrix CloudFormation Template to launch CloudBridge VPX for AWS

Using the Citrix Cloud Formation Template to launch NetScaler VPX for AWS

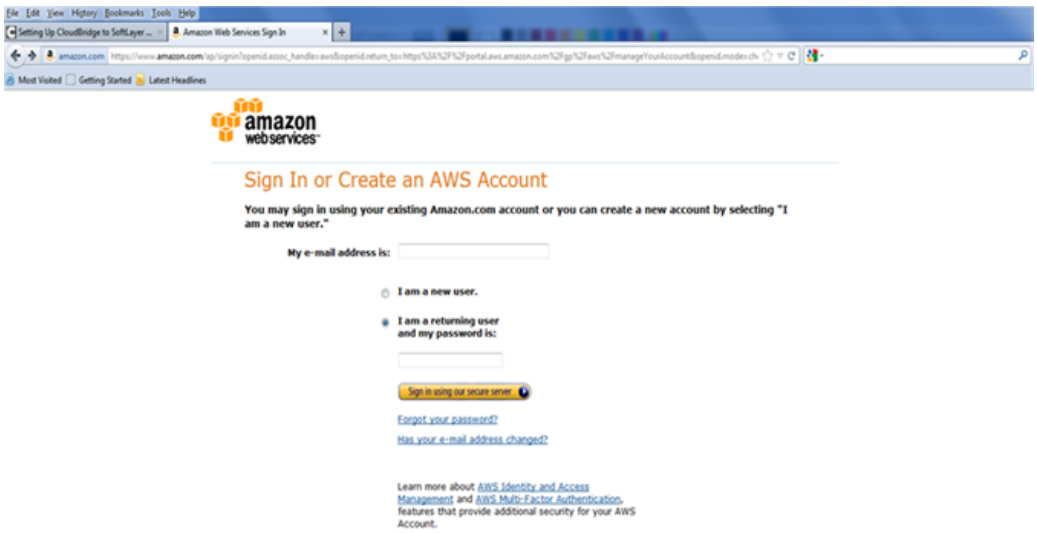
Citrix also provides a CloudFormation template that can be used to automate NetScaler instance launch. The tool requires an existing VPC environment. It launches a NetScaler instance with three ENIs. Therefore, to use the CloudFormation template, make sure that you have the following:

1. AWS account
2. AWS VPC
3. Three subnets within the VPC
4. A security group to use for the NetScaler instances ENIs

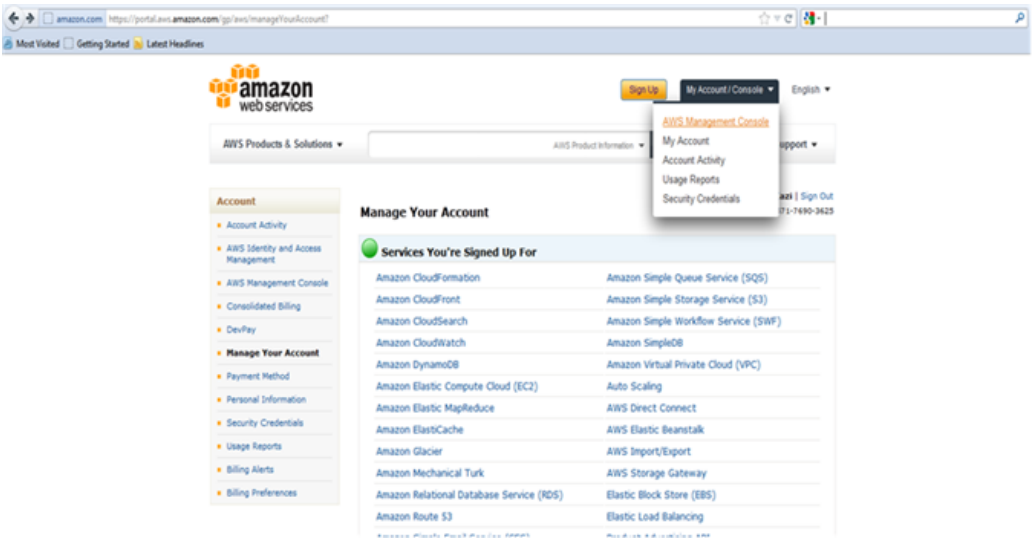
Refer to Creating an AWS Virtual Private Cloud (VPC) for information about how to configure subnets and security groups within a VPC. After configuring the required subnets and security groups, you can launch the NetScaler VPX AMI in AWS VPC. The CloudFormation tool provides functionality to launch a single NetScaler VPX instance or, to create a high availability environment, a pair of NetScaler VPX instances.

Launching a single NetScaler VPX instance in AWS

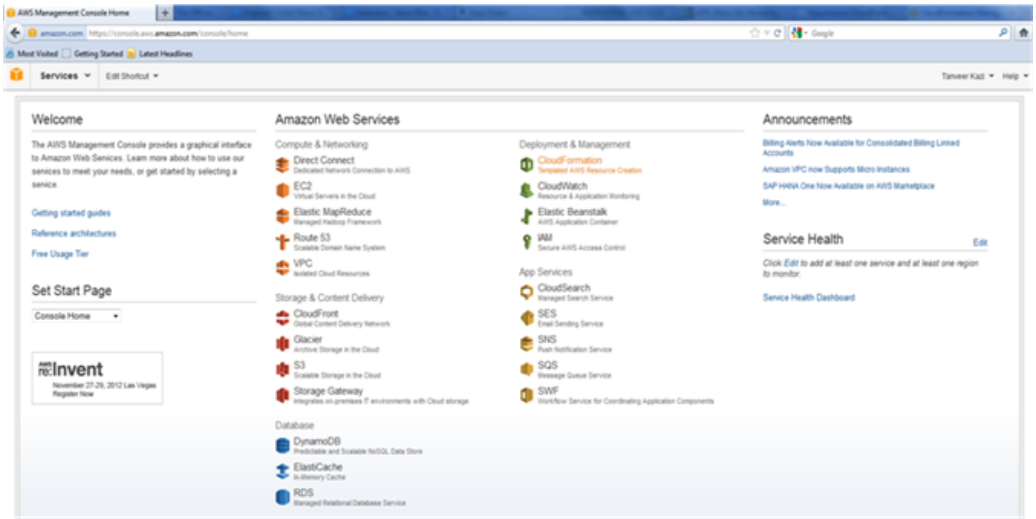
1. In a web browser, open the website at www.aws.amazon.comand log on with AWS credentials.



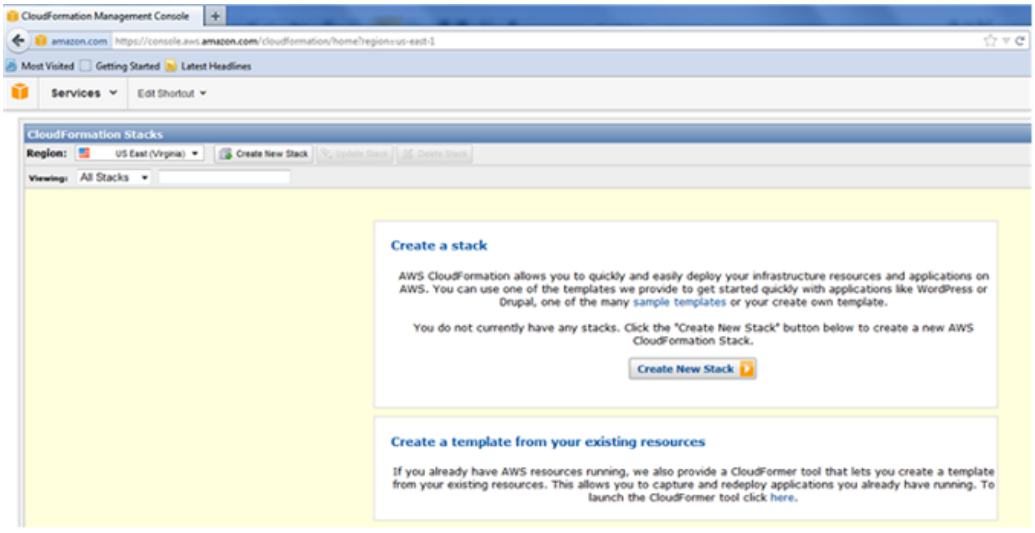
2. Click My Account/Console, and then click AWS Management Console.



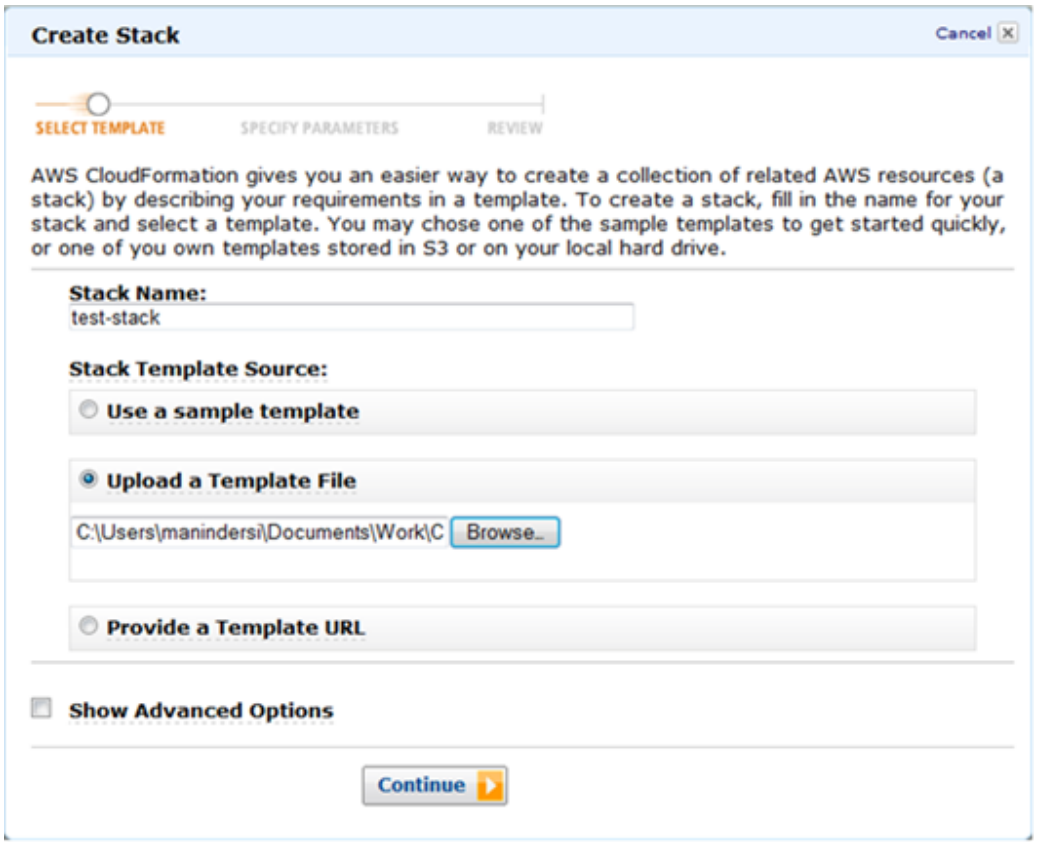
3. On the Amazon Web Services page, click Cloud Formation in the Deployment & Management section.



4. On the CloudFormation Stacks page, select the Region in which you plan to deploy the NetScaler VPX instance, and then click Create New Stack.



5. In the Create Stack dialog box, specify a value for Stack Name, select the Upload a Template File option, and then click Browse. Select the template for a standalone NetScaler VPX from the local drive, and then click Continue.



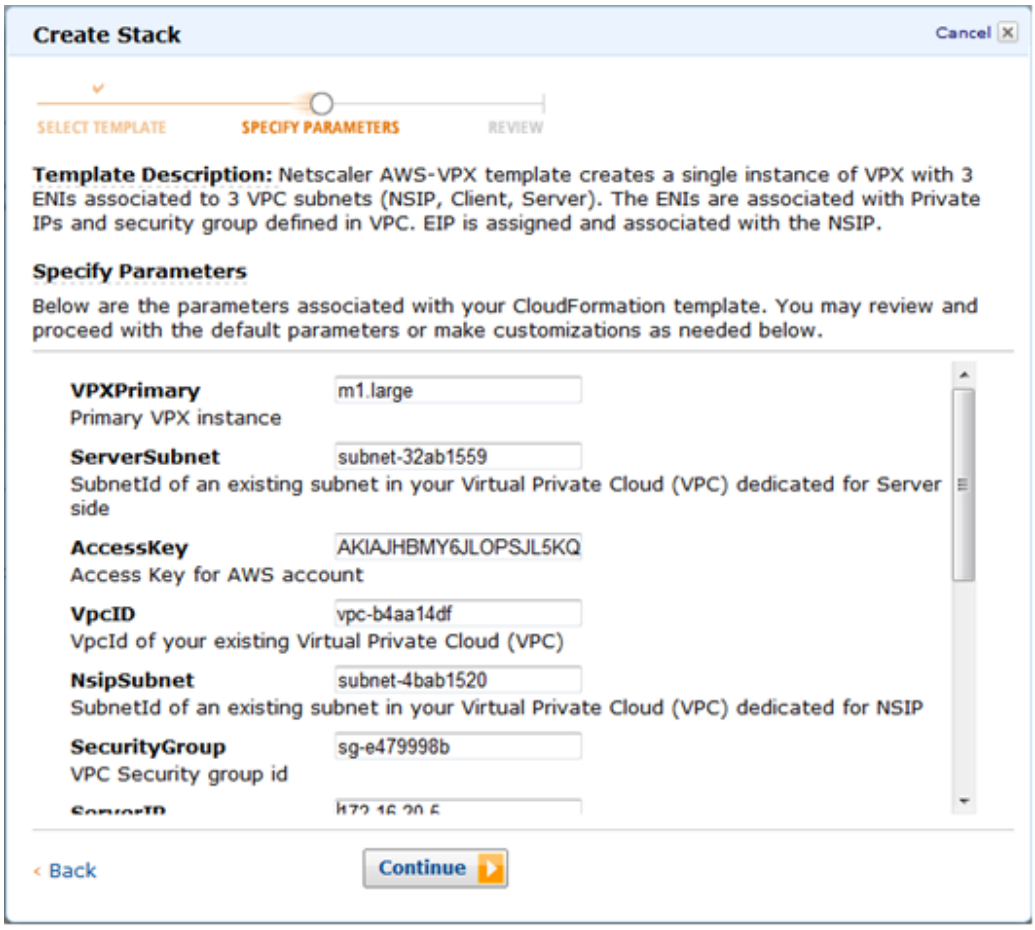
Note:

6. In the next pane, specify values for:

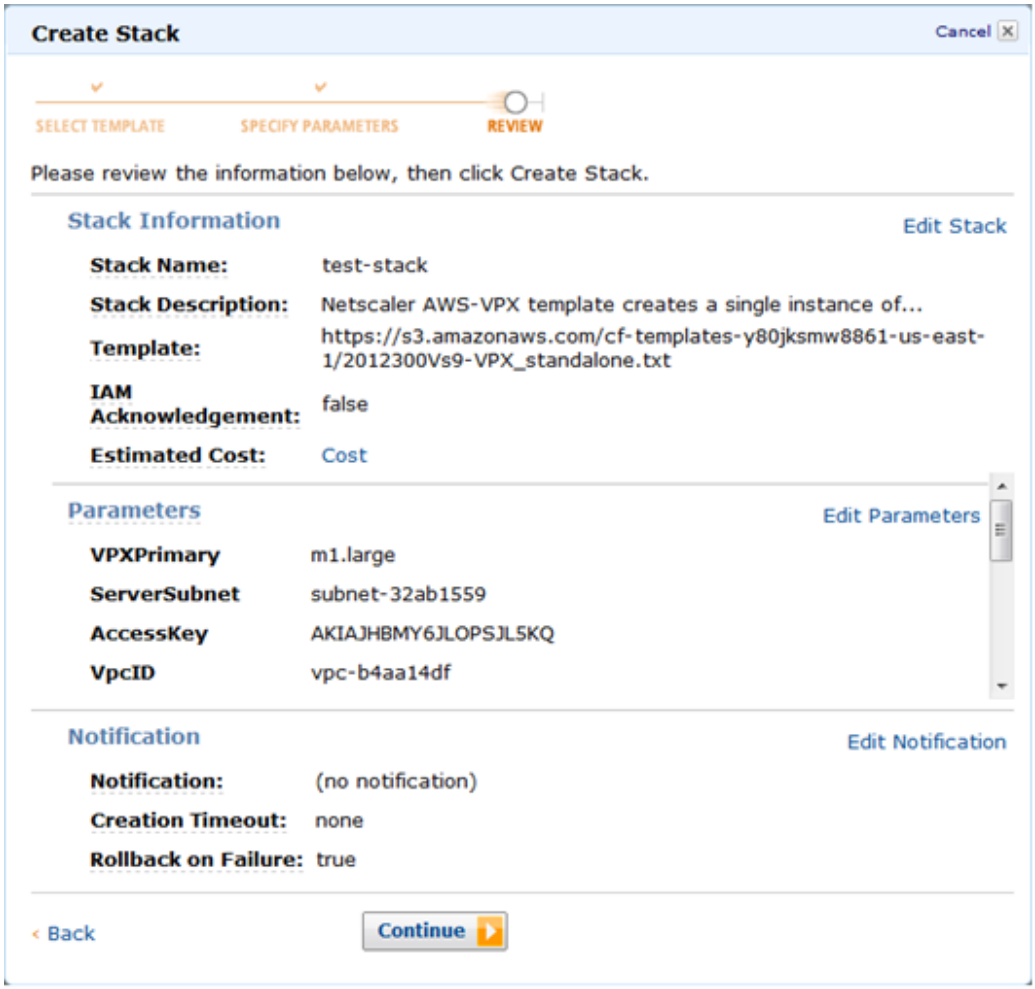
   - **VpcID** : An identifier to assign to the Virtual Private Cloud (VPC).
   - **NsipSubnet** : Subnet in which the NSIP is configured in the VPC
   - **ServerSubnet**: Subnet in which the server farm is configured in the VPC
   - **ClientSubnet**: SubnetId in which the client side is configured in the VPC
   - **SecurityGroup**: VPC Security group ID
   - **VPXPrimary**: Name of the primary VPX instance type
   - **AccessKey**: Access Key for IAM user account
   - **SecretKey**: Secret Key for IAM user account
   - **TenancyType**: Instance tenancy type, can be default or dedicated
   - **NsIP**: Private IP assigned to the NSIP ENI. The last octet of NSIP should be between 5 and 254.

- **ServerIP**: Private IP assigned to the Server ENI. The last octet should be between 5 and 254.
- **ClientIP**: Private IP assigned to the Client ENI. The last octet should be between 5 and 254.
- **KeyName**: Name of an existing EC2 KeyPair to enable SSH access to the instances.

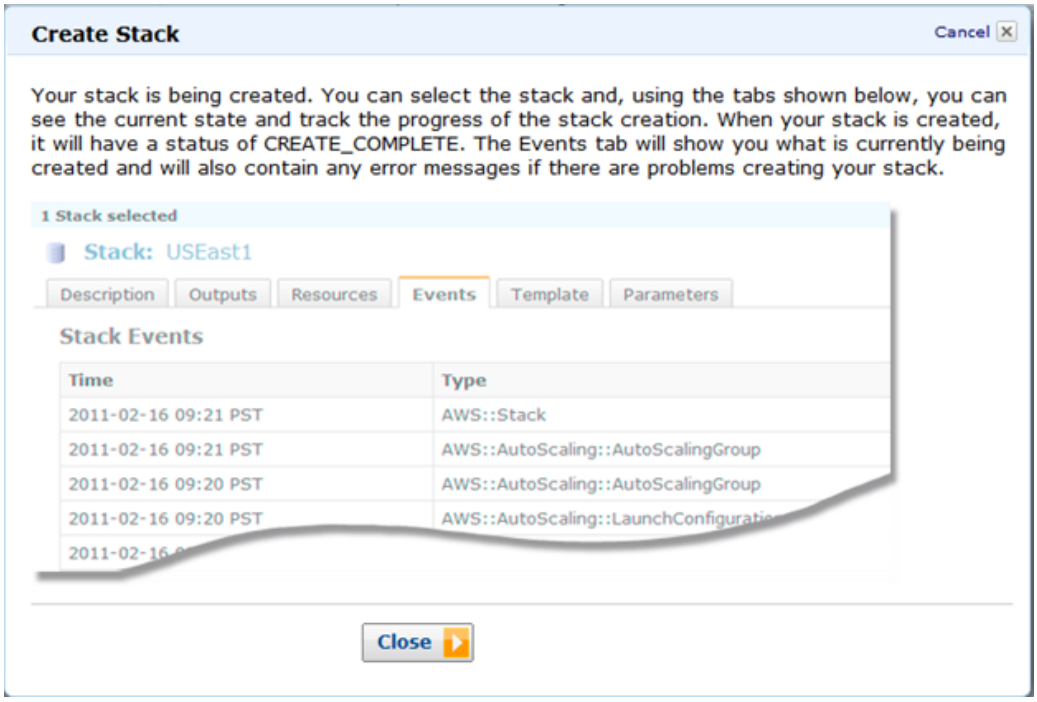
Note: Make sure that the VPC, subnets, security groups, routes and gateway associations are already configured.



7. Click Continue.
8. Review the values in the Create Stack dialog box.



9. Click Continue to create a Stack.



10. Click Close to close the Create Stack dialog box.

11. The new stack that you created appears on the CloudFormation Stacks page.

Note:

- Currently, the CloudFormation utility does not provide the functionality to add secondary IP addresses. Use the AWS console, after deploying a NetScaler VPX instance, to add the secondary IP addresses to the ENIs.
- The CloudFormation scripts for the standalone and HA pair VPX instances have the latest AMIs for the five supported regions. You have to update the scripts to synchronize with the latest AMIs.
- The script automatically selects the correct AMI for the region in which the VPX instance is being deployed.
- By default, all the ENIs are attached to one security group, use the AWS console to attach an ENI to a different security group.
- EIPs are automatically allocated and assigned to an instance. If the EIP limit exceeds the threshold for the region, the CloudFormation script fails and displays an error message.

Collaborating to Deliver High-Quality Products and Content Launching NetScaler VPX by using the AWS 1-Click

1-Click helps you to launch an instance of NetScaler VPX on AWS, quickly as compared to other launching methods, with the default options. After the instance is launched on AWS, you can modify these options by using either the AWS CLI or the AWS GUI.

The default options include the following elastic network interfaces (ENIs) for the NetScaler instance:

- **Management Interface**—Associates a subnet for management related traffic. You add the NetScaler management IP (NSIP) address to this subnet.
- **Public Interface**—Associates a subnet for the client-access (user-to-NetScaler) traffic. You add one or more virtual IP (VIP) addresses on this subnet.
- **Private Interface**—Associates a subnet for server-access (NetScaler-to-server) traffic. You add subnet IP (SNIP) addresses on this subnet.

Before you begin launching an instance of NetScaler VPX on AWS, consider the following points :

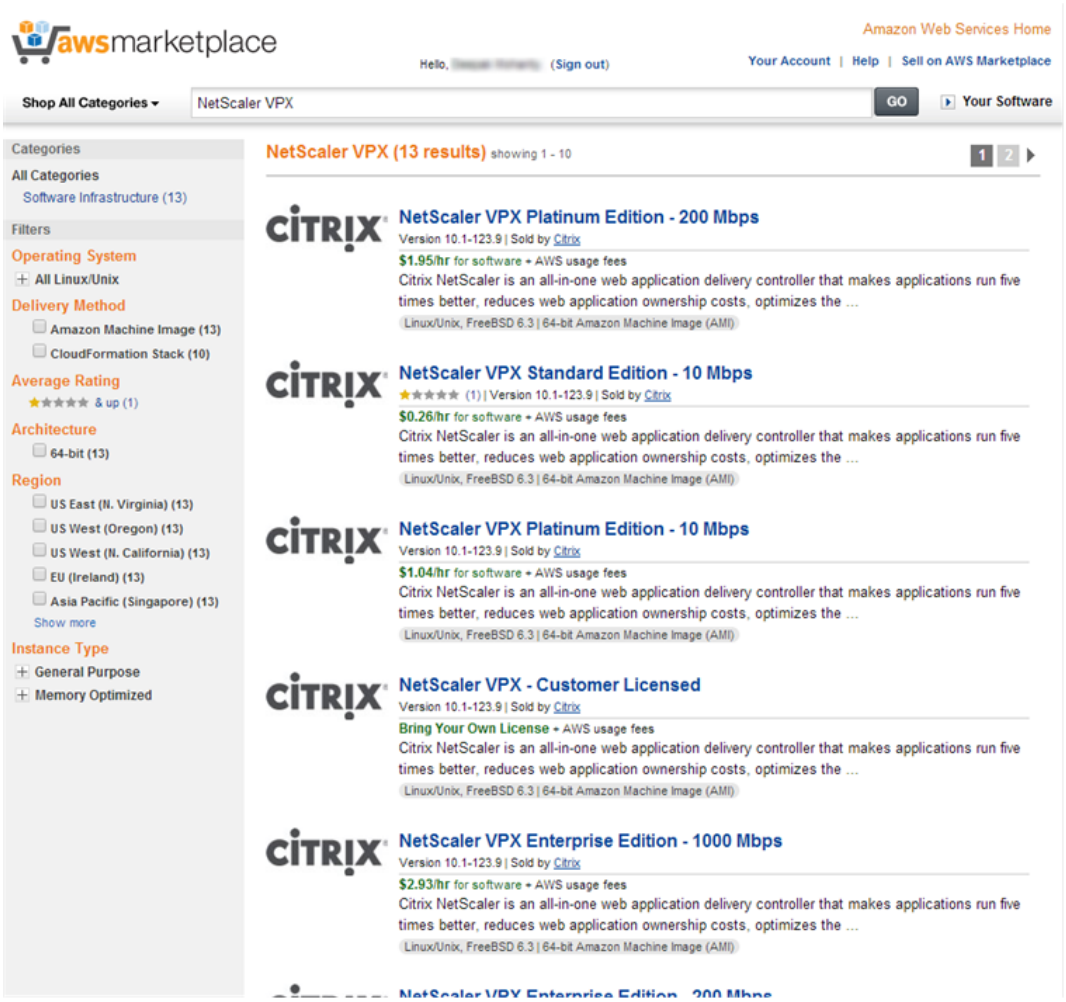
- For security reasons, none of the elastic IP addresses are attached to the ENIs of the NetScaler VPX instance launched by using 1-Click. This means that the NetScaler VPX instance (including the management IP address) is not reachable from outside the AWS Virtual Private Cloud (VPC). If your VPC uses a Virtual Gateway or other method to provide a VPN access to the VPC, you can administer the instance by using the IP address of the network interface in the management subnet. If you do not have VPN access to your VPC, Citrix recommends that you set up a jump box instance within the VPC, and then use this as the source for accessing or managing other instances within the VPC. For instructions to create an SSH jump box, see https://s3.amazonaws.com/awsmp-usageinstructions/Creating_and_using_VPC.txt.
- Three default security policies are created. A policy each is attached to the management, public and private interfaces, respectively.
    - The security policy for the management interface allows traffic from a set of ports.
    - The security policies for the public and private interfaces block all the traffic to or from these interfaces. You can later modify these security groups to filter the desired traffic.
- High Availability configuration is not supported for a NetScaler VPX instance launched by using AWS 1-click.

Before you begin launching an instance of NetScaler VPX on AWS, make sure that you have the following:

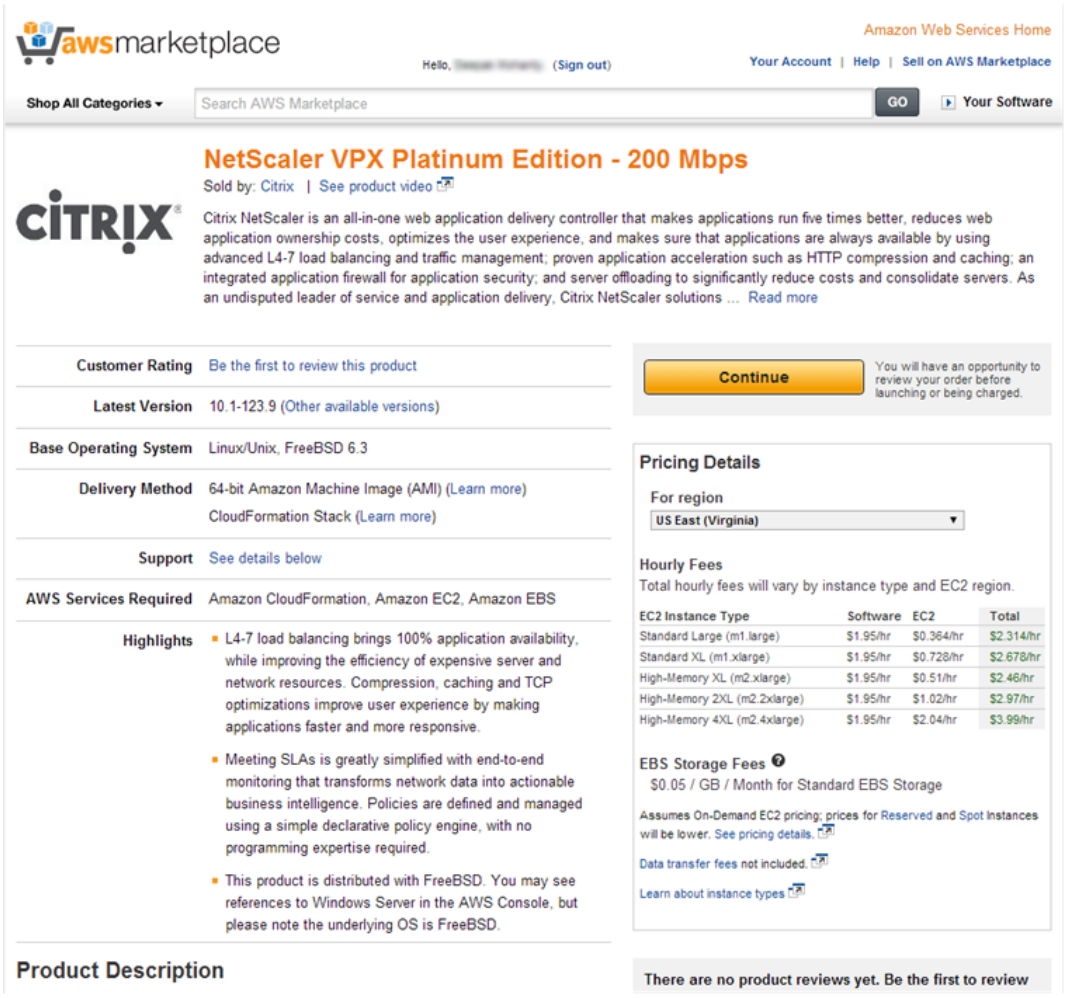
- An AWS account
- An AWS Virtual Private Cloud (VPC)
- Three subnets within the AWS VPC (one each for management interface, public interface, and private interface of the NetScaler instance)
- An IAM key pair

For information about creating an AWS account, a VPC, subnets in a VPC, and an IAM key pair, see Launching NetScaler VPX for AWS by Using the Amazon GUI and CLI toolkit.

To launch an instance of NetScaler VPX on AWS by using 1-Click

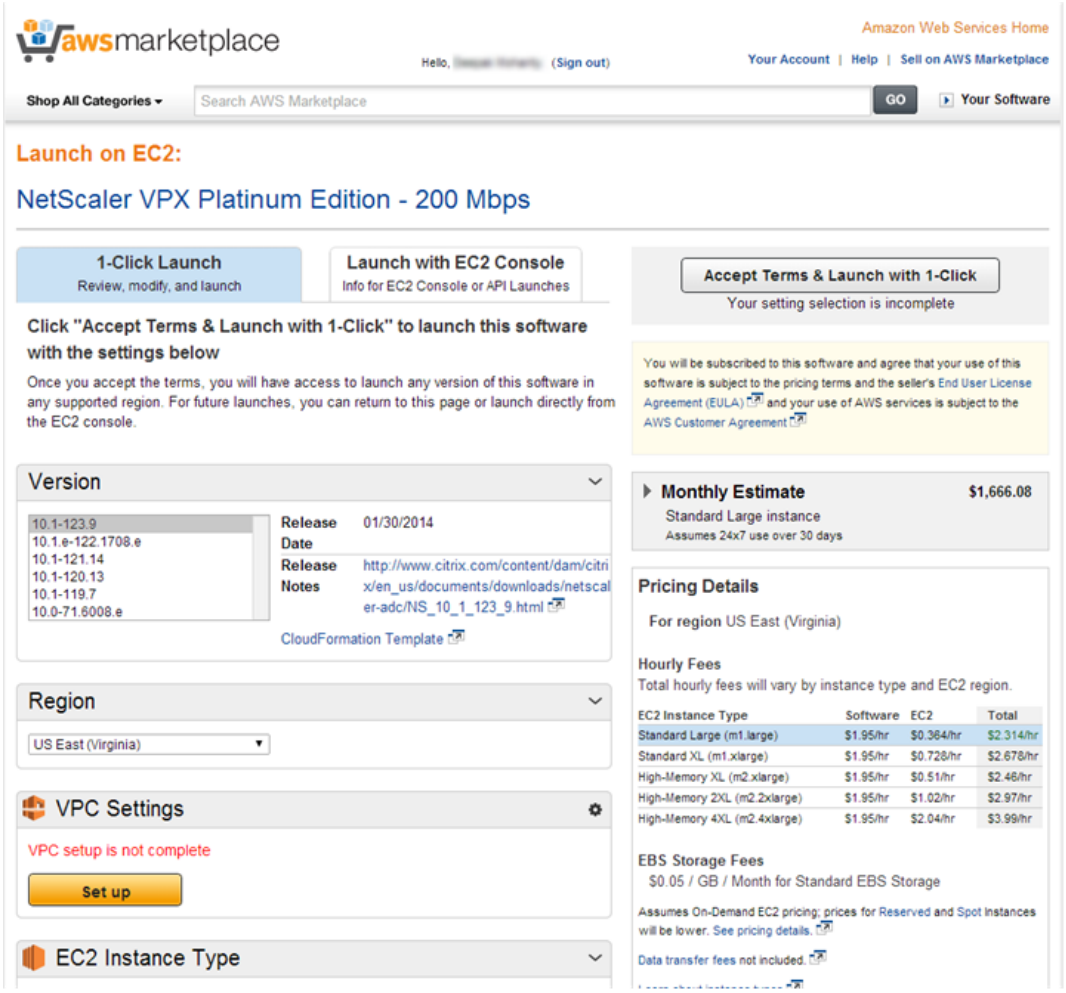
1. Log on to the AWS marketplace (https://aws.amazon.com/marketplace) by using your Amazon AWS credentials.
2. In the search field, type NetScaler VPX to search for the NetScaler AMI, and click Go.
3. 

On the search result page, click the desired Citrix NetScaler VPX offering.

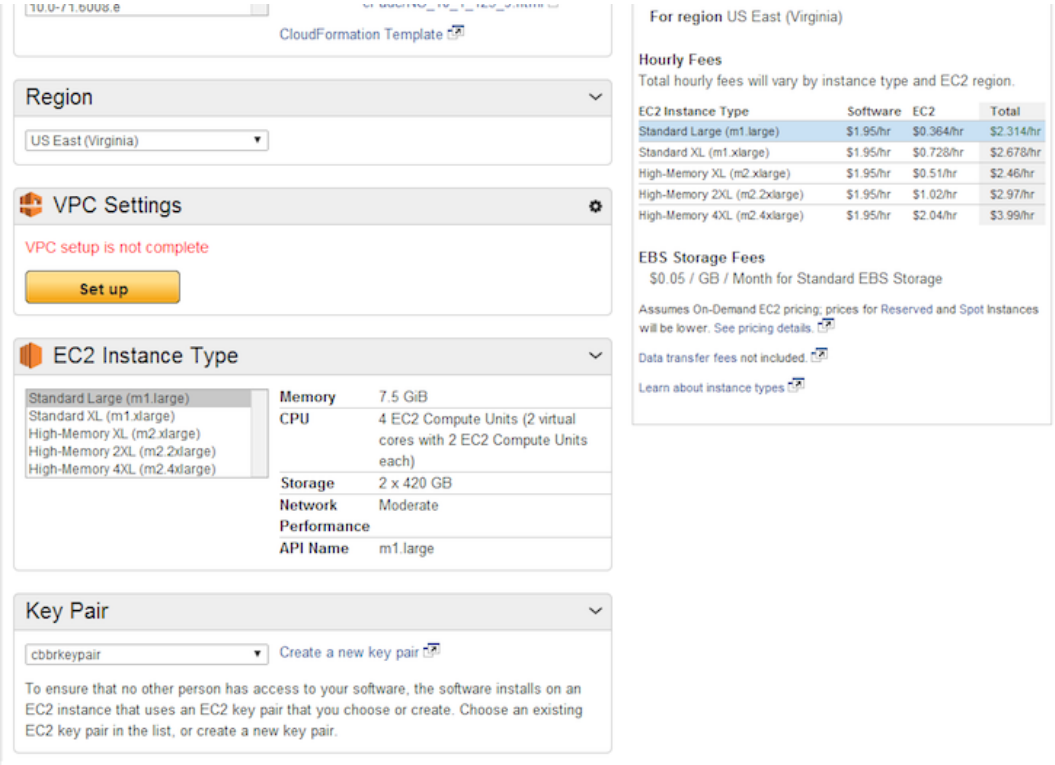
4. 

   On the Citrix NetScaler VPX page, click Continue.
5. Click the 1-Click Launch tab. On the 1-Click Launch tab, specify values for the following fields:

   - Version
   - Region
   - EC2 Instance type
   - Key Pair



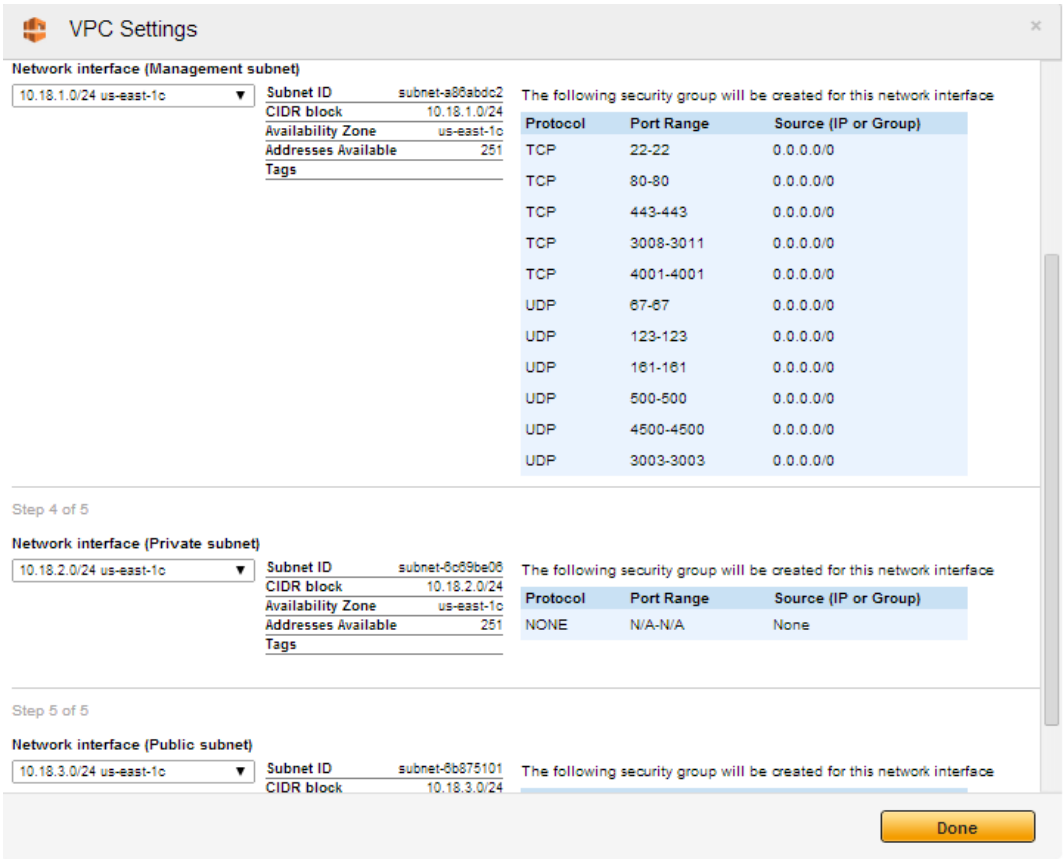
6. On the VPC Settings pane, click Setup.

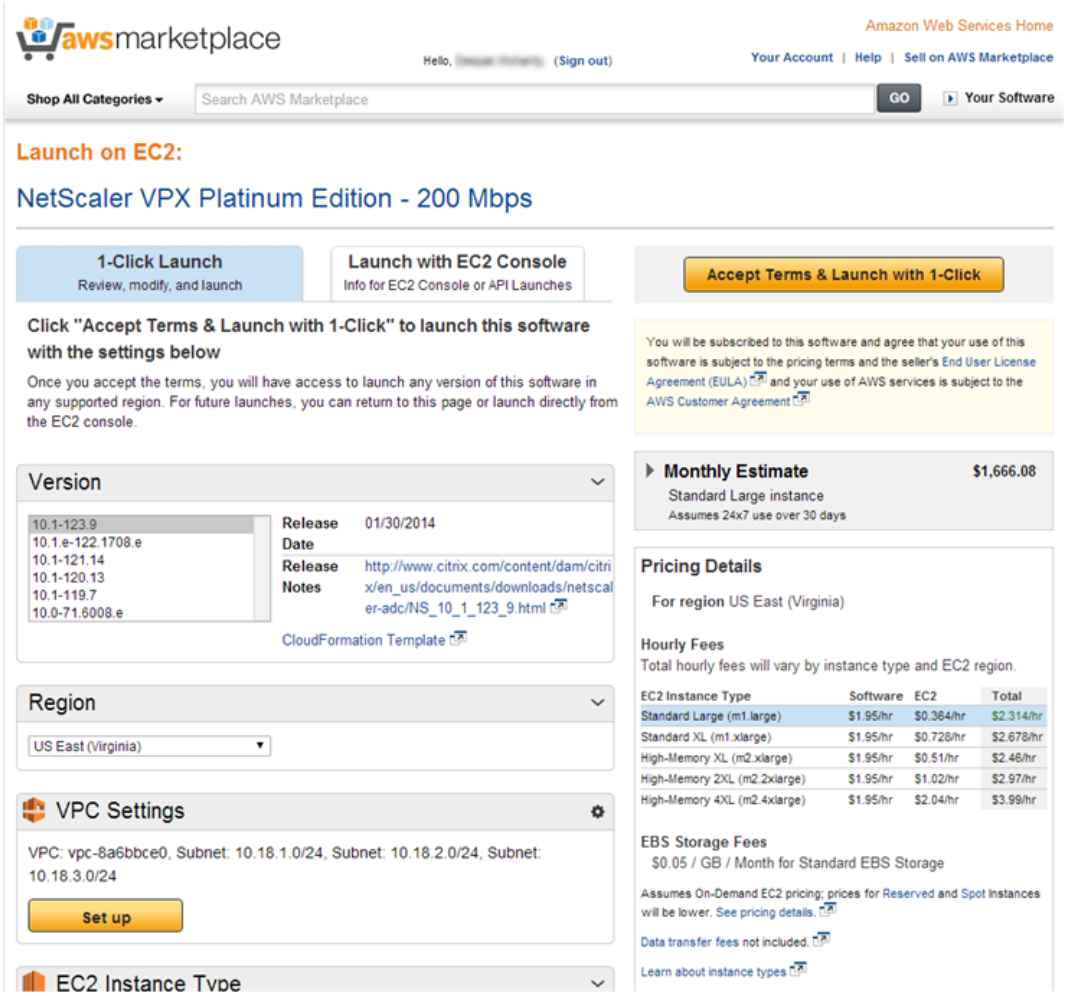


7. On the VPC Settings page, specify values for the following fields, and then click Done:

   - VPC
   - Network Interface (Management subnet)
   - Network Interface (Private subnet)
   - Network Interface (Public subnet)

   Note: You need to make sure that the subnets attached to these ENIs are different from each other. Attaching the same subnet to more than one ENI might cause routing issues.


VPC Settings
Network interface (Management subnet)
10.18.1.0/24 us-east-1c
Subnet ID subnet-a86abdc2
CIDR block 10.18.1.0/24
Availability Zone us-east-1c
Addresses Available 251
Tags
The following security group will be created for this network interface
Protocol Port Range Source (IP or Group)
TCP 22-22 0.0.0.0/0
TCP 80-80 0.0.0.0/0
TCP 443-443 0.0.0.0/0
TCP 3008-3011 0.0.0.0/0
TCP 4001-4001 0.0.0.0/0
UDP 67-67 0.0.0.0/0
UDP 123-123 0.0.0.0/0
UDP 161-161 0.0.0.0/0
UDP 500-500 0.0.0.0/0
UDP 4500-4500 0.0.0.0/0
UDP 3003-3003 0.0.0.0/0
Step 4 of 5
Network interface (Private subnet)
10.18.2.0/24 us-east-1c
Subnet ID subnet-6c69be06
CIDR block 10.18.2.0/24
Availability Zone us-east-1c
Addresses Available 251
Tags
The following security group will be created for this network interface
Protocol Port Range Source (IP or Group)
NONE N/A-N/A None
Step 5 of 5
Network interface (Public subnet)
10.18.3.0/24 us-east-1c
Subnet ID subnet-6b875101
CIDR block 10.18.3.0/24
The following security group will be created for this network interface
Done

8. 

Click Accept Terms & Launch with 1-Click.

After few minutes, the NetScaler instance is launched with three ENIs. You can now connect to the NSIP address (the IP address on the management ENI) of the instance by using the NetScaler CLI or NetScaler GUI and start configuring the NetScaler features, for example, load balancing.

Verifying the NetScaler VPX on AWS Installation

When the NetScaler instance is running, you can access the instance through the NetScaler GUI or the NetScaler CLI by connecting to the EIP associated with the management ENI (NSIP). For example, use the following addressing notation in a web browser:

http://<Elastic_IP> (unsecured access)

or

https://<Elastic_IP> (secured access)

Note:

- To access a NetScaler instance through SSH, provide the .pem file.
- You can use the AWS GUI console to manually add the private IP addresses for SNIPs on server subnets and VIPs on client subnets.
- If you want to access the NSIP from the Internet, you must assign an EIP to the NSIP address of each NetScaler instance. Also, make sure that the NSIP subnet is associated with a routing table that has a default route set to the Internet gateway.
- If you want VIP addresses to be accessible through the Internet, you must associate an EIP with each VIP address that is defined in the configuration.
- The following are the default login credentials to access a NetScaler instance:
  - Username—nsroot
  - Password—nsroot

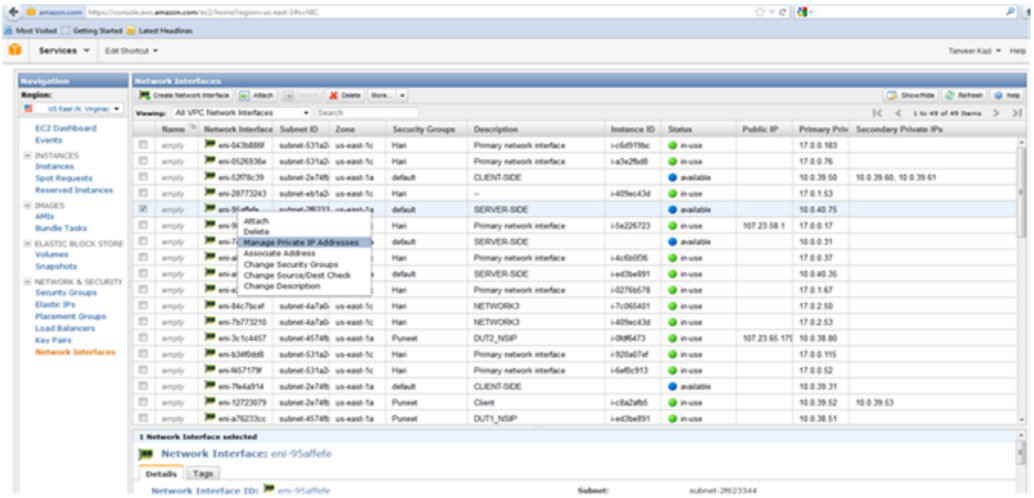
Attaching Additional IP Addresses to an Instance

You can attach additional IP addresses to an instance as follows:

1. Add a secondary IP address to an ENI.
2. Associate an EIP with the secondary IP address that you created.

To add a secondary IP address to the ENI

1. In a web browser, open the website at www.aws.amazon.com and log on with AWS credentials.
2. Click My Account/Console, and then click AWS Management Console.
3. On the Amazon Web Services page, click EC2.
4. On the Amazon EC2 Console's Dashboard page, in the Navigation pane, in NETWORK & SECURITY, click Network Interfaces.
5. In the Network Interfaces pane, right-click the ENI attached to the subnet, and then select the Manage Private IP Addresses option from the pop-up menu.



6. In the Manage Private IP Addresses dialog box, click Assign a secondary private IP address and either let AWS automatically assign an IP address or type an IP address in the auto-assign text-field. Click Yes, Update.

Associating an EIP with the secondary IP

Complete the following steps to associate an EIP with a secondary IP address:

1. On the Amazon EC2 Console Dashboard page, in the Navigation pane, in NETWORK & SECURITY, click Elastic IPs.
2. In the Addresses pane, click Allocate New Address.
3. In the Allocate New Address dialog box, select VPC from the EIP used in drop-down list and click Yes, Allocate.
4. Select the newly allocated EIP, and click Associate Address.
5. In the Associate Address dialog box, select, from the **Instance** and the **Private IP address** drop-down lists, the instance and private address that you want to associate with the EIP. Then, click Yes, Associate.

Downloading a NetScaler VPX License

After the initial instance launch, NetScaler VPX for AWS requires a license. If you are bringing your own license (BYOL), see the *VPX Licensing Guide* at http://support.citrix.com/article/CTX122426

You have to:

1. Use the licensing portal within MyCitrix to generate a valid license.
2. Upload the license to the instance.

If this is a **paid** marketplace instance, then you do not need to install a license. The correct feature set and performance will activate automatically.

Load Balancing Servers in different Availability Zones

A NetScaler instance can be used to load balance servers running in the same availability zone, or in:

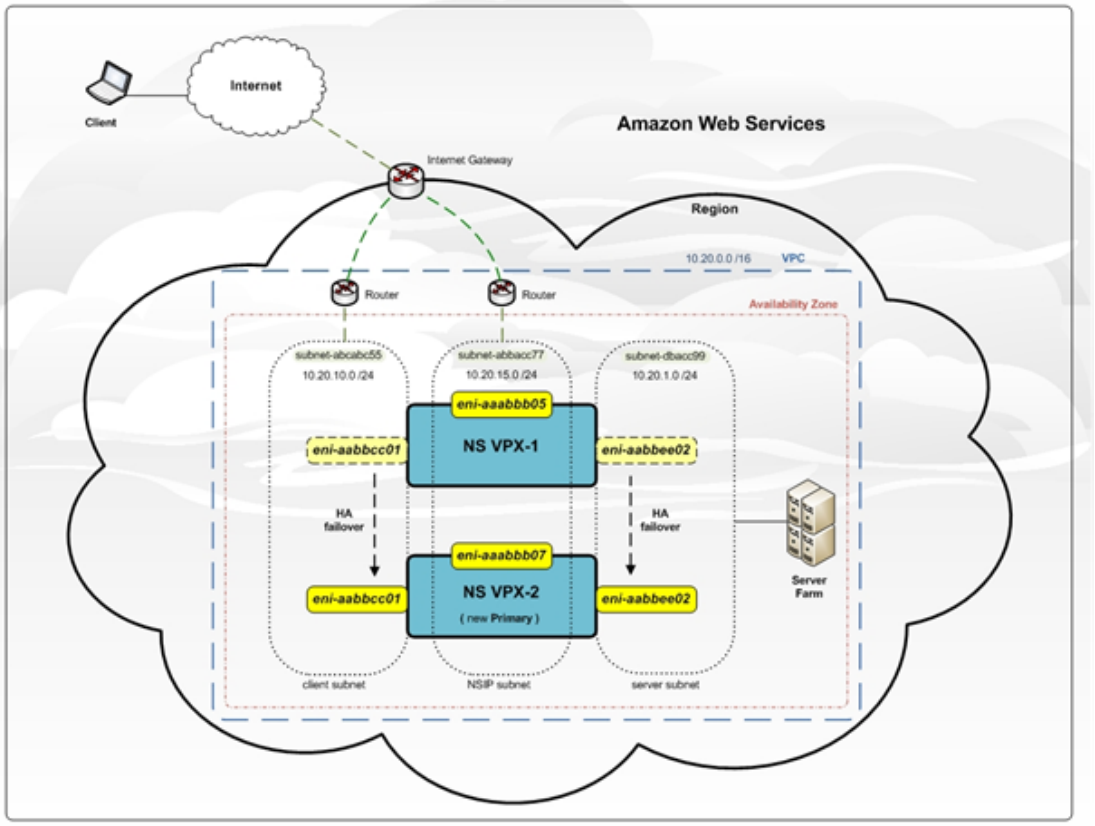
- A different availability zone (AZ) in the same AWS VPC
- A different AWS region
- AWS EC2 in a VPC

To enable NetScaler to load balance servers running outside the AWS VPC that the NetScaler instance is in, configure the NetScaler to use EIPs to route traffic through the Internet gateway, as follows:

1. Configure a SNIP on the NetScaler by using the NetScaler CLI or the NetScaler GUI
2. Enable traffic to be routed out of the AZ, by creating a public facing subnet for the server-side traffic.
3. Add an Internet gateway route to the routing table, using the AWS GUI console.
4. Associate the routing table you just updated with the server-side subnet.
5. Associate an EIP with the server-side private IP address that is mapped to a NetScaler SNIP address.

High Availability

Two Citrix® NetScaler® VPX™ instances in AWS can be configured as a high availability (HA) pair. With one instance configured as the primary node and the other as the secondary node, the primary node accepts connections and manages servers while the secondary node monitors the primary. If, for any reason, the primary node is unable to accept connections, the secondary node takes over.



The following figure shows an example of the HA deployment architecture for NetScaler VPX on AWS. Figure 1. NetScaler VPX on AWS - HA Deployment

To deploy HA for VPX on AWS, you must configure at least two ENIs on the primary instance and a single ENI on the secondary instance. On each instance, configure the NetScaler IP (NSIP) address (the management address) on the default ENI. On the primary instance, use the additional ENIs for client and server connections.

For instructions on obtaining access and secret keys, in the AWS documentation, see "How Do I Get Security Credentials?" and "Creating, Modifying, and Viewing User Access Keys (AWS Management Console)." For instructions to create an IAM user and set permissions, see "Creating an IAM Account."

Example format for a key file is:

ACCESS_KEY="AKIAJPBBBBBBBVA2PR2OHJNA"
SECRET_KEY="d75KxU7ukd44444NNNNtrrAOgynwBdJoSiooP"

Note: For HA failover to work:

1. The NSIP addresses for each NetScaler instance in an HA pair must be configured on the default ENI of the instance.
2. Both the primary and secondary instances must have EIPs associated with the NSIP or NAT configured to handle outgoing traffic in order to have access to the AWS API servers.
3. Client and server traffic (data-plane traffic) must not be configured on the default ENI.
4. Access and secret keys associated with the user's AWS Identity and Access Management (IAM) account. If the correct key information is not used when creating VPX instances, the HA deployment will fail. The access and secret keys are required for sending Query APIs to the AWS server.
5. Nameservers/DNS servers are configured at VPC level using DHCP options.

Notes on HA:

- Because Amazon does not allow any broadcast/multicast packets in AWS, HA is implemented by migrating data-plane ENIs from the primary to the secondary (new primary) VPX instance when the primary VPX instance fails.
- To deploy HA for VPX on AWS, you must configure at least two ENIs on the primary instance and a single ENI on the secondary instance.
- Because the default ENI cannot be moved to another VPX instance, you should not use the default ENI for data.
- The message AWSCONFIG IOCTL NSAPI_HOTPLUG_INTF success output 0 indicates that the two data ENI's have successfully attached to the secondary instance (the new primary).
- Failover might take up to 20 seconds due to the AWS detach/attach ENI mechanism.
- Upon failover, the failed instance always restarts.
- The secondary node always has one ENI interface (for management) and the primary node can have up to four ENIs.
- The heartbeat packets are received only on the management interface.
- **The AWS debug messages are available in the log file, /var/log/ns.log, on the VPX instance**.

Configuring High Availability for VPX on AWS

To deploy HA for two VPX instances on AWS, you must create the primary NetScaler VPX instances with three ENIs and the secondary NetScaler VPX with a single ENI.

Following is an example of launching a primary VPX instance with three ENIs:

C:\aws-vpc-config>ec2-run-instances ami-bd2986d4 -n 1 -t m1.large -k keyPairName -f ./keyPairFile -a :0:subnet-15fa057e:"NSIP":10.20.15.21 -a :1:subnet-1547ba7e:"CLIENT-SIDE":10.20.10.21::::"10.20.10.22,10.20.10.23,10.20.10.24,10.20.10.25,10.20.10.26,10.20.10.27,10.20.10.28,10.20.10.29,10.20.10.30" -a :2:subnet-cc47baa7:"SERVER-SIDE":10.20.1.21::::"10.20.1.22,10.20.1.23,10.20.1.24,10.20.1.25,10.20.1.26,10.20.1.27,10.20.1.28,10.20.1.29,10.20.1.30"

Following is an example of launching a secondary VPX instance with a single ENI:

C:\aws-vpc-config>ec2-run-instances ami-bd2986d4 -n 1 -t m1.large -k keyPairName -f keyPairFile -a :0:subnet-15fa057e:"NSIP":10.20.15.31

Note: The keyPairFile argument contains the access and secret key. (You cannot change the keyPairFile associated with a VPC instance after it is created.)

After the two NetScaler instances are UP, configure the HA pairing on both the instances. You have to configure the instance with two or more ENIs before configuring HA on the instance with one ENI. Use the add HA node command, from within the NetScaler CLI, or from the NetScaler GUI. For example:

On the VPX instance with two or more ENIs:

add HA node 1 10.20.15.31

On the VPX instance with one ENI:

add HA node 1 10.20.15.21

After you enter add HA node commands, the two nodes form an HA pair, and configuration information is synchronized between the two VPX instances.

To remove HA from NetScaler VPX pair

You can remove HA configuration from the NetScaler VPX pair by using the remove ha node command. You have to remove the HA configuration from the secondary NetScaler VPX before removing the HA configuration from the primary NetScaler VPX.

For example, on the Secondary NetScaler VPX instance, at the NetScaler command line, type:

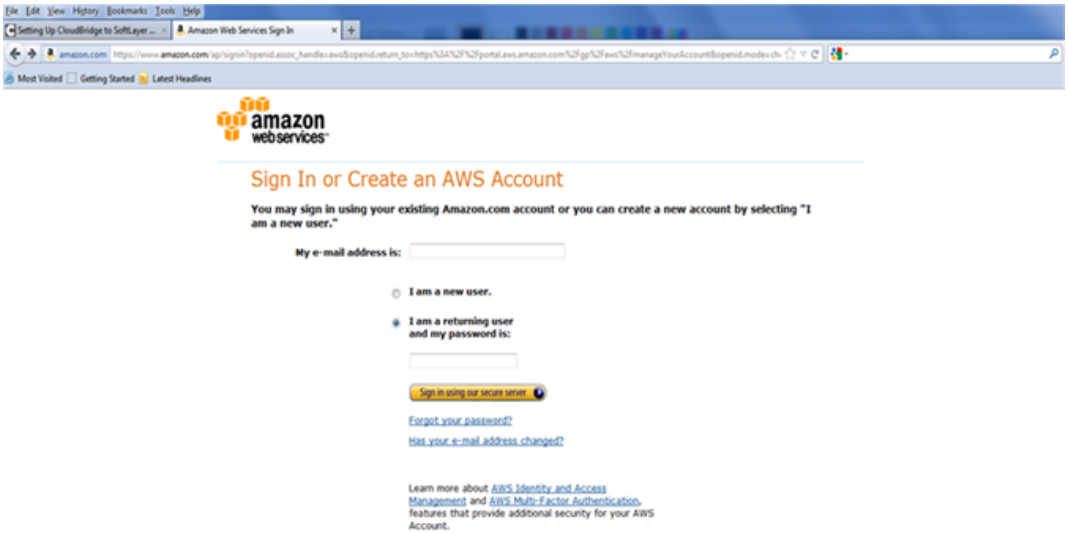
```
remove ha node

save config
```

On the Primary NetScaler VPX instance, at the NetScaler command line, type:

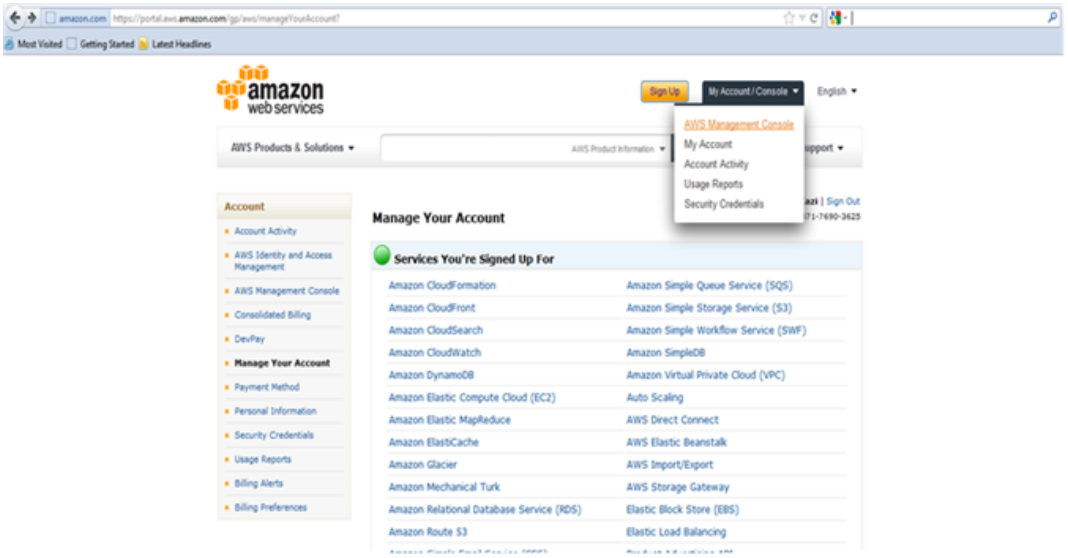
```
remove ha node

save config
```

Launching NetScaler VPX pairs for HA by using Citrix CloudFormation

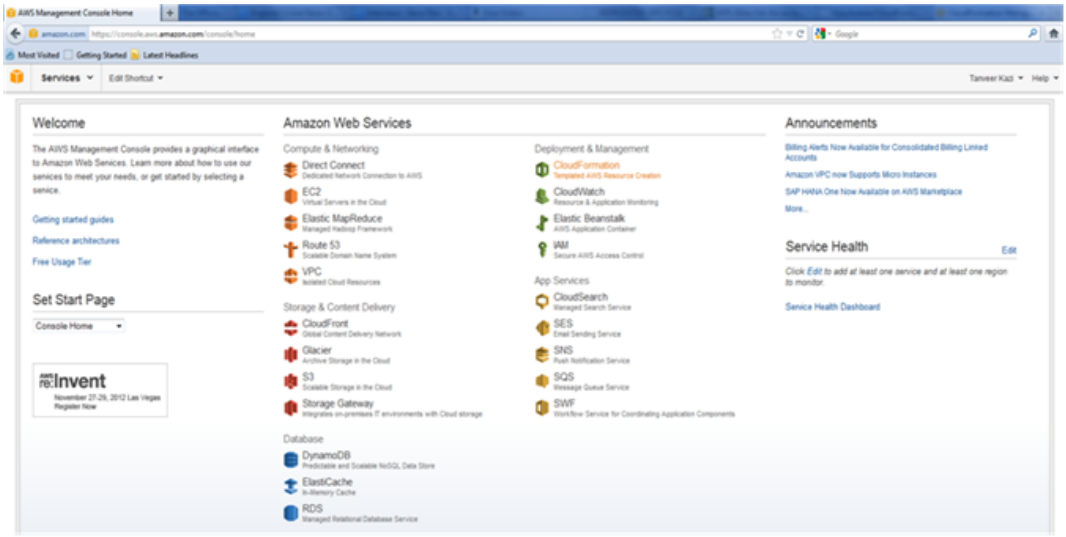
1. In a web browser, open the website at www.aws.amazon.com and log on with AWS credentials.



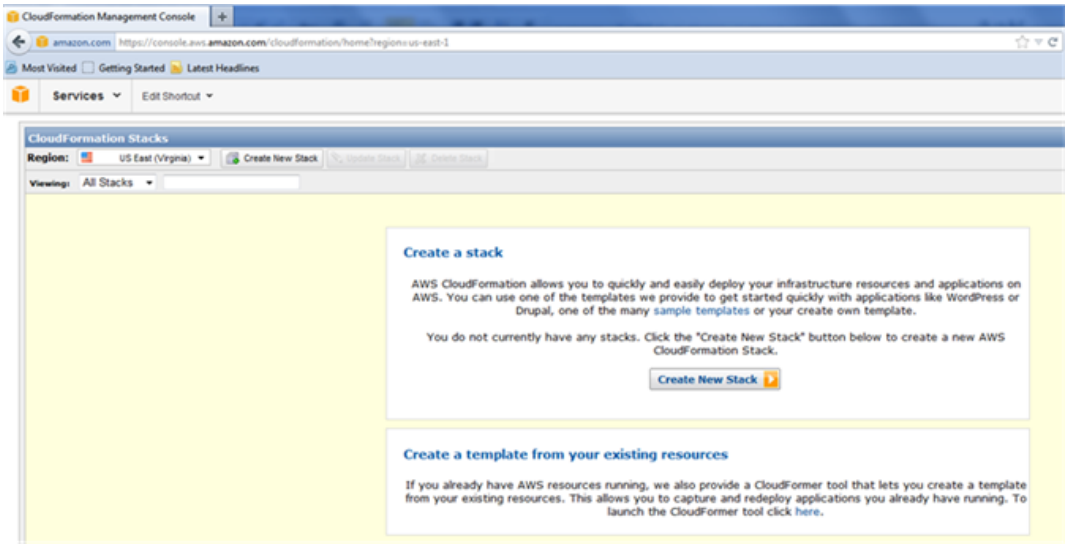
2. Click My Account/Console, and then click AWS Management Console.



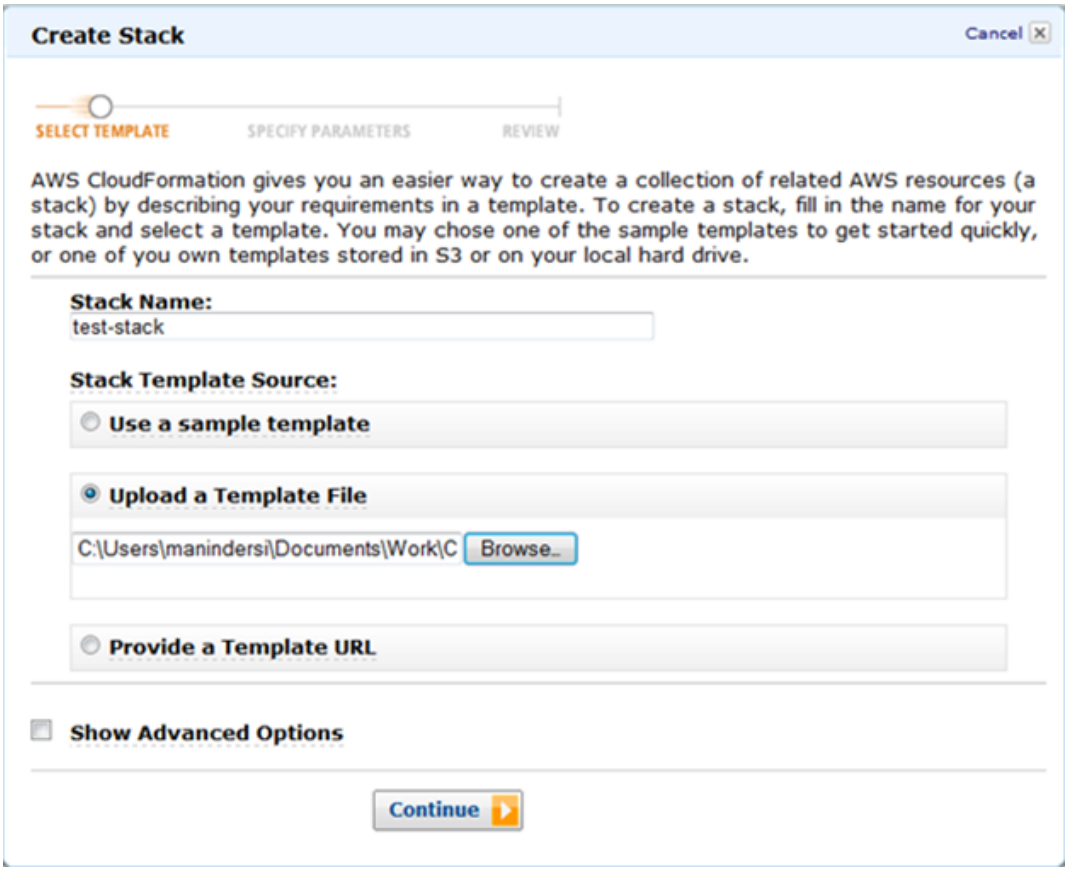
3. On the Amazon Web Services page, in the Deployment & Management section, click Cloud Formation.



4. On the CloudFormation Stacks page, select the Region in which you plan to deploy the NetScaler VPX instance, and then click Create New Stack.



5. In the Create Stack dialog box, specify value for Stack Name, select the Upload a Template File option, and then click Browse. Select the template for HA NetScaler VPX from the local drive, and then click **Continue**.



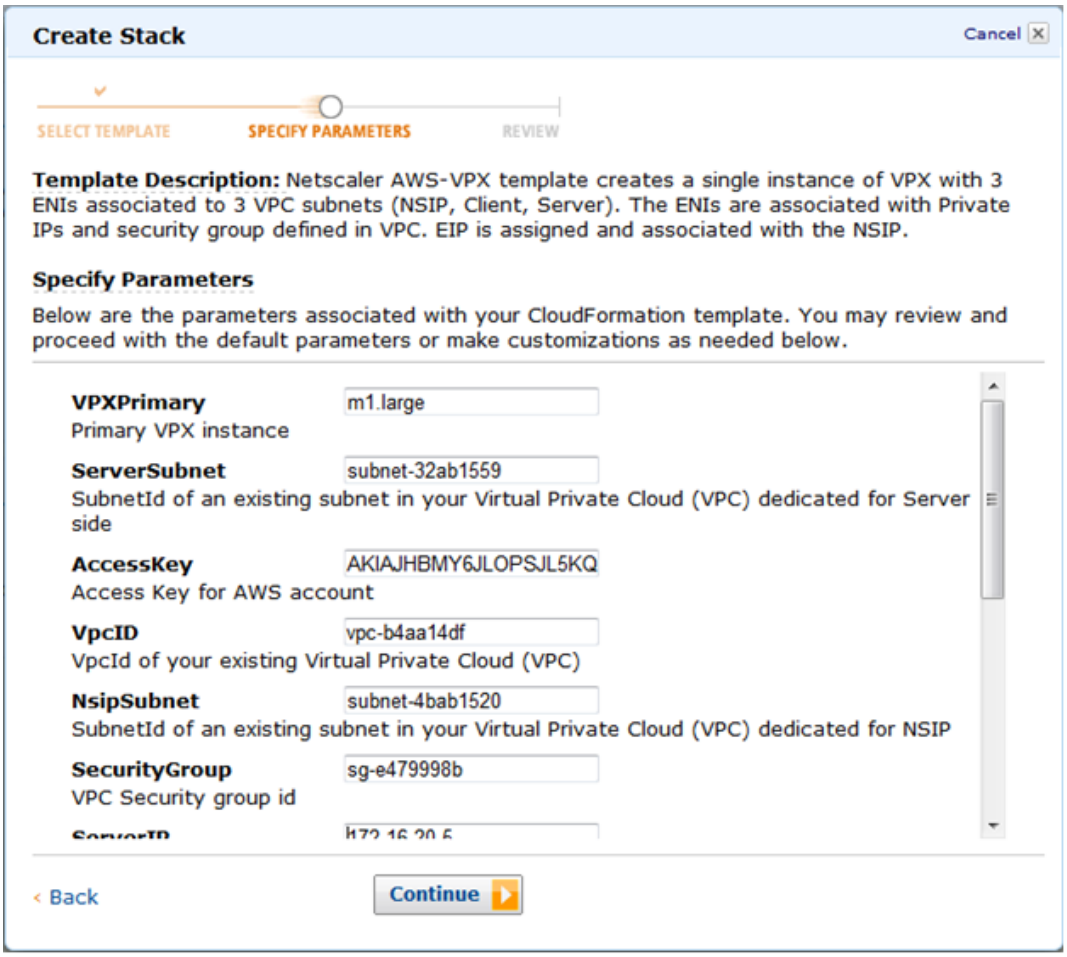
6. In the next pane, specify values for:

   - **VpcID**: An identifier to assign to the Virtual Private Cloud (VPC).
   - **NsipSubnet**: Subnet in which the NSIP is configured in VPC.
   - **ServerSubnet**: Subnet in which the server farm is configured in VPC.
   - **ClientSubnet**: SubnetId in which the client side is configured in VPC.
   - **SecurityGroup**: VPC Security group id.
   - **VPXPrimary**: Name of Primary VPX instance type.
   - **AccessKey**: Access Key for IAM user account.
   - **SecretKey**: Secret Key for IAM user account.
   - **TenancyType**: Instance tenancy type, can be default or dedicated.
   - **NsIP**: Private IP assigned to the NSIP ENI. The last octet of NSIP should be between 5 and 254.
   - **NsIPSec**: Private IP assigned to the NSIP ENI of Secondary. last octet has to be between 5 and 254.
   - **ServerIP**: Private IP assigned to the Server ENI. The last octet should be between 5 and 254.

- **ClientIP**: Private IP assigned to the Client ENI. The last octet should be between 5 and 254.

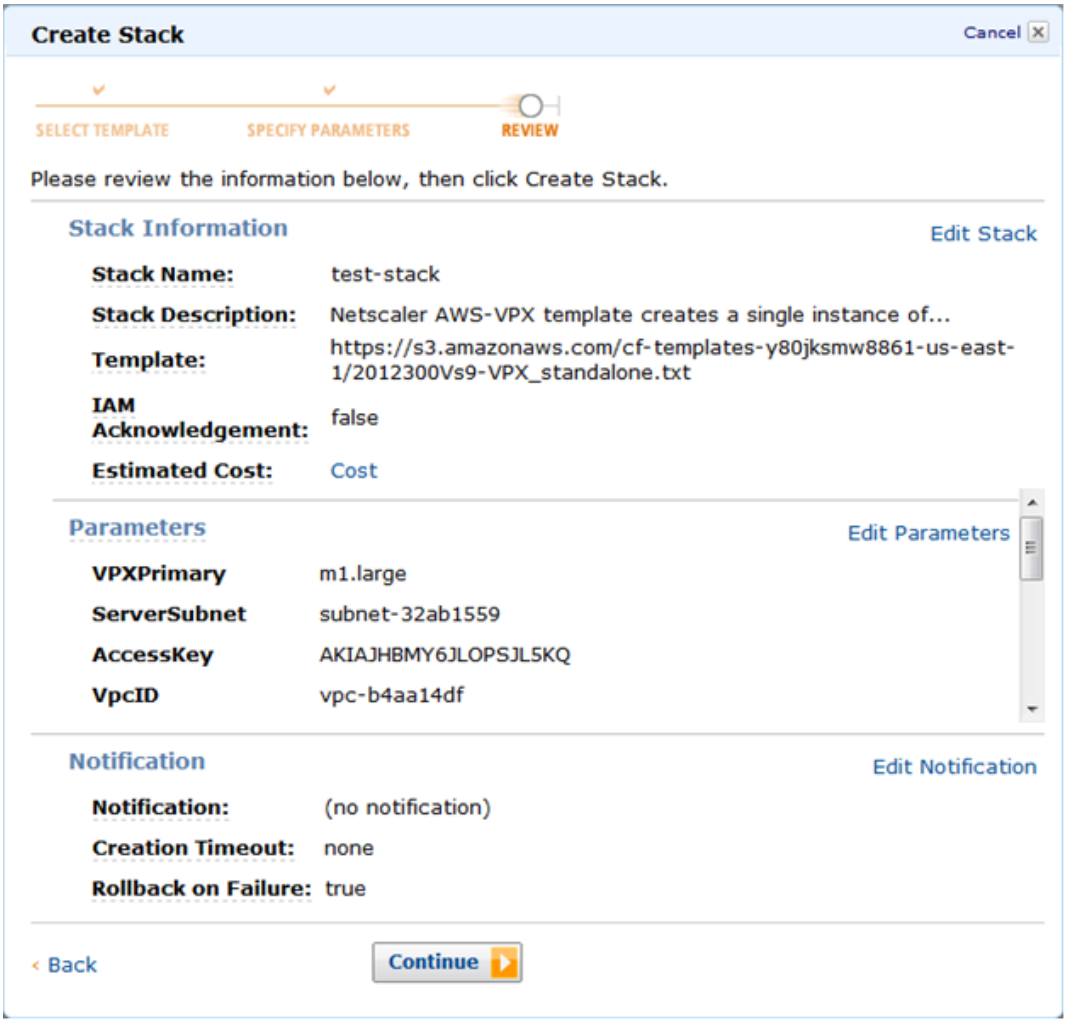
- **KeyName**: Name of an existing EC2 KeyPair to enable SSH access to the instances.

Note: Make sure that the VPC, subnets, security groups, routes associations, gateway associations are already configured.

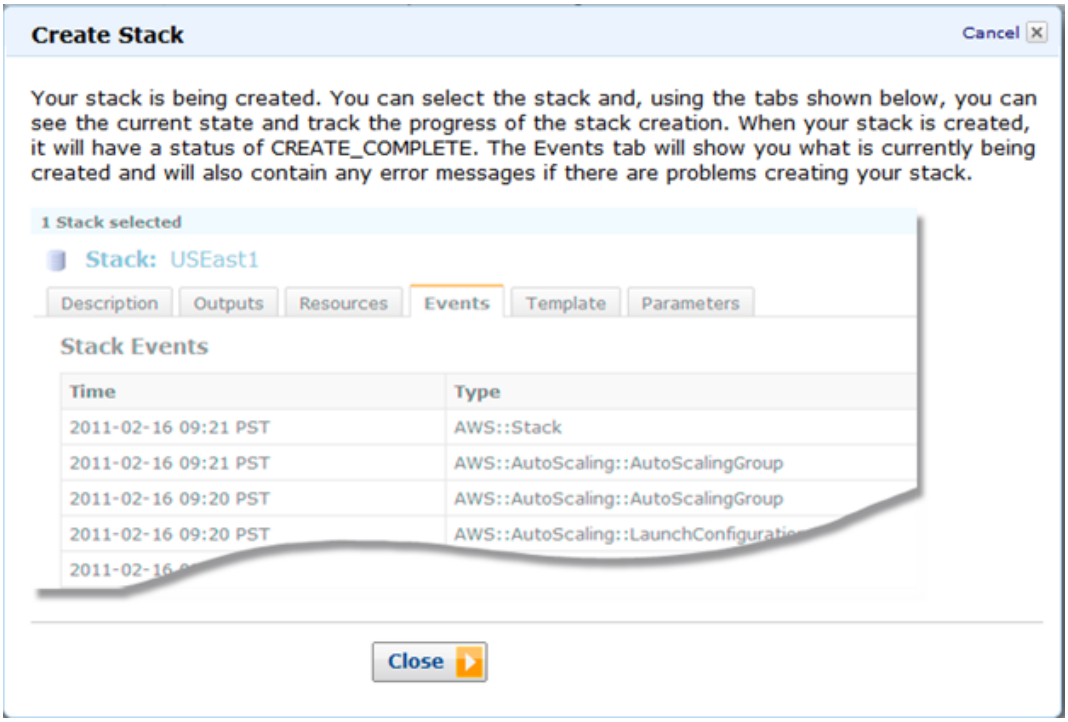


7. Click Continue.

8. Review the specified values in the Create Stack dialog box.



9. Click Continue to create a Stack.



10. Click Close to close the Create Stack dialog box.

11. The new stack that you created appears on the CloudFormation Stacks page.

Upgrading a NetScaler VPX instance on AWS

You can upgrade the EC2 instance type, throughput, software edition, and the system software of a NetScaler VPX running on AWS. For certain types of upgrades, Citrix recommends using the High Availability Configuration method to minimize downtime.

Note:

- NetScaler software release 10.1.e-124.1308.e or later for a NetScaler VPX AMI (including both utility license and customer license) does not support the M1 and M2 instance families.
- Because of changes in NetScaler instance support, downgrading from 10.1.e-124 or a later release to 10.1.123.x or an earlier release is not supported.
- Most of the upgrades do not require the launch of a new AMI, and the upgrade can be done on the current NetScaler AMI instance. If you do want to upgrade to a new NetScaler AMI instance, use the high availability configuration method.

Changing the EC2 Instance Type of a NetScaler VPX Instance on AWS

If your NetScaler VPX instances are running release 10.1.e-124.1308.e or later, you can change the EC2 instance type from the AWS console as follows:

1. Stop the VPX instance.
2. Change the EC2 instance type from the AWS console.
3. Start the instance.

You can also use the above procedure to change the EC2 instance type for a release, earlier than 10.1.e-124.1308.e, unless you want to change the instance type to M3. In that case, you must first follow the standard NetScaler upgrade procedure, at , to upgrade the NetScaler software to 10.1.e-124 or a later release, and then follow the above steps.

Upgrading the Throughput or Software Edition for a NetScaler VPX Instance on AWS

To upgrade the software edition (for example, to upgrade from standard to platinum edition) or throughput (for example, to upgrade from 200 mbps to 1000mbps), the method depends on the instance's license.

Using a customer license (Bring-Your-Own-License)

If you are using a customer license, you can purchase and download the new license from the Citrix Licensing portal (MyCitrix), and then install the license on the VPX instance. For more information about downloading and installing a license from the MyCitrix portal, see the VPX Licensing Guide.

Using a utility license (Utility license with hourly fee)

AWS does not support direct upgrades for fee-based instances. To upgrade the software edition or throughput of a fee based NetScaler VPX instance, launch a new AMI with the desired license and capacity and migrate the older instance configuration to the new instance. This can be achieved by using a NetScaler high availability configuration as described in "Upgrading to a New NetScaler AMI Instance by Using a NetScaler High Availability Configuration."

Upgrading the System Software of a NetScaler VPX Instance on AWS

If you need to upgrade a NetScaler instance running 10.1.e-124.1308.e or a later release, follow the standard NetScaler upgrade procedure at .

If you need to upgrade a NetScaler instance running a release older than 10.1.e-124.1308.e to 10.1.e-124.1308.e or a later release, first upgrade the system software, and then change the instance type to M3 as follows:

1. Stop the VPX instance.
2. Change the EC2 instance type from the AWS console.
3. Start the instance.

Upgrading to a New NetScaler AMI Instance by Using a NetScaler High Availability Configuration

To use the high availability method of upgrading to a new NetScaler AMI instance, perform the following tasks:

- Create a new instance with the desired EC2 instance type, software edition, throughput, or software release from the AWS marketplace.
- Configure high availability between the old instance (to be upgraded) and the new instance. After high availability is configured between the old and the new instance, configuration from the old instance is synchronized to the new instance.
- Force an HA failover from the old instance to the new instance. As a result, the new instance becomes primary and starts receiving traffic.
- Stop, and reconfigure or remove the old instance from AWS.

Prerequisites and Points to Consider

- Make sure you understand how high availability works between two NetScaler VPX instances on AWS. For more information about high availability configuration between two NetScaler VPX instances on AWS, see High Availability.
- You must create the new instance in the same availability zone as the old instance, having the exact same security group and subnet.
- High availability setup requires access and secret keys associated with the user's AWS Identity and Access Management (IAM) account for both instances. If the correct key information is not used when creating VPX instances, the HA setup fails. For more information about creating an IAM account for a VPX instance, see Creating an IAM Account.
- You must use the EC2 console to create the new instance. You cannot use the AWS 1-click launch, because it does not accept the access and secret keys as the input.
- The new instance should have only one ENI interface.

To upgrade a NetScaler VPX Instance by using a high availability configuration

1. Configure high availability between the old and the new instance. To configure high availability between two NetScaler VPX instances, at the NetScaler command prompt of each intance, type:
   - add ha node <nodeID> <IPaddress of the node to be added>
   - save config

   Example

At the NetScaler command prompt of the old instance, type:
> add ha node 30 192.0.2.30
Done
At the NetScaler command prompt of the new instance, type:
> add ha node 10 192.0.2.10
Done

Note the following:

- In the HA setup, the old instance is the primary node and the new instance is the secondary node.
- The NSIP IP address is not copied from the old instance to the new instance. Therefore, after the upgrade, your new instance has a different management IP address from the previous one.
- The nsroot account password of the new instance is set to that of the old instance after HA synchronization.

For more information about high availability configuration between two NetScaler VPX instances on AWS, see High Availability.

2. Force an HA failover. To force a failover in a high availability configuration, at the NetScaler command prompt of either of the instances, type:

   - force HA failover

   As the result of forcing a failover, the ENIs of the old instance are migrated to the new instance and traffic flows through the new instance (the new primary node). The old instance (the new secondary node) restarts.

   If the following warning message appears, type N to abort the operation:

   WARNING]:Force Failover may cause configuration loss, peer health not optimum. Reason(s):
   HA version mismatch
   HA heartbeats not seen on some interfaces
   Please confirm whether you want force-failover (Y/N)?

   The warning message appears because the system software of the two VPX instances is not HA compatible. As a result, the configuration of the old instance cannot be automatically synced to the new instance during a forced failover.

   Following is the workaround for this issue:

   a. At the NetScaler shell prompt of the old instance, type the following command to create a backup of the configuration file (ns.conf):

      - copy /nsconfig/ns.conf to /nsconfig/ns.conf.bkp

   b. Remove the following line from the backup configuration file (ns.conf.bkp):

      - set ns config -IPAddress <IP> -netmask <MASK>

        For example, set ns config -IPAddress 192.0.2.10 -netmask 255.255.255.0

   c. Copy the old instance's backup configuration file (ns.conf.bkp) to the /nsconfig directory of the the new instance.

d. At the NetScaler shell prompt of the new instance, type the following command to load the old instance's configuration file (ns.conf.bkp) on the new instance:

   - batch -f /nsconfig/ns.conf.bkp

e. Save the configuration on the new instance.

   - Save conifg

f. At the NetScaler command prompt of either of the nodes, type the following command to force a failover, and then type Y for the warning message to confirm the force failover operation:

   - force ha failover

   Example

   > force ha failover

   WARNING]:Force Failover may cause configuration loss, peer health not optimum.
   Reason(s):
   HA version mismatch
   HA heartbeats not seen on some interfaces
   Please confirm whether you want force-failover (Y/N)? Y

3. Remove the HA configuration, so that the two instances are no longer in an HA configuration. First remove the HA configuration from the secondary node and then remove the HA configuration from the primary node.

   To remove an HA configuration between two NetScaler VPX instances, at the command prompt of each instance, type:

   - remove ha node <nodeID>

   - save config

   For more information about high availability configuration between two NetScaler instances on AWS, see High Availability.

   Example

   At the NetScaler command prompt of the old instance (new secondary node), type:
   > remove ha node 30
   Done
   > save config
   Done
   At the NetScaler command prompt of the new instance (new primary node), type:
   > remove ha node 10
   Done
   > save config
   Done

Troubleshooting the NetScaler VPX on AWS

Amazon does not provide console access to a NetScaler VPX virtual instance. To troubleshoot, you have to use the AWS GUI to view the activity log. You can debug only if the network is connected. To view an instance's system log, right-click the instance and select system log.

Citrix provides support for fee based NetScaler VPX instances (utility license with hourly fee) on AWS. To file a support case, find your AWS account number and support PIN code, and call Citrix support. You will also be asked for your name and email address. To find the support PIN, log on to the NetScaler configuration utility and navigate to the System page.

Installing CloudBridge VPX in a Data Center

The Citrix CloudBridge VPX virtual appliance can be hosted on Citrix XenServer®, VMware ESX or ESXi, and Microsoft Hyper-V virtualization platforms.

Installing NetScaler Virtual Appliances on XenServer

To install NetScaler virtual appliances on Citrix XenServer, you must first install XenServer on a machine with adequate system resources. To perform the NetScaler virtual appliance installation, you use Citrix XenCenter, which must be installed on a remote machine that can connect to the XenServer host through the network.

Note: After the initial configuration of the NetScaler appliance, if you want to upgrade the appliance to the latest software release, see Upgrading or Downgrading the System Software.

Prerequisites for Installing NetScaler Virtual Appliances on XenServer

Before you begin installing a virtual appliance, do the following:

- Install XenServer® version 5.6 or later on hardware that meets the minimum requirements.
- Install XenCenter® on a management workstation that meets the minimum system requirements.
- Obtain virtual appliance license files. For more information about virtual appliance licenses, see the *NetScaler VPX Licensing Guide* at http://support.citrix.com/article/ctx122426.

XenServer Hardware Requirements

The following table describes the minimum hardware requirements for a XenServer platform running NetScaler.

Table 1. Minimum System Requirements for XenServer Running NetScaler nCore virtual appliance

Component	Requirement
CPU	2 or more 64-bit x86 CPUs with virtualization assist (Intel-VT or AMD-V) enabled **Note:** To run NetScaler virtual appliance, hardware support for virtualization must be enabled on the XenServer host. Make sure that the BIOS option for virtualization support is not disabled. Consult your BIOS documentation for more details.
RAM	3 gigabytes (GB)
Disk space	Locally attached storage (PATA, SATA, SCSI) with 40 GB of disk space **Note:** XenServer installation creates a 4 GB partition for the XenServer host control domain; the remaining space is available for NetScaler virtual appliance and other virtual machines.
Network Interface Card (NIC)	One 1-Gbps NIC Recommended: Two 1-Gbps NICs

For information about installing XenServer, see the XenServer documentation at http://support.citrix.com/product/xens/.

The following table lists the virtual computing resources that XenServer must provide for each NetScaler nCore virtual appliance .

Table 2. Minimum Virtual Computing Resources Required for Running NetScaler ncore virtual appliance

Component	Requirement
Memory	2 GB
Virtual CPU (VCPU)	2
Virtual network interfaces	2

Note: For production use of NetScaler virtual appliance, Citrix recommends that CPU priority (in virtual machine properties) be set to the highest level, in order to improve scheduling behavior and network latency.

XenCenter System Requirements

XenCenter® is a Windows client application. It cannot run on the same machine as the XenServer® host. The following table describes the minimum system requirements.

Table 3. Minimum System Requirements for XenCenter Installation

Component	Requirement
Operating system	Windows 7, Windows XP, Windows Server 2003, or Windows Vista
.NET framework	Version 2.0 or later
CPU	750 megahertz (MHz) Recommended: 1 gigahertz (GHz) or faster
RAM	1 GB Recommended: 2 GB
Network Interface Card (NIC)	100 megabits per second (Mbps) or faster NIC

For information about installing XenCenter, see the XenServer documentation at http://support.citrix.com/product/xens/.

Installing NetScaler Virtual Appliances on XenServer by Using XenCenter

After you have installed and configured XenServer and XenCenter, you can use XenCenter to install virtual appliances on XenServer. The number of virtual appliances that you can install depends on the amount of memory available on the hardware that is running XenServer.

After you have used XenCenter to install the initial NetScaler virtual appliance (.xva image) on XenServer, you have the option to use Command Center to provision NetScaler virtual appliance. For more information, see the Command Center documentation.

To install NetScaler virtual appliances on XenServer by using XenCenter

1. Start XenCenter on your workstation.
2. On the Server menu, click Add.
3. In the Add New Server dialog box, in the Hostname text box, type the IP address or DNS name of the XenServer that you want to connect to.
4. In the User Name and Password text boxes, type the administrator credentials, and then click Connect. The XenServer name appears in the navigation pane with a green circle, which indicates that the XenServer is connected.
5. In the navigation pane, click the name of the XenServer on which you want to install NetScaler virtual appliance.
6. On the VM menu, click Import.
7. In the Import dialog box, in Import file name, browse to the location at which you saved the NetScaler virtual appliance .xva image file. Make sure that the Exported VM option is selected, and then click Next.
8. Select the XenServer on which you want to install the virtual appliance, and then click Next.
9. Select the local storage repository in which to store the virtual appliance, and then click Import to begin the import process.
10. You can add, modify, or delete virtual network interfaces as required. When finished, click Next.
11. Click Finish to complete the import process.

    Note: To view the status of the import process, click the **Log** tab.
12. If you want to install another virtual appliance, repeat steps 5 through 11.

Installing NetScaler Virtual Appliances on VMware ESX

Important: You cannot install standard VMware Tools or upgrade the VMware Tools version available on a NetScaler virtual appliance. VMware Tools for a NetScaler virtual appliance are delivered as part of the NetScaler software release.

Before installing NetScaler virtual appliances on VMware ESX, make sure that VMware ESX Server is installed on a machine with adequate system resources. To install NetScaler virtual appliances on VMware ESXi version 4.0 or later, you use VMware vSphere client. The client or tool must be installed on a remote machine that can connect to VMware ESX through the network.

After the installation, you can use vSphere client or vSphere Web Client to manage virtual appliances on VMware ESX 4.0 or later release.

Note:

The VMware vSphere client shows the guest operating system as "Sun Solaris 10" for NetScaler virtual machine. This is by design because VMware ESXi does not recognize FreeBSD.

After the initial configuration of the NetScaler appliance, if you want to upgrade the appliance to the latest software release, see "Upgrading or Downgrading the System Software."

Prerequisites for Installing NetScaler Virtual Appliances on VMware

Before you begin installing a virtual appliance, do the following:

- Install VMware ESX version 4.1 or later on hardware that meets the minimum requirements.
- Install VMware Client on a management workstation that meets the minimum system requirements.
- Download the NetScaler virtual appliance setup files.
- Label the physical network ports of VMware ESX.
- Obtain NetScaler license files. For more information about NetScaler virtual appliance licenses, see the *NetScaler VPX Licensing Guide* at http://support.citrix.com/article/ctx131110.

VMware ESX Hardware Requirements

The following table describes the minimum system requirements for VMware ESX servers running NetScaler ncore virtual appliance.

Table 1. Minimum System Requirements for VMware ESX Servers Running NetScaler nCore virtual appliance

Component	Requirement
CPU	2 or more 64-bit x86 CPUs with virtualization assist (Intel-VT or AMD-V) enabled **Note:** To run NetScaler virtual appliance, hardware support for virtualization must be enabled on the VMware ESX host. Make sure that the BIOS option for virtualization support is not disabled. For more information, see your BIOS documentation.
RAM	3 GB
Disk space	40 GB of disk space available
Network	One 1-Gbps NIC; Two 1-Gbps NICs recommended (The network interfaces must be Intel E1000.)

For information about installing VMware ESX, see http://www.vmware.com/.

The following table lists the virtual computing resources that the VMware ESX server must provide for each NetScaler ncore virtual appliance.

Table 2. Minimum Virtual Computing Resources Required for Running NetScaler ncore virtual appliance

Component	Requirement
Memory	2 GB
Virtual CPU (VCPU)	2 **Important:** Do not modify the system resources to create a virtual CPU (VCPU) in addition to the two CPUs already allotted to the virtual appliance.
Virtual network interfaces	1 **Note:** With ESX 4.0 or later, you can install a maximum of 10 virtual network interfaces if the VPX hardware is upgraded version to 7 or higher.
Disk space	20 GB **Note:** This is in addition to any disk requirements for the hypervisor.

Note: For production use of NetScaler virtual appliance, the full memory allocation must be reserved. CPU cycles (in MHz) equal to at least the speed of one CPU core of the ESX should also be reserved.

VMware vSphere Client System Requirements

VMware vSphere is a client application that can run on Windows and Linux operating systems. It cannot run on the same machine as the VMware ESX server. The following table describes the minimum system requirements.

Table 3. Minimum System Requirements for VMware vSphere Client Installation

Component	Requirement
Operating system	For detailed requirements from VMware, search for the "vSphere Compatibility Matrixes" PDF file at http://kb.vmware.com/.
CPU	750 megahertz (MHz); 1 gigahertz (GHz) or faster recommended
RAM	1 GB; 2 GB recommended
Network Interface Card (NIC)	100 Mbps or faster NIC

OVF Tool 1.0 System Requirements

OVF Tool is a client application that can run on Windows and Linux systems. It cannot run on the same machine as the VMware ESX server. The following table describes the minimum system requirements.

Table 4. Minimum System Requirements for OVF Tool Installation

Component	Requirement
Operating system	For detailed requirements from VMware, search for the "OVF Tool User Guide" PDF file at http://kb.vmware.com/.
CPU	750 MHz minimum, 1 GHz or faster recommended.
RAM	1 GB Minimum, 2 GB recommended.
Network Interface Card (NIC)	100 Mbps or faster NIC

For information about installing OVF, search for the "OVF Tool User Guide" PDF file at http://kb.vmware.com/.

Downloading the NetScaler virtual appliance Setup Files

The NetScaler virtual appliance setup package for VMware ESX follows the Open Virtual Machine (OVF) format standard. You can download the files from MyCitrix.com. You need a My Citrix account to log on. If you do not have a My Citrix account, access the home page at http://www.mycitrix.com, click the New Users link, and follow the instructions to create a new My Citrix account.

Once logged on, navigate the following path from the My Citrix home page:

MyCitrix.com > Downloads > NetScaler > Virtual Appliances.

Copy the following files to a workstation on the same network as the ESX server. Copy all three files into the same folder.

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (for example, NSVPX-ESX-9.3-39.8-disk1.vmdk)
- NSVPX-ESX-<release number>-<build number>.ovf (for example, NSVPX-ESX-9.3-39.8.ovf)
- NSVPX-ESX-<release number>-<build number>.mf (for example, NSVPX-ESX-9.3-39.8.mf)

Labeling the Physical Network Ports of VMware ESX

Before installing a NetScaler virtual appliance, label of all the interfaces that you plan to assign to virtual appliances, in a unique format. Citrix recommends the following format: NS_NIC_1_1, NS_NIC_1_2, and so on. In large deployments, labeling in a unique format helps in quickly identifying the interfaces that are allocated to the NetScaler virtual appliance among other interfaces used by other virtual machines, such as Windows and Linux. Such labeling is especially important when different types of virtual machines share the same interfaces.

To label the physical network ports of VMware ESX server

1. Log on to the VMware ESX server by using the vSphere client.
2. On the vSphere client, select the Configuration tab, and then click Networking.
3. At the top-right corner, click Add Networking.
4. In the Add Network Wizard, for **Connection Type**, select **Virtual Machine**, and then click Next.
5. Scroll through the list of vSwitch physical adapters, and choose the physical port that will map to interface 1/1 on the virtual appliances.
6. Enter NS_NIC_1_1 as the name of the vSwitch that will be associated with interface 1/1 of the virtual appliances.
7. Click Next to finish the vSwitch creation. Repeat the procedure, beginning with step 2, to add any additional interfaces to be used by your virtual appliances. Label the interfaces sequentially, in the correct format (for example, NS_NIC_1_2).

Installing NetScaler Virtual Appliances on VMware ESX 4.0 or Later

After you have installed and configured VMware ESX 4.0 or later, you can use the VMware vSphere client to install virtual appliances on the VMware ESX. The number of virtual appliances that you can install depends on the amount of memory available on the hardware that is running VMware ESX.

To install NetScaler virtual appliances on VMware ESX 4.0 or later by using VMware vSphere Client

1. Start the VMware vSphere client on your workstation.
2. In the IP address / Name text box, type the IP address of the VMware ESX server that you want to connect to.
3. In the User Name and Password text boxes, type the administrator credentials, and then click Login.
4. On the File menu, click Deploy OVF Template.
5. In the Deploy OVF Template dialog box, in Deploy from file, browse to the location at which you saved the NetScaler virtual appliance setup files, select the .ovf file, and click Next.
6. Map the networks shown in the virtual appliance OVF template to the networks that you configured on the ESX host. Click Next to start installing a virtual appliance on VMware ESX. When installation is complete, a pop-up window informs you of the successful installation.
7. You are now ready to start the NetScaler virtual appliance. In the navigation pane, select the NetScaler virtual appliance that you have just installed and, from the right-click menu, select Power On. Click the Console tab to emulate a console port.
8. If you want to install another virtual appliance, repeat steps 4 through 6.

Installing NetScaler Virtual Appliances on VMware ESX 3.5

To install virtual appliances on ESX 3.5, you need to use the VMware OVF tool, version 1.0. The number of virtual appliances that you can install depends on the amount of memory available on the hardware that is running VMware ESX. After installation, you can use the VMware Infrastructure (VI) client 2.5 to manage the virtual appliances on VMware ESX version 3.5.

Note: You cannot use version 4.0 of the vSphere client for installing virtual appliances on ESX 3.5. If you connect the vSphere 4.0 client to ESX 3.5, the vSphere client downgrades to VI client version 2.5, which supports only the OVF 0.9 standard. The NetScaler virtual appliance installation package is based on the OVF 1.0.

To install NetScaler virtual appliances on VMware ESX 3.5 by using the VMware OVF Tool

1. On your workstation, open the command-line interface and execute the following command:

   ```
   ovftool <path of the NetScaler VPX OVF file>
   vi://<Username>:<Password>@<IP address of the ESX server>
   ```

   For example, in Windows command shell, type:

   ```
   ovftool c:/NetScalerVPX vi://root:free@<10.217.20.14>
   ```

2. When the OVF tool has installed the virtual appliances on the ESX server, use the VI client to log on to the VMware ESX server on which you performed the installation.

3. In the navigation pane, right-click a virtual appliance that you want to enable, and then click **Power On**. Repeat this for each virtual appliance you want to enable.

4. Click the Console tab to emulate a console port.

Installing Citrix NetScaler Virtual Appliances on Microsoft Hyper-V Servers

To install Citrix NetScaler virtual appliances on Microsoft Windows Server, you must first install Windows Server, with the Hyper-V role enabled, on a machine with adequate system resources. While installing the Hyper-V role, be sure to specify the network interface cards (NICs) on the server that Hyper-V will use to create the virtual networks. You can reserve some NICs for the host. Use Hyper-V Manager to perform the NetScaler virtual appliance installation.

NetScaler virtual appliance for Hyper-V is delivered in virtual hard disk (VHD) format. It includes the default configuration for elements such as CPU, network interfaces, and hard-disk size and format. After you install NetScaler virtual appliance, you can configure the network adapters on virtual appliance, add virtual NICs, and then assign the NetScaler IP address, subnet mask, and gateway, and complete the basic configuration of the virtual appliance.

Note:

After the initial configuration of the NetScaler appliance, if you want to upgrade the appliance to the latest software release, see "Upgrading or Downgrading the System Software."

Prerequisites for Installing NetScaler Virtual Appliance on Microsoft Servers

Before you begin installing a virtual appliance, do the following:

- Enable the Hyper-V role on Windows Servers . For more information, see http://technet.microsoft.com/en-us/library/ee344837(WS.10).aspx.
- Download the virtual appliance setup files.
- Obtain NetScaler virtual appliance license files. For more information about NetScaler virtual appliance licenses, see the *NetScaler VPX Licensing Guide* at http://support.citrix.com/article/ctx131110.

Microsoft Server Hardware Requirements

The following table describes the minimum system requirements for Microsoft Servers .

Table 1. Minimum System Requirements for Microsoft Servers

Component	Requirement
CPU	1.4 GHz 64-bit processor
RAM	3 GB
Disk Space	32 GB or greater

The following table lists the virtual computing resources for each NetScaler virtual appliance.

Table 2. Minimum Virtual Computing Resources Required for Running NetScaler Virtual Appliance

Component	Requirement
RAM	2 GB
Virtual CPU	2
Disk Space	20 GB
Virtual Network Interfaces	1

Downloading the NetScaler Virtual Appliance Setup Files

NetScaler virtual appliance for Hyper-V is delivered in virtual hard disk (VHD) format. You can download the files from MyCitrix.com. You will need a My Citrix account to log on. If you do not have a My Citrix account, access the home page at http://www.mycitrix.com, click the New Users link, and follow the instructions to create a new My Citrix account.

To download the NetScaler virtual appliance setup files

1. In a Web browser, go to http://www.citrix.com/ and click My Citrix.
2. Type your user name and password.
3. Click Downloads.
4. In Search Downloads by Product, select NetScaler.
5. Under Virtual Appliances, click NetScaler VPX.
6. Copy the compressed file to your server.

Installing NetScaler Virtual Appliance on Microsoft Servers

After you have enabled the Hyper-V role on Microsoft Server and extracted the virtual appliance files, you can use Hyper-V Manager to install NetScaler virtual appliance. After you import the virtual machine, you need to configure the virtual NICs by associating them to the virtual networks created by Hyper-V.

You can configure a maximum of eight virtual NICs. Even if the physical NIC is DOWN, the virtual appliance assumes that the virtual NIC is UP, because it can still communicate with the other virtual appliances on the same host (server).

Note: You cannot change any settings while the virtual appliance is running. Shut down the virtual appliance and then make changes.

To install NetScaler Virtual Appliance on Microsoft Server by using Hyper-V Manager

1. To start Hyper-V Manager, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In the navigation pane, under Hyper-V Manager, select the server on which you want to install NetScaler virtual appliance.
3. On the **Action** menu, click **Import Virtual Machine**.
4. In the **Import Virtual Machine** dialog box, in **Location**, specify the path of the folder that contains the NetScaler virtual appliance software files, and then select **Copy the virtual machine (create a new unique ID)**. This folder is the parent folder that contains the Snapshots, Virtual Hard Disks, and Virtual Machines folders.

   Note: If you received a compressed file, make sure that you extract the files into a folder before you specify the path to the folder.
5. Click **Import**.
6. Verify that the virtual appliance that you imported is listed under **Virtual Machines**.
7. To install another virtual appliance, repeat steps 2 through 6.

   Important: Make sure that you extract the files to a different folder in step 4.

To configure virtual NICs on the NetScaler Virtual Appliance

1. Select the virtual appliance that you imported, and then on the **Action** menu, select **Settings**.
2. In the **Settings for** <virtual appliance name> dialog box, click **Add Hardware** in the left pane.
3. In the right pane, from the list of devices, select **Network Adapter**.
4. Click **Add**.
5. Verify that **Network Adapter** (**not connected**) appears in the left pane.
6. Select the network adapter in the left pane.
7. In the right pane, from the **Network** drop-down list, select the virtual network to connect the adapter to.
8. To select the virtual network for additional network adapters that you want to use, repeat steps 6 and 7.
9. Click **Apply**, and then click **OK**.

To configure NetScaler Virtual Appliance

1. Right-click the virtual appliance that you previously installed, and then select **Start**.
2. Access the console by double-clicking the virtual appliance.
3. Type the NetScaler IP address, subnet mask, and gateway for your virtual appliance.

You have completed the basic configuration of your virtual appliance. Type the IP address in a Web browser to access the virtual appliance.

Configuring CloudBridge for Common Deployment Scenarios

To create a CloudBridge, you can perform the configuration tasks on the CloudBridge VPX instance at either of the sites that you want to bridge. You must specify the IP addresses of the CloudBridge VPX instances at the two sites (for example, the IP address of the instance in the data center and the IP address of the instance in AWS). You also need to configure the IPSec security settings. For more information on common CloudBridge topologies, see CloudBridge Topologies

Configuring CloudBridge between a Data Center and AWS

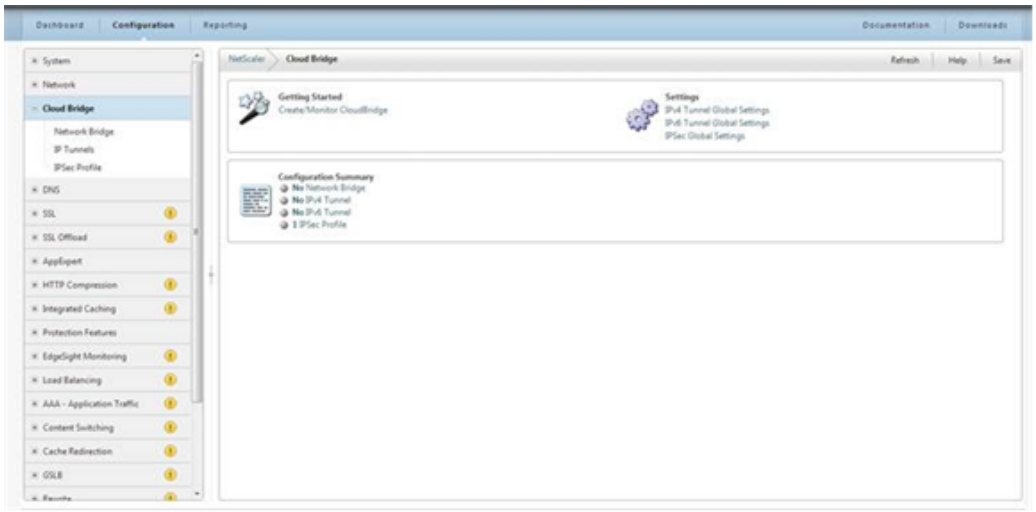
Before configuring CloudBridge between your local data center and a remote AWS cloud (to extend your network and leverage the cloud capabilities), make sure that you have publically accessible IP addresses for both locations. These publically accessible IP addresses are used to create a connection between the two locations.

You have to log on to the local CloudBridge instance and provide the AWS credentials (Access key and Secret Access key) and IP address of the remote CloudBridge instance in the AWS cloud.

To configure CloudBridge from a CloudBridge instance in the data center to a CloudBridge instance in AWS by using the configuration utility

1. Access the configuration utility by using a web browser to connect to the IP address of the CloudBridge instance in the datacenter.

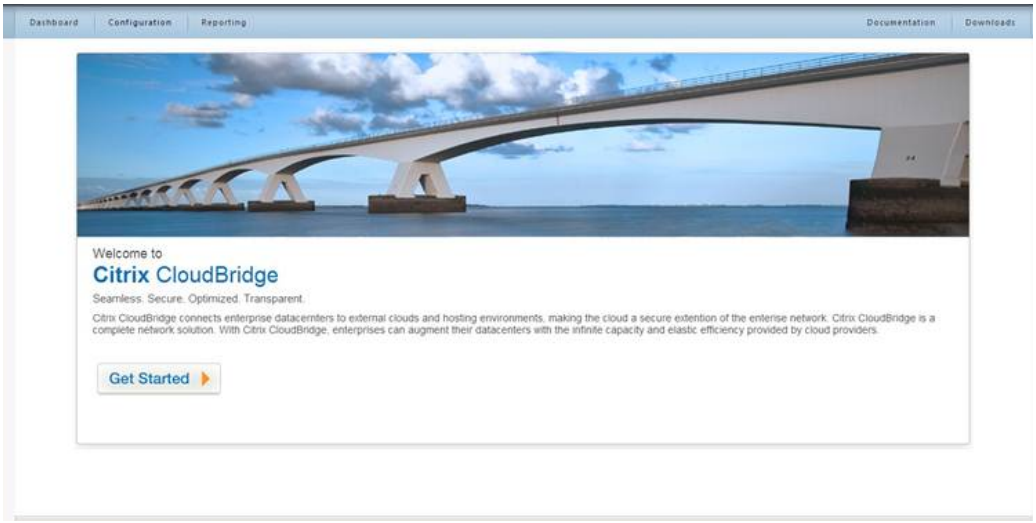
2. On the Configuration tab, in the Navigation pane, click CloudBridge.



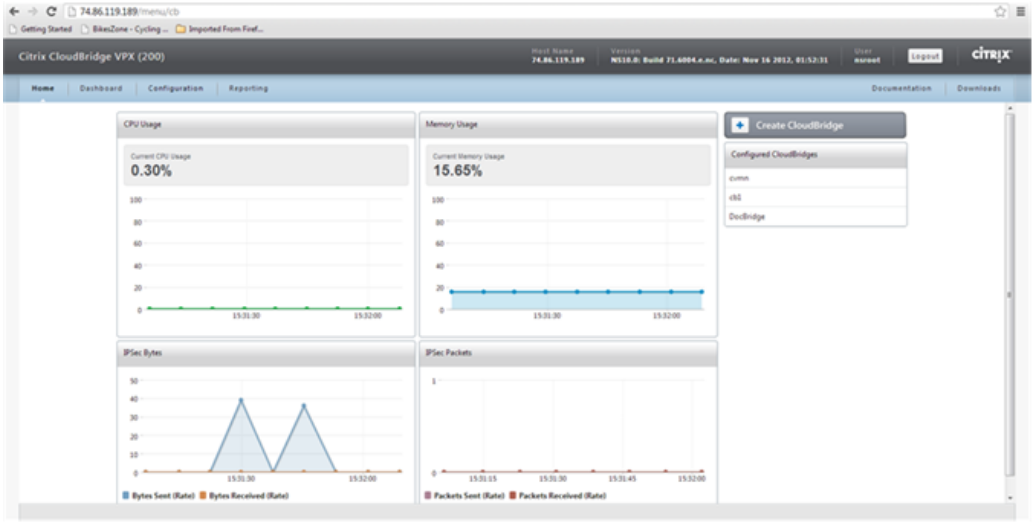
   Note: This screen appears only when you are using platinum edition license. For other licenses, you are taken to the Step 4 or Step 5 depending on whether CloudBridge is already configured on the CloudBridge VPX instance.

3. In the right pane, under Getting Started, click Create/Monitor CloudBridge.

4. Click **Get Started**.

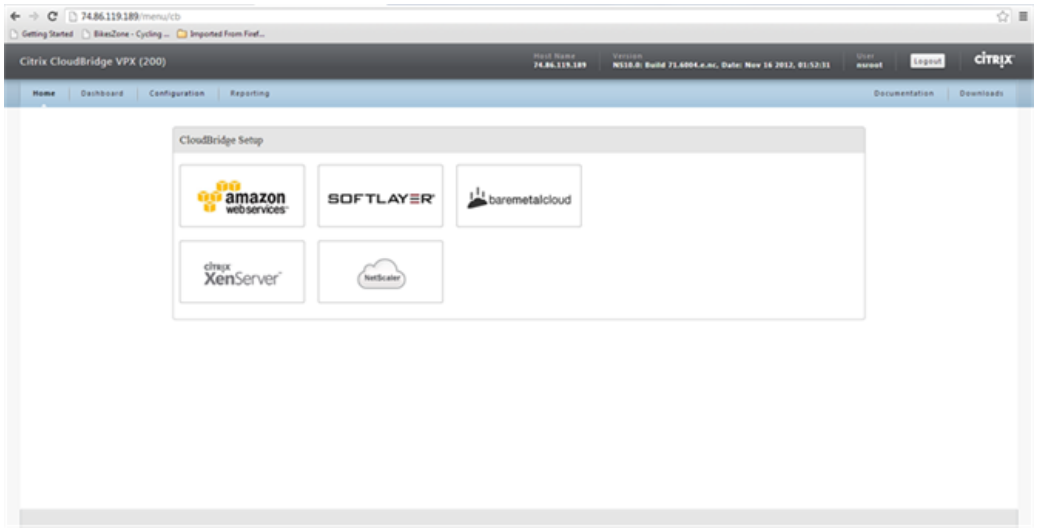


Note: If you already have a network bridge configured on the CloudBridge VPX instance, this screen does not appear. Instead, you are taken to the Citrix CloudBridge VPX page. Click Create CloudBridge to proceed.

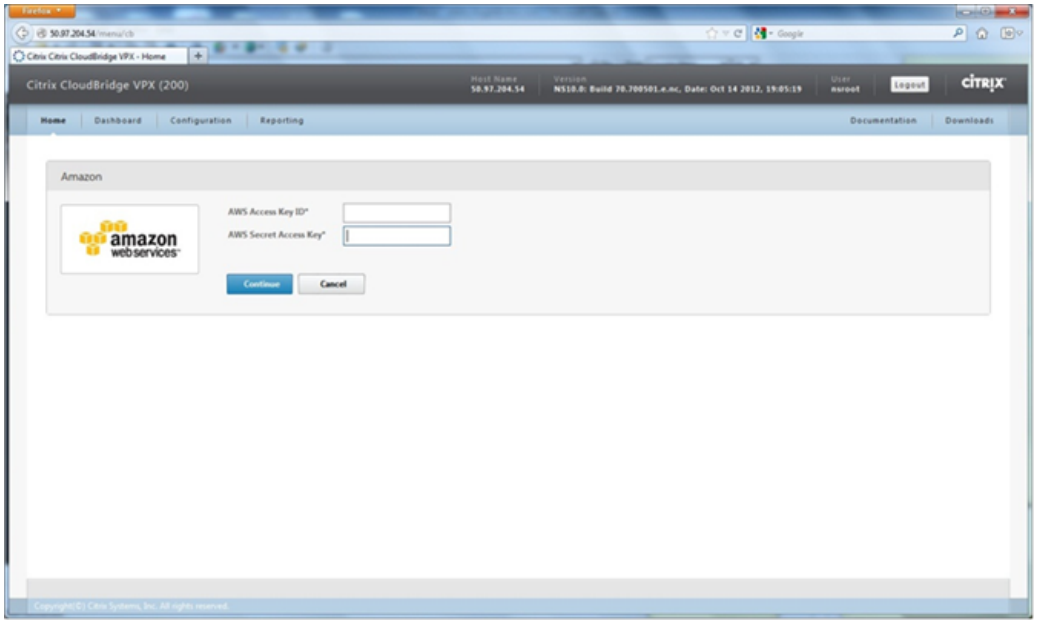


Note: If you are configuring first network bridge on an instance, this screen does not appear. Instead, after the **Get Started** page you are taken to the next page (**CloudBridge Setup**).

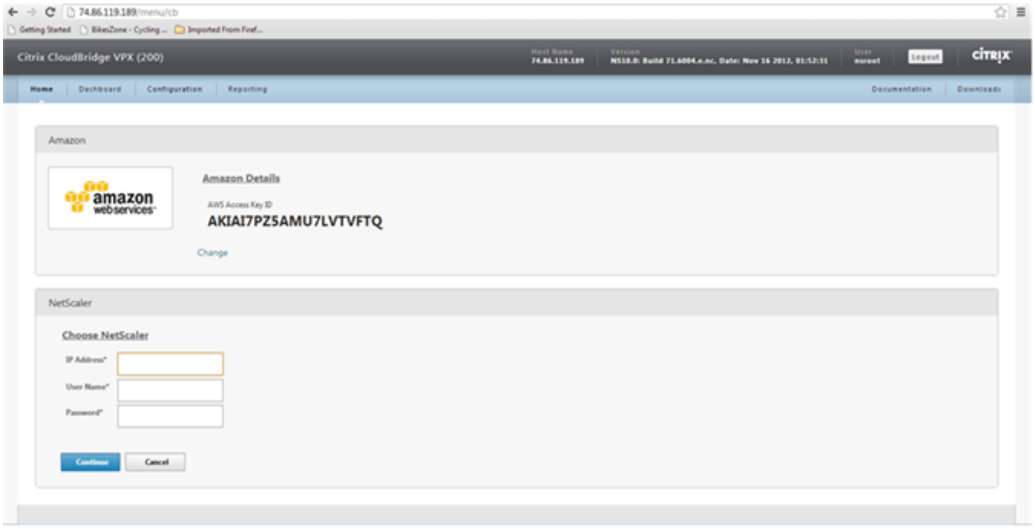
5. In the CloudBridge Setup pane, click amazon web services.



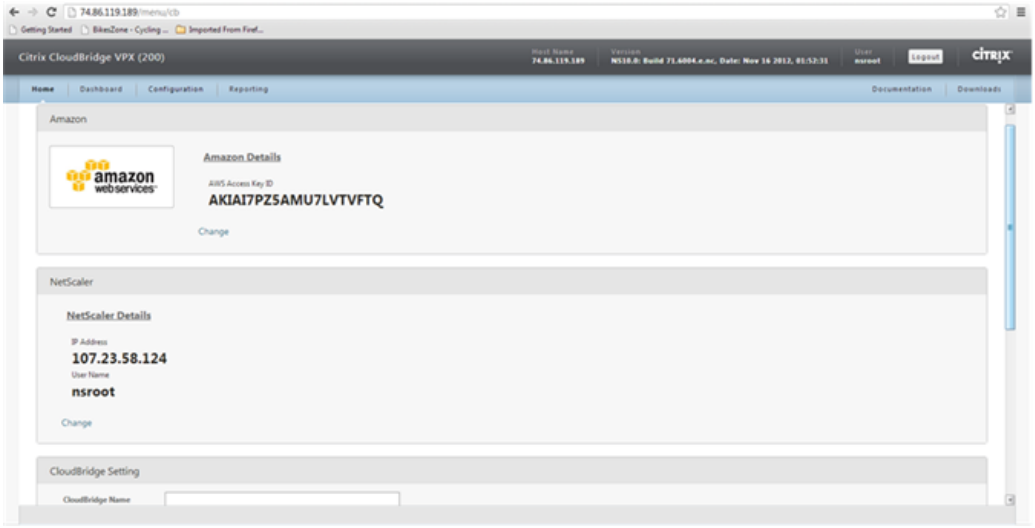
6. In the **Amazon** pane, enter the values for the access keys in the**AWS Access Key ID** and **AWS Secret Access Key** text boxes, and then click **Continue**. You can obtain these access keys from the AWS GUI console.



7. In the NetScaler pane, either select an IP address from the IP Address drop-down list or type the IP address, user name, and password in the corresponding text boxes for the CloudBridge VPX instance in AWS, and then click Continue. The IP address should be a publicly accessible address.



8. In the CloudBridge Setting pane, in the CloudBridge Name text box, type the name of the CloudBridge that you want to create.



9. Under Local Setting, from the Subnet IP drop-down list, select the subnet IP address of the local CloudBridge instance.

10. Under Remote Setting, from the Subnet IP drop-down list, select the subnet IP address of the CloudBridge VPX instance on the AWS.

11. Select the NetScaler Behind NAT checkbox and, in the IP Address text box, type the public IP address (EIP) that is mapped to the subnet IP you selected in step 10.

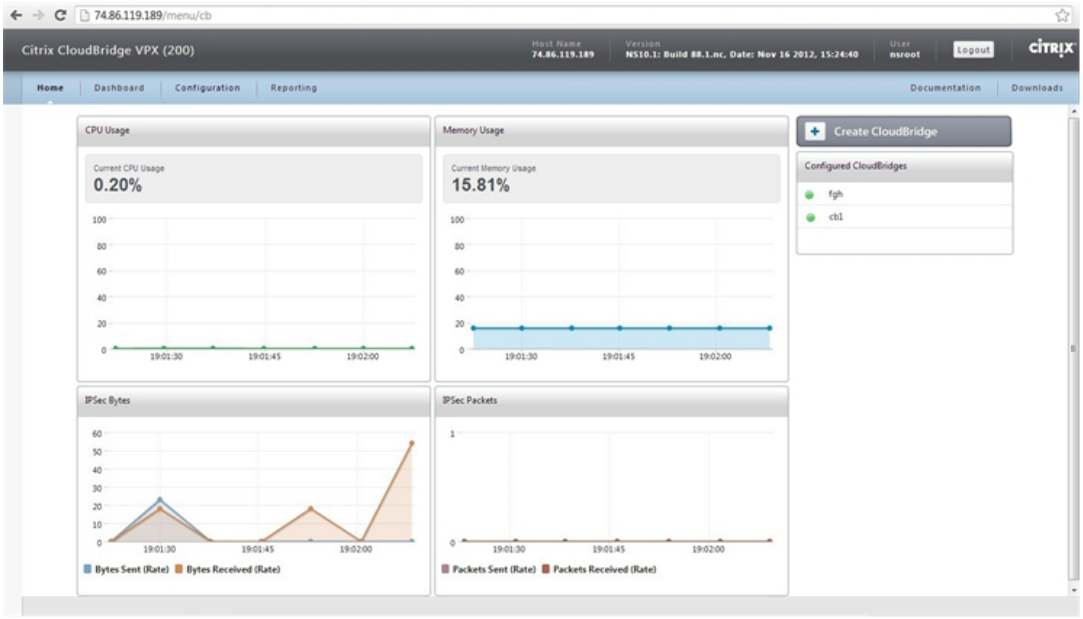
12. Under Security Settings, from the Encryption Algorithm and Hash Algorithm drop-down lists, select the algorithms that you want to use.

13. Select the Specify Key option and, in the Pre Shared Security Key text box, type the security key.

14. Click Done.

The new CloudBridge instance appears on the **Home** page. The current status of the CloudBridge is indicated in the **Configured CloudBridges** pane. A green dot indicates

that the tunnel is up. A red dot indicates that the tunnel is down.



To configure CloudBridge from a CloudBridge instance in the data center to a CloudBridge instance in AWS by using the command line

To set up a CloudBridge, on the CloudBridge instance in the data center:

- Create a network bridge
- Configure an IPsec profile
- Create a GRE tunnel with the IPsec profile
- Bind the IPsec tunnel to the network bridge

To create a network bridge by using the command line

At the local CloudBridge instance (in the data center) command prompt, type:

add netbridge <name>

Parameter for configuring a network bridge

name

Name of the CloudBridge that you are configuring. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equal (=), and hyphen (-) characters.

To configure IPsec profile by using the command line

At the local CloudBridge instance (in the data center) command prompt, type:

addipsec profile <name> [-encAlgo (AES | 3DES) ...] [-hashAlgo<hashAlgo> ...] [-lifetime<positive_integer>] (-psk |(-publickey<string>-privatekey<string>-peerPublicKey<string>))

Parameters for configuring IPsec profile

name

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

encAlgo

Encryption algorithm to be used in IPsec configuration for a CloudBridge. Possible values: AES, 3DES.

hashAlgo

Encryption algorithm to be used in IPsec configuration for a CloudBridge. Possible values: HMAC_SHA1, HMAC_SHA256, HMAC_MD5. Default: HMAC_SHA1.

lifetime

Time, in seconds, after which the security association expires. After expiration, new SAs are established, and new cryptographic keys are negotiated between the peers connected by the CloudBridge. Maximum value: 31536000. Default: 28800.

psk

Text string, called the pre-shared key, to be manually configured on each peer. The pre-shared keys of the peers are matched against each other for authentication before security associations are established. Therefore, for the authentication to be successful, you must configure the same pre-shared key on both of the peers of the CloudBridge. Maximum Length: 63 characters.

livenessCheckInterval

Time, in seconds, after which a notify payload is sent to check the status of the peer (UP or DOWN). Additional payloads are sent as per the retransmit interval setting. Zero value disables liveliness checks.

retransmissiontime

Time, in seconds, after which an IKE retry message is sent to a peer. The retry message is sent upto three times. Each failure doubles the amount of time before sending another retry message.

publickey

A local digital certificate to be used to authenticate the local CloudBridge appliance to the remote peer before establishing IPsec security associations. The same certificate should be present and set for the Peer Public Key parameter in the remote peer.

privatekey

Private key of the local digital certificate.

peerPublicKey

Digital certificate of the remote peer. This certificate is used to authenticate the remote peer to the local peer before establishing IPsec security associations. The same certificate should be present and set for the Public key parameter in the remote peer.

To create a GRE tunnel with IPsec profile by using the command line

At the local CloudBridge instance (in the data center) command prompt type:

add iptunnel <name><remoteIp><remoteSubnetMask><localIp>-type -protocol (GRE) -ipsecprofile<name>

Parameters for creating a GRE tunnel with IPsec profile

name

Name of the IP Tunnel. This alphanumeric string is required and cannot be changed after the service group is created. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

remoteIp

A public IP address of the remote CloudBridge appliance,in AWS, used to set up the tunnel.

remoteSubnetMask

Subnet mask of the remote IP address of the tunnel.

localIp

A public address of the local CloudBridge instance used to set up the tunnel. Possible values: Auto, MIP, SNIP, and VIP. Default: Auto.

protocol

The protocol to be used in setting up the IP tunnel. Select GRE to set up a GRE tunnel.

ipsecProfileName

Name of the IPsec profile that is used for securing communication in the GRE tunnel. If this parameter is not specified, the default profile (ns_ipsec_default_profile) is configured and, if this parameter is set to none, a GRE tunnel is created.

To bind an IPsec tunnel to the network bridge by using the command line

At the local CloudBridge instance (in the data center) command prompt, type:

bindnetbridge <name> [-tunnel <name>] [-vlan <id>] [-IPAddress <ip_addr | ipv6_addr>]

Parameters for binding IPsec tunnel to the network bridge

name

Name of the CloudBridge that you are configuring.Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

tunnel

Name of the GRE tunnel to be associated with the CloudBridge.

VLAN

Identifier of the local VLAN that needs to be extended to the cloud.

IPAddress

The IPV4 subnet that needs to be extended to the cloud.

Configuring CloudBridge between Two CloudBridge VPX Instances in two Different VPCs in AWS

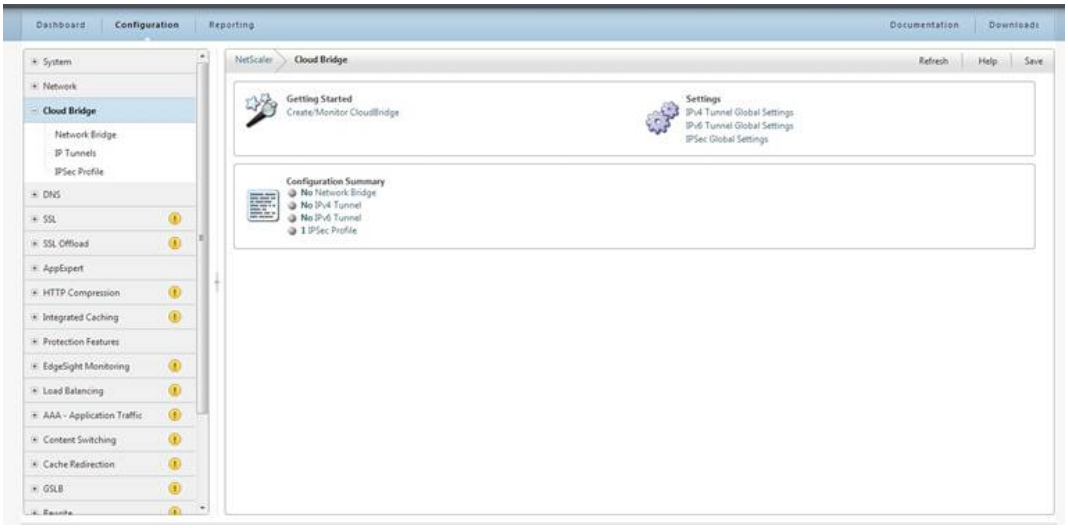
Before configuring a CloudBridge between two VPC instances (to extend your network and implement redundancy and backup functionality), make sure that you have publically accessible IP addresses for both the VPCs. These publically accessible IP addresses are used to create the connection between the two VPC locations.

You must log on to the CloudBridge VPX instance in one of the AWS VPC and connect to the CloudBridge VPX instance in the other AWS VPC (consider this one to be the remote cloud). To create the connection, use the remove instance's AWS credentials (Access key and Secret Access key) and IP address.

To configure a CloudBridge between two CloudBridge VPX instances in different VPCs by using the configuration utility

1. Access the configuration utility by using the web browser to connect to the IP address of one of the CloudBridge instances in AWS.

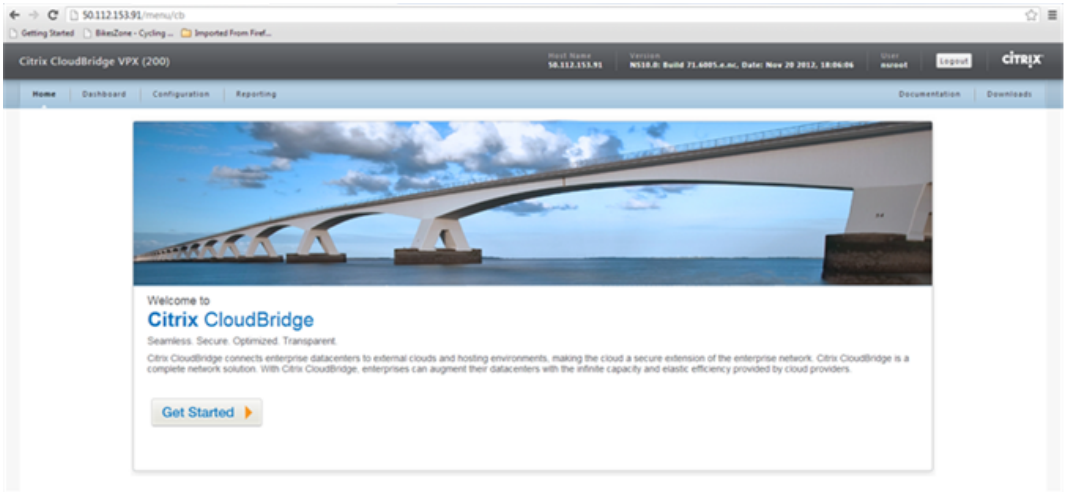
2. On the Configuration tab, in the Navigation pane, click CloudBridge.



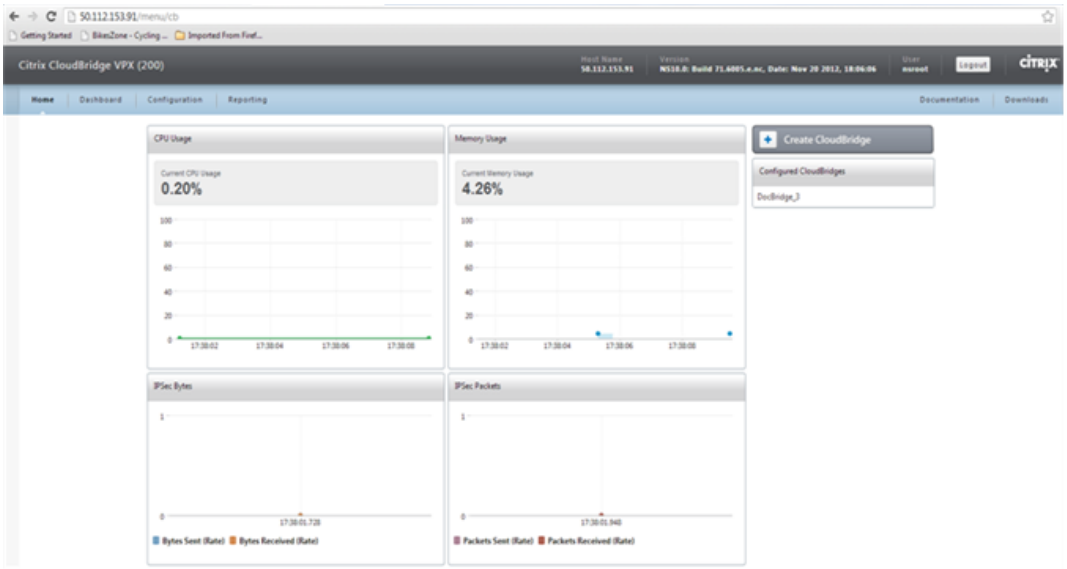
Note: This screen appears only when you are using a platinum edition license. For other licenses, you are taken to Step 4 or Step 5 depending on whether CloudBridge is already configured on the CloudBridge VPX instance.

3. In the right pane, under Getting Started, click Create/Monitor CloudBridge.

4. Click Get Started.

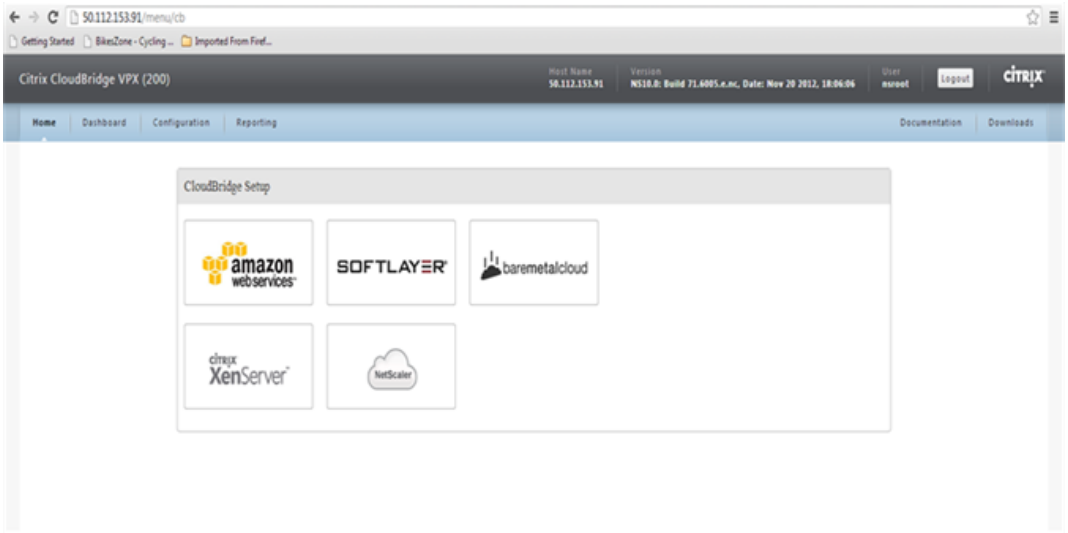


Note: If you already have a network bridge configured on the CloudBridge VPX instance, this screen does not appear. Instead, you are taken to the Citrix CloudBridge VPX page. Click Create CloudBridge to proceed.

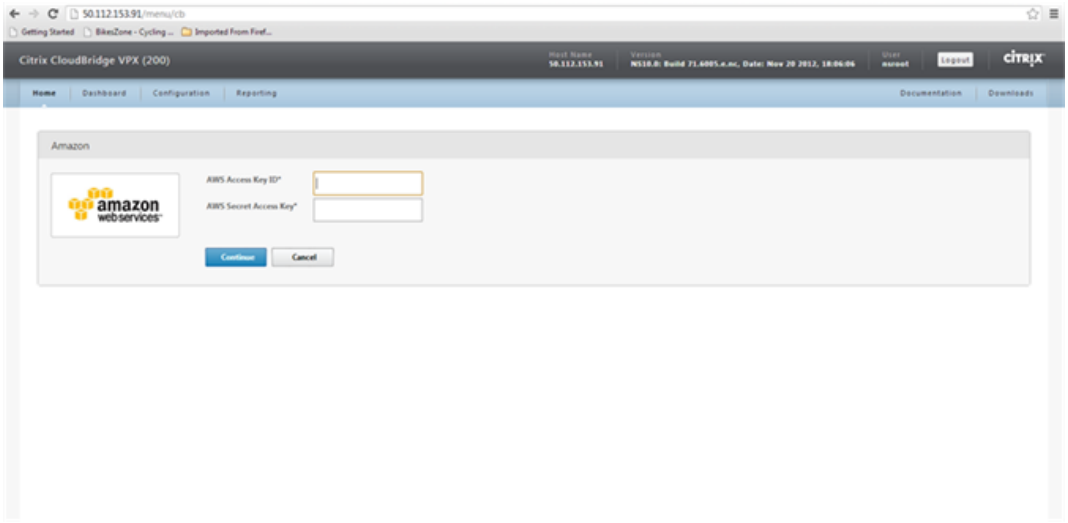


Note: If you are configuring the first network bridge on an instance, this screen does not appear. Instead, after the Get Started page you are taken to the next page (**CloudBridge Setup**).

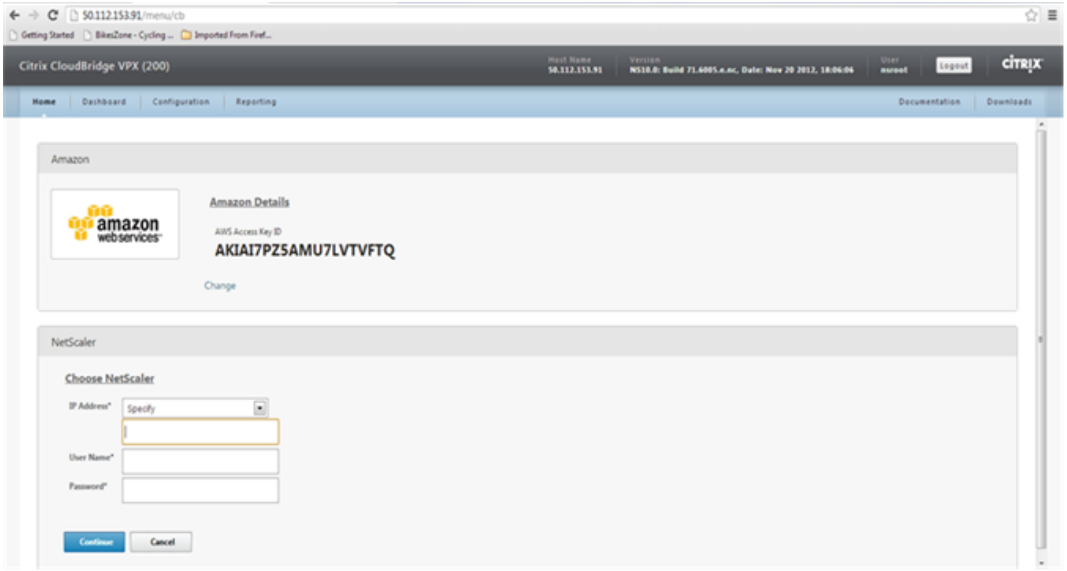
5. In the CloudBridge Setup pane, click amazon web services.



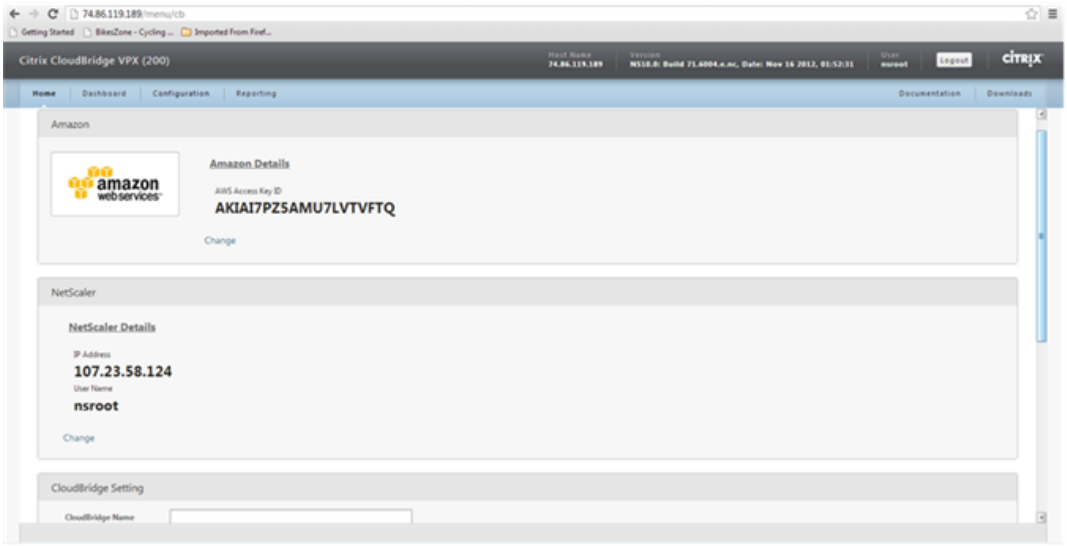
6. In the Amazon pane, type the values for the access keys in the AWS Access Key ID and AWS Secret Access Key text boxes, and then click Continue. You can obtain these access keys from the AWS GUI console.



7. In the NetScaler pane, either select an IP address from the IP Address drop-down list or type the IP address, user name, and password in the corresponding text boxes for the local CloudBridgeVPX instance in the AWS cloud, and then click Continue. The IP address should be a publicly accessible address.



8. In the CloudBridge Setting pane, in the CloudBridge Name text box, type the name of the CloudBridge that you want to create.



9. Under **Local Setting**, from the Subnet IP drop-down list, select the subnet IP address of the local CloudBridge instance.

10. Select the NetScaler Behind NAT checkbox and, in the IP Address text box, type the public IP address (EIP) that is mapped to the subnet IP you selected in step 9.

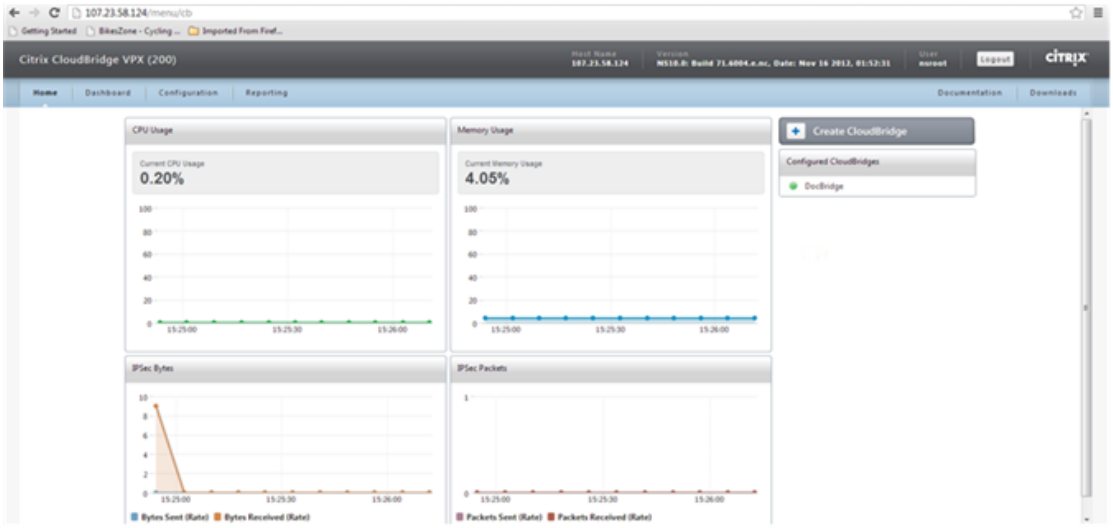
11. Under **Remote Setting**, from the Subnet IP drop-down list, select the subnet IP address of the remote CloudBridge instance.

12. Select the **NetScaler Behind NAT** checkbox and, in the **IP Address** text box, type the public IP address (EIP) that is mapped to the subnet IP you selected in step 11.

13. Under **Security Settings**, from the **Encryption Algorithm** and **Hash Algorithm** drop-down lists, select the algorithms that you want to use.

14. Select the **Specify Key** option and, in the **Pre Shared Security Key** text box, type the security key. Click **Done**.

The new CloudBridge instance appears on the **Home** page. The current status of the CloudBridge is indicated in the **Configured CloudBridge** pane. A green dot indicates that the tunnel is up. A red dot indicates that the tunnel is down.



To configure a CloudBridge between two CloudBridge VPX instances in different VPCs by using the command line

To set up a CloudBridge between two CloudBridge VPX instances in different VPCs:

- Create a network bridge
- Configure an IPSec profile
- Create a GRE tunnel with the IPSec profile
- Bind the IPSec tunnel with the network bridge

To create a network bridge by using the command line

At the local CloudBridge instance (in the local VPC) command prompt, type:

add netbridge <*name*>

Parameter for configuring a network bridge

name

Name of the CloudBridge that you are configuring must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

To configure IPSec profile by using the command line

At the local CloudBridge instance (in the local VPC) command prompt, type:

addipsec profile <name> [-encAlgo (AES | 3DES) ...] [-hashAlgo<hashAlgo> ...]
[-lifetime<positive_integer>] (-psk
|(-publickey<string>-privatekey<string>-peerPublicKey<string>))

Parameters for configuring an IPSec profile

name

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

encAlgo

Encryption algorithm to be used in IPSec configuration for a CloudBridge. Possible values: AES, 3DES.

hashAlgo

Encryption algorithm to be used in IPSec configuration for a CloudBridge. Possible values: HMAC_SHA1, HMAC_SHA256, HMAC_MD5. Default: HMAC_SHA1.

lifetime

Time, in seconds, after which the security association expires. After expiration, new SAs are established, and new cryptographic keys are negotiated between the peers connected by the CloudBridge. Maximum value: 31536000. Default: 28800.

psk

Text string, called the pre-shared key, to be manually configured on each peer. The pre-shared keys of the peers are matched against each other for authentication before security associations are established. Therefore, for the authentication to be successful, you must configure the same pre-shared key on both of the peers of the CloudBridge. Maximum Length: 63 characters.

livenessCheckInterval

Time, in seconds, after which a notify payload is sent to check the status of the peer (UP or DOWN). Additional payloads are sent as specified by the retransmit interval setting. A value of zero disables liveliness checks.

retransmissiontime

Time, in seconds, after which an IKE retry message is sent to a peer. The retry message is sent upto three times. Each failure doubles the amount of time before sending another retry message.

publickey

A local digital certificate to be used to authenticate the local CloudBridge appliance to the remote peer before establishing IPSec security associations. The same certificate should be present and set for the Peer Public Key parameter in the remote peer.

privatekey

Private key of the local digital certificate.

peerPublicKey

Digital certificate of the remote peer. This certificate is used to authenticate the remote peer to the local peer before establishing IPSec security associations. The same certificate should be present and set for the Public key parameter in the remote peer.

To create a GRE tunnel with IPSec profile by using the command line

At the local CloudBridge instance (in the local VPC) command prompt type:

add iptunnel <name><remoteIp><remoteSubnetMask><localIp>-type -protocol (GRE) -ipsecprofile<name>

Parameters for creating a GRE tunnel with IPSec profile

name

Name of the IP Tunnel. This alphanumeric string is required and cannot be changed after the service group is created. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.),

space, colon (:), at (@), equals (=), and hyphen (-) characters.

remoteIp

A public IP address of the remote CloudBridge appliance, in AWS, used to set up the tunnel.

remoteSubnetMask

Subnet mask of the remote IP address of the tunnel.

localIp

A public address of the local CloudBridge instance used to set up the tunnel. Possible values: Auto, MIP, SNIP, and VIP. Default: Auto.

protocol

The protocol to be used in setting up the IP tunnel. Select GRE to set up a GRE tunnel.

ipsecProfileName

Name of the IPSec profile that is used for securing communication in the GRE tunnel. If this parameter is not specified, the default profile (ns_ipsec_default_profile) is configured and, if this parameter is set to none, a GRE tunnel is created.

To bind IPSec tunnel to the network bridge by using the command line

At the local CloudBridge instance (in the local VPC) command prompt, type:

bindnetbridge<name> [-tunnel<name>] [-vlan<id>] [-IPAddress<ip_addr|ipv6_addr>]

Parameters for binding IPSec tunnel to the network bridge

name

Name of the CloudBridge that you are configuring.Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

tunnel

Name of the GRE tunnel to be associated with the CloudBridge.

VLAN

Identifier of the local VLAN that needs to be extended to the cloud.

IPAddress

The IPV4 subnet that needs to be extended to the cloud.

Parameter Descriptions (of commands listed in the CLI procedure)

add netbridge

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

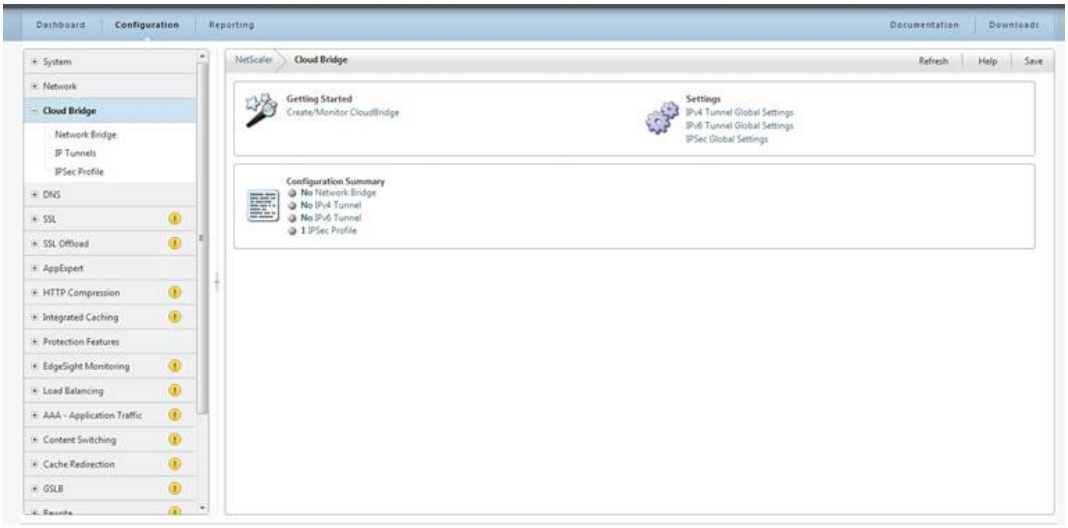
Configuring CloudBridge from AWS to Data Center

To configure a CloudBridge between AWS cloud and your data center from the CloudBridge VPX instance in the AWS cloud, you log on into the CloudBridge VPX instance in AWS and connect to the CloudBridge instance in the data center.

To configure CloudBridge from a CloudBridge VPX in the AWS cloud to a CloudBridge instance in the data center by using the configuration utility

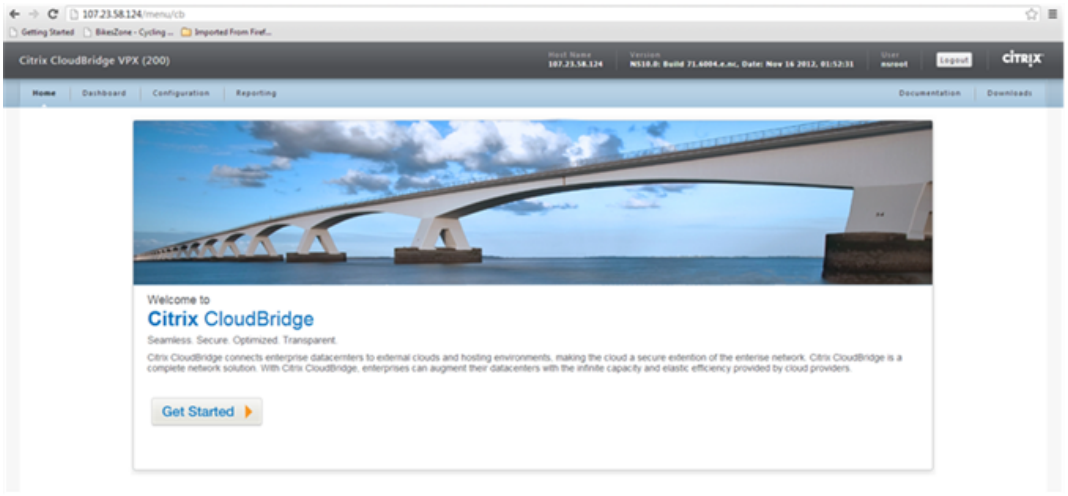
1. Access the configuration utility by using a web browser to connect to the IP address of the CloudBridge instance in the AWS cloud.

2. On the Configuration tab, in the Navigation pane, click CloudBridge.

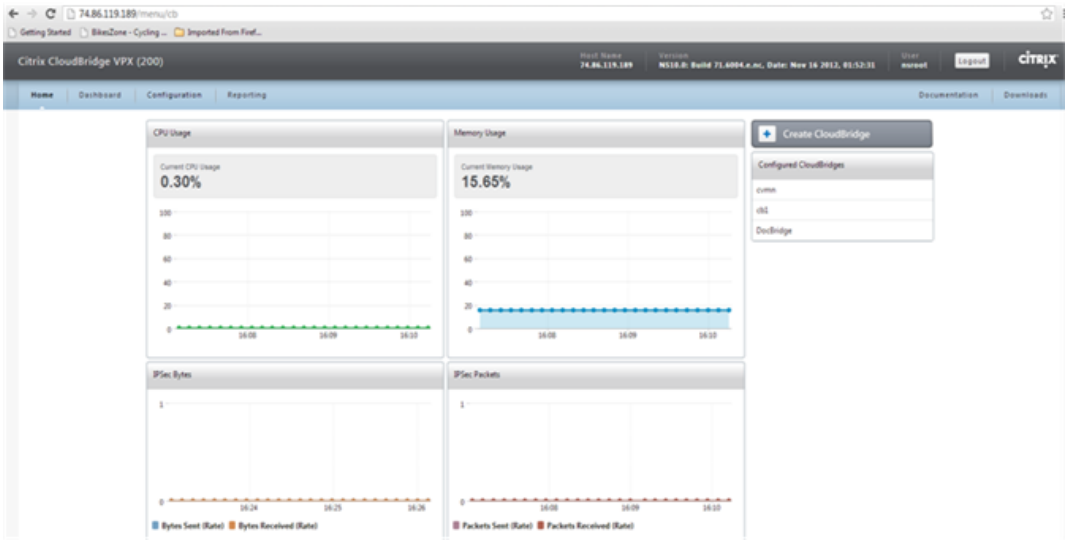


3. In the right pane, under **Getting Started**, click Create/Monitor CloudBridge.

4. Click Get Started.

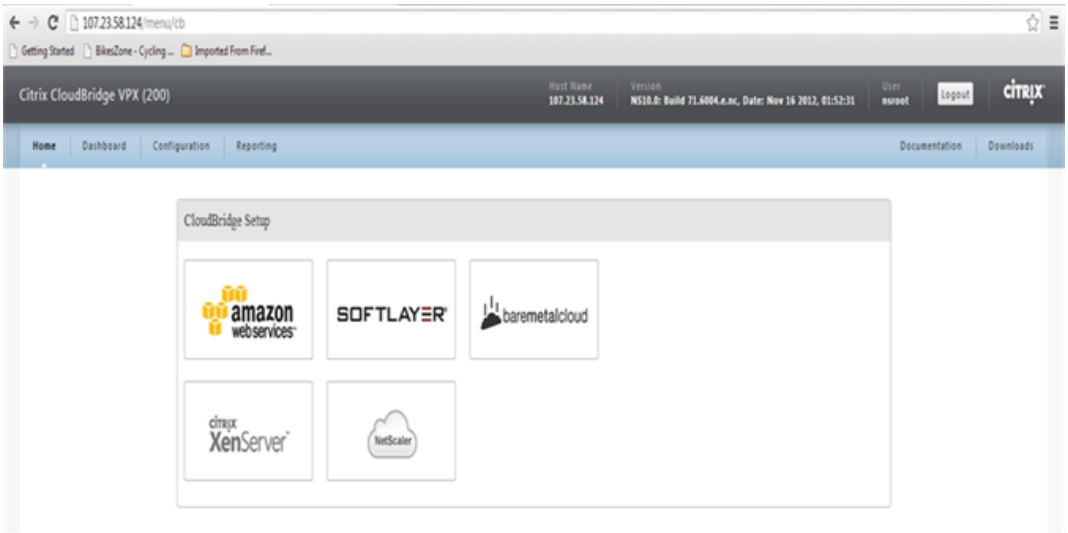


Note: If you already have a network bridge configured on the CloudBridge VPX, this screen does not appear. Instead, you are taken to the **CitrixCloudBridge VPX** page. Click **Create CloudBridge** to proceed.

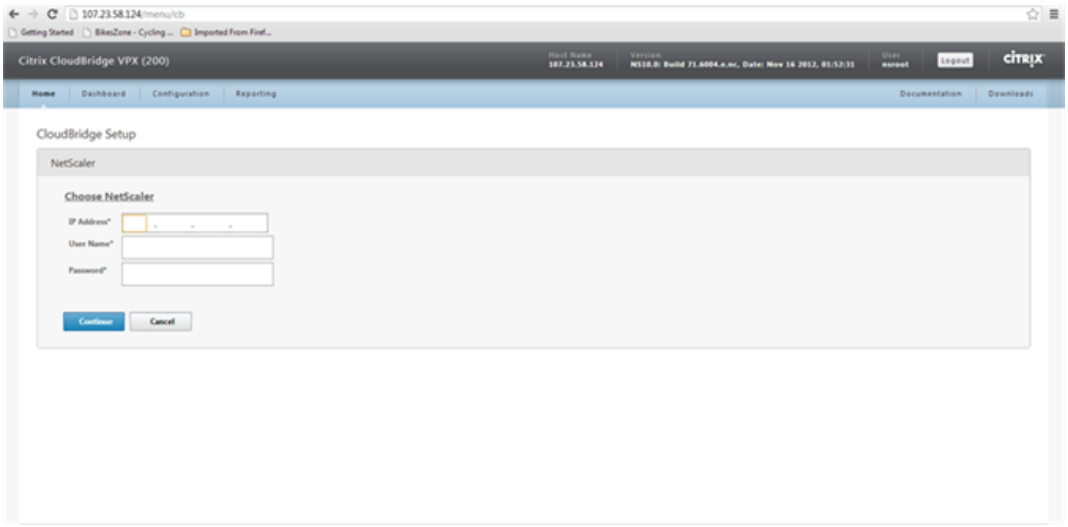


Note: If you are configuring first network bridge on an instance, this screen does not appear. Instead, after the **Get Started** page you are taken to the next page (**CloudBridge Setup**).

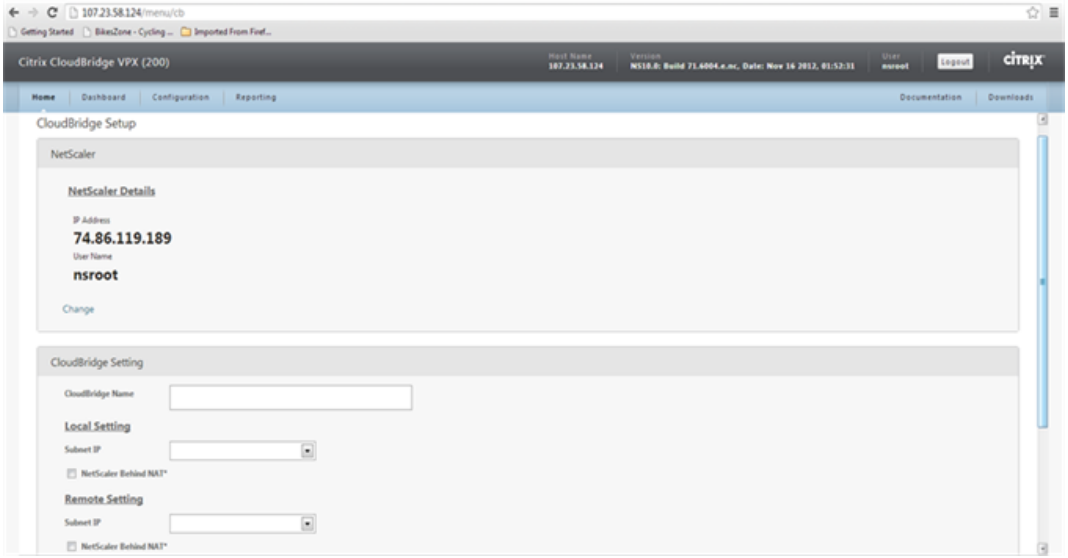
5. In the CloudBridge Setup pane, click NetScaler.



6. In the NetScaler pane, type values in the **IP Address**, **User Name**, and **Password** text boxes for the CloudBridge VPX instance on AWS, and then click Continue. The IP address should be a publicly accessible address.



7. In the **CloudBridge Setting** pane, in the **CloudBridge Name** text box, type the name of the CloudBridge that you want to create.



8. Under **Local Setting**, from the **Subnet IP** drop-down list, select the subnet IP address of the CloudBridge VPX appliance on AWS.

9. Under **Remote Setting**, from the **Subnet IP** drop-down list, select the subnet IP address of the CloudBridge instance in the data center. The subnet IP address should not be the NSIP.

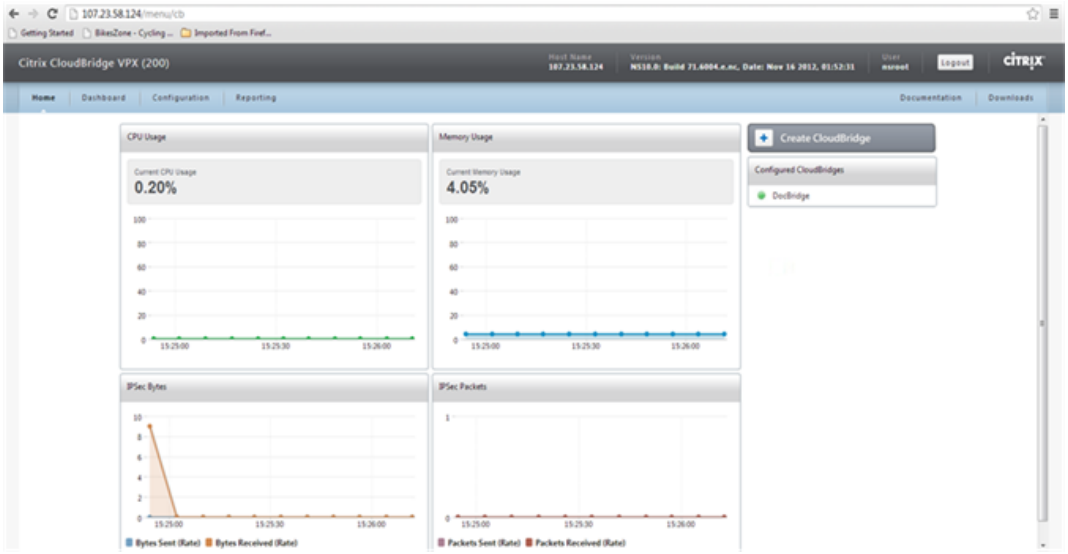
10. Select the **NetScaler Behind NAT** checkbox and, in the **IP Address** text box, type the public IP address (EIP) that is mapped to the subnet IP you selected in step 9.

11. Under **Security Settings**, from the **Encryption Algorithm** and **Hash Algorithm** drop-down lists, select the algorithms that you want to use.

12. Select the **Specify Key** option and, in the **Pre Shared Security Key** text box, type the security key.

13. Click **Done**.

The new CloudBridge instance appears on the **Home** page. The current status of the CloudBridge is indicated in the **Configured CloudBridges** pane. A green dot indicates that the tunnel is up. A red dot indicates that the tunnel is down.



To configure CloudBridge from a CloudBridge VPX in the AWS cloud to a CloudBridge instance in the data center by using the command line

To set up a CloudBridge, on the CloudBridge instance in the AWS:

- Create a network bridge
- Configure an IPsec profile
- Create a GRE tunnel with the IPsec profile
- Bind the IPsec tunnel to the network bridge

To create a network bridge by using the command line

At the local CloudBridge instance (in the AWS VPC) command prompt, type:

addnetbridge<name>

Parameter for configuring a network bridge

name

Name of the CloudBridge that you are configuring. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equal (=), and hyphen (-) characters.

To configure an IPsec profile by using the command line

At the local CloudBridge instance (in the AWS VPC) command prompt, type:

addipsec profile<name> [-encAlgo (AES | 3DES) ...] [-hashAlgo<hashAlgo> ...] [-lifetime<positive_integer>] (-psk |(-publickey<string> -privatekey<string> -peerPublicKey<string>))

Parameters for configuring an IPsec profile

name

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

encAlgo

Encryption algorithm to be used in IPsec configuration for a CloudBridge. Possible values: AES, 3DES.

hashAlgo

Encryption algorithm to be used in IPsec configuration for a CloudBridge. Possible values: HMAC_SHA1, HMAC_SHA256, HMAC_MD5. Default: HMAC_SHA1.

lifetime

Time, in seconds, after which the security association expires. After expiration, new SAs are established, and new cryptographic keys are negotiated between the peers connected by the CloudBridge. Maximum value: 31536000. Default: 28800.

psk

Text string, called the pre-shared key, to be manually configured on each peer. The pre-shared keys of the peers are matched against each other for authentication before security associations are established. Therefore, for the authentication to be successful, you must configure the same pre-shared key on both of the peers of the CloudBridge. Maximum Length: 63 characters.

livenessCheckInterval

Time, in seconds, after which a notify payload is sent to check the status of the peer (UP or DOWN). Additional payloads are sent as specified by the retransmit interval setting. A value of zero disables liveliness checks.

retransmissiontime

Time, in seconds, after which an IKE retry message is sent to a peer. The retry message is sent upto three times. Each failure doubles the amount of time before sending another retry message.

publickey

A local digital certificate to be used to authenticate the local CloudBridge appliance to the remote peer before establishing IPsec security associations. The same certificate should be present and set for the Peer Public Key parameter in the remote peer.

privatekey

Private key of the local digital certificate.

peerPublicKey

Digital certificate of the remote peer. This certificate is used to authenticate the remote peer to the local peer before establishing IPsec security associations. The same certificate should be present and set for the Public key parameter in the remote peer.

To create GRE tunnel with an IPsec profile by using the command line

At the local CloudBridge instance (in the AWS VPC) command prompt type:

add iptunnel <name> <remoteIp> <remoteSubnetMask> <localIp> -type -protocol (GRE) -ipsecprofile <name>

Parameters for creating a GRE tunnel with IPsec profile

name

Name of the IP Tunnel. This alphanumeric string is required and cannot be changed after the service group is created. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equal (=), and hyphen (-) characters.

remoteIp

A public IP address of the remote CloudBridge appliance, in the data center, used to set up the tunnel.

remoteSubnetMask

Subnet mask of the remote IP address of the tunnel.

localIp

A public address of the local CloudBridge instance used to set up the tunnel. Possible values: Auto, MIP, SNIP, and VIP. Default: Auto.

protocol

The protocol to be used in setting up the IP tunnel. Select GRE to set up a GRE tunnel.

ipsecProfileName

Name of the IPsec profile that is used for securing communication in the GRE tunnel. If this parameter is not specified, the default profile (ns_ipsec_default_profile) is configured and, if this parameter is set to none, a GRE tunnel is created.

To bind IPsec tunnel to the network bridge by using the command line

At the local CloudBridge instance (in the AWS VPC) command prompt, type:

bindnetbridge<name> [-tunnel<name>] [-vlan<id>] [-IPAddress<ip_addr|ipv6_addr>]

Parameters for binding an IPsec tunnel to the network bridge

name

Name of the CloudBridge that you are configuring. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

tunnel

Name of the GRE tunnel to be associated with the CloudBridge.

VLAN

Identifier of the local VLAN that needs to be extended to the cloud.

IPAddress

The IPV4 subnet that needs to be extended to the cloud.

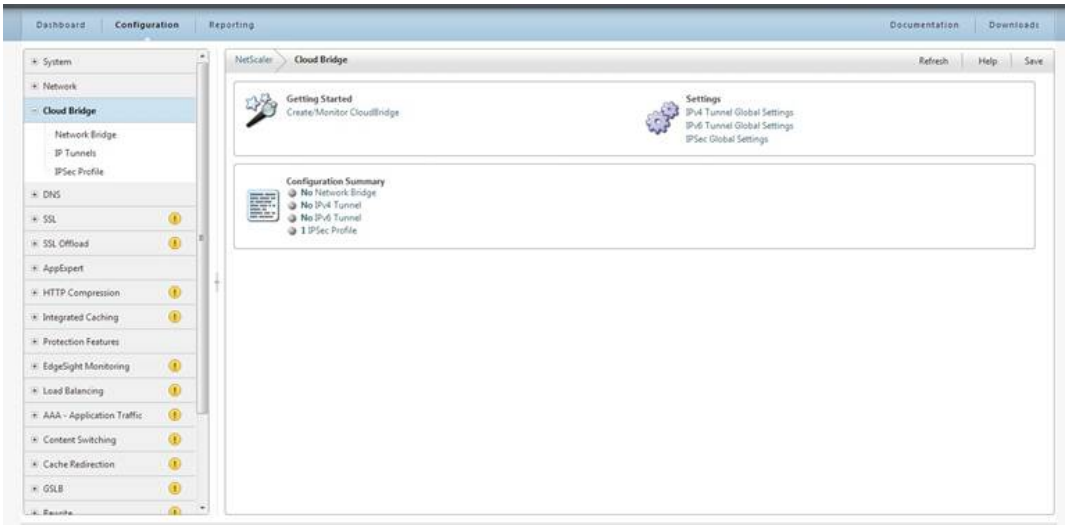
Configuring a CloudBridge between Two Data Centers

You can configure a CloudBridge between two different data centers to extend your network without reconfiguring the setup, and leverage the capabilities of the two data centers. Having a CloudBridge configured between the two geographically separated data centers enables you to implement redundancy and safeguard your setup from failure. The applications available across the two data centers appear as local to the user.

To configure CloudBridge between two CloudBridge instances in two different data centers by using the configuration utility

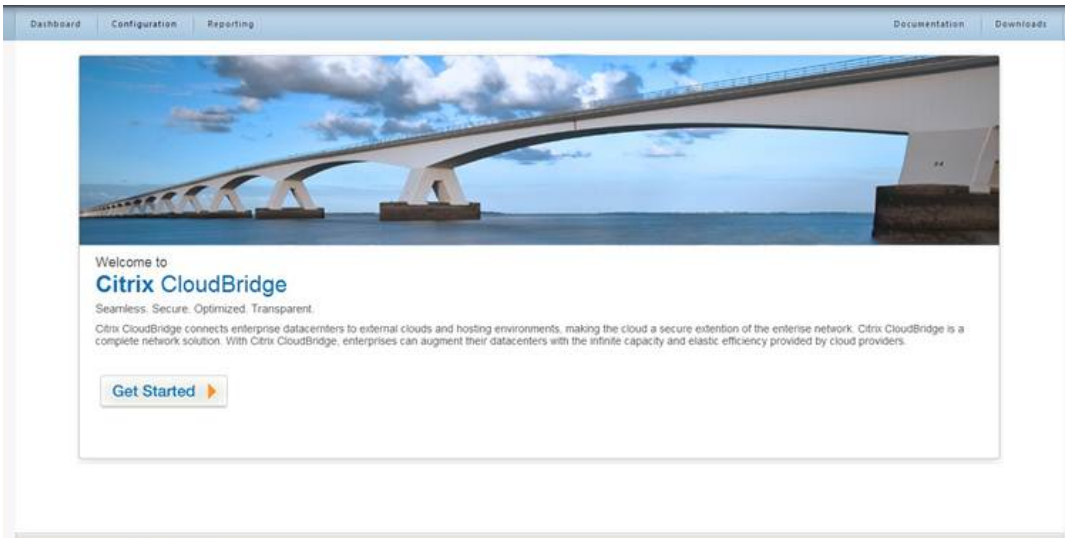
1. Access the configuration utility by using a web browser to connect to the IP address of the CloudBridge instance in the local data center.

2. On the **Configuration** tab, in the Navigation pane, click CloudBridge.

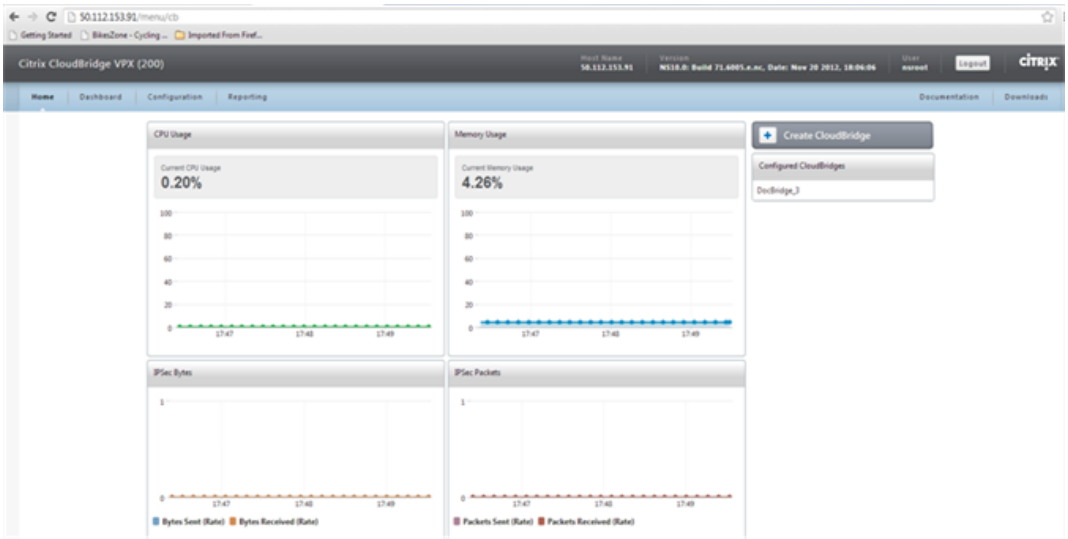


3. In the right pane, under **Getting Started**, click Create/Monitor CloudBridge.

4. Click Get Started.

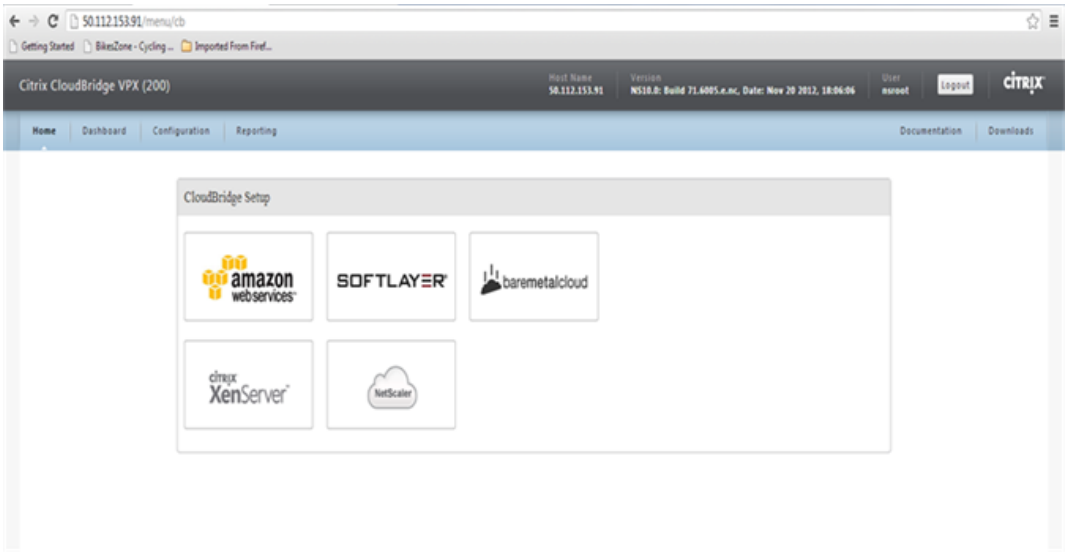


Note: If you already have a network bridge configured on the CloudBridge VPX, this screen does not appear. Instead, you are taken to the **CitrixCloudBridge VPX** page. Click **Create CloudBridge** to proceed.

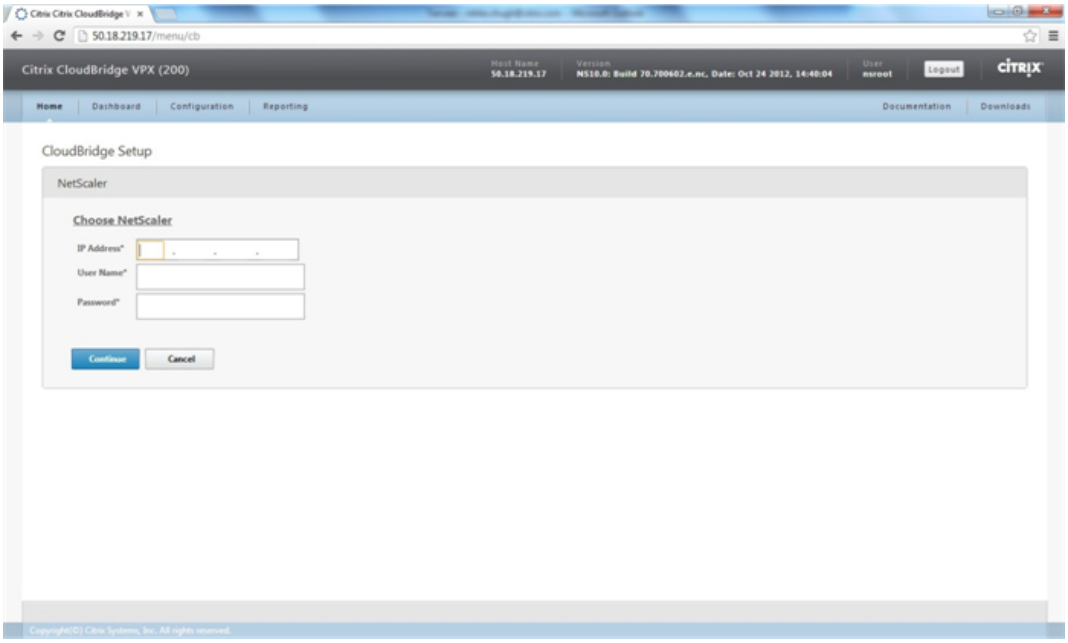


Note: If you are configuring the first network bridge on an instance, this screen does not appear. Instead, after the **Get Started** page you are taken to the next page (**CloudBridge Setup**).

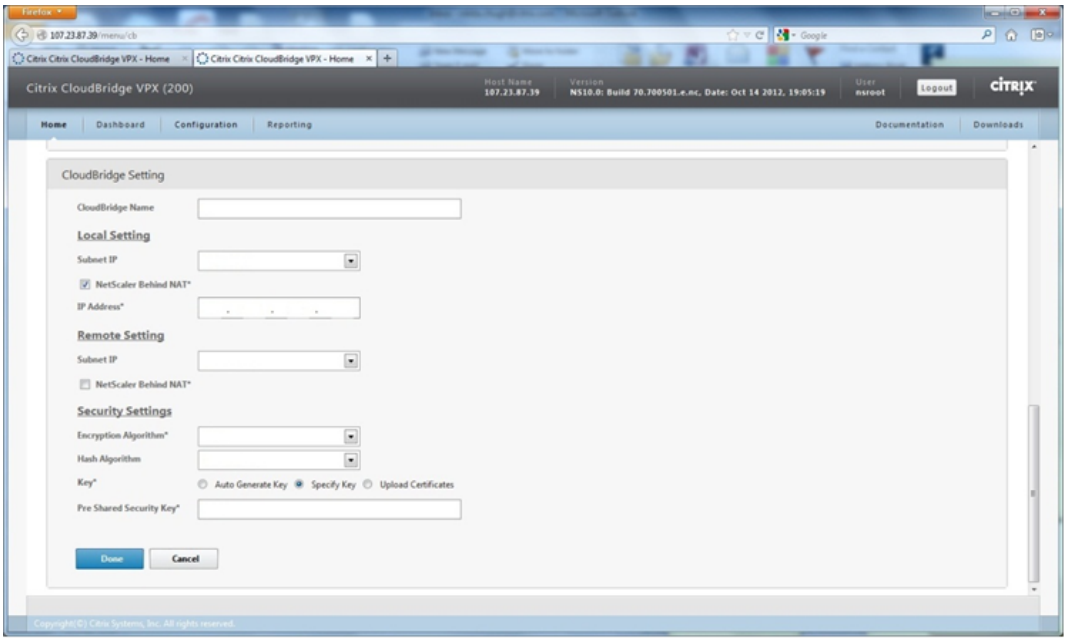
5. In the CloudBridge Setup pane, click NetScaler.



6. In the NetScaler pane, type values in the **IP Address**, **User Name**, and **Password** text boxes for the local CloudBridge instance in the data center, and then click Continue. The IP address should be a publicly accessible address.



7. In the **CloudBridge Setting** pane, in the **CloudBridge Name** text box, type the name of the CloudBridge that you want to create.



8. Under **Local Setting**, from the **Subnet IP** drop-down list, select the subnet IP address of the CloudBridge instancein the local data center.

9. Under **Remote Setting**, from the **Subnet IP** drop-down list, select the subnet IP address of the CloudBridge instance in the remote data center.

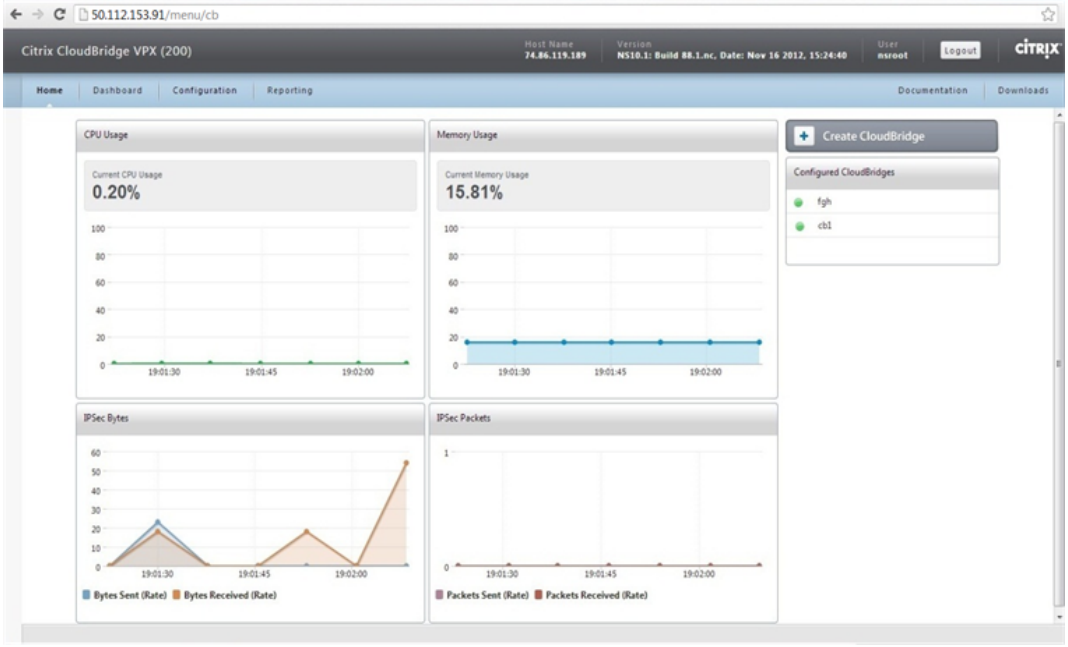
10. Select the **NetScaler Behind NAT** checkbox and, in the **IP Address** text box, type the public IP address (EIP) that is mapped to the subnet IP that you selected in step 9.

11. Under **Security Settings**, from the **Encryption Algorithm** and **Hash Algorithm** drop-down lists, select the algorithms that you want to use.

12. Select the **Specify Key** option and, in the **Pre Shared Security Key** text box, type the security key.

13. Click **Done**.

    The new CloudBridge instance appears on the**Home** page. The current status of the CloudBridge is indicated in the **Configured CloudBridges** pane. A green dot indicates that the tunnel is up. A red dot indicates that the tunnel is down.



To configure CloudBridge between two CloudBridge instances in two different data centers by using the command line

To set up a CloudBridge, between two CloudBridge VPX instances in two different data centers:

- Create a network bridge
- Configure an IPSec profile
- Create a GRE tunnel with the IPSec profile
- Bind the IPSec tunnel to the network bridge

To create a network bridge by using the command line

At the CloudBridge instance (in the local data center) command prompt, type:

addnetbridge<name>

Parameter for configuring a network bridge

name

Name of the CloudBridge that you are configuring.Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters.

To configure an IPSec profile by using the command line

At the CloudBridge instance (in the local data center) command prompt, type:

addipsec profile<name> [-encAlgo (AES | 3DES) ...] [-hashAlgo<hashAlgo> ...] [-lifetime<positive_integer>] (-psk |(-publickey<string> -privatekey<string> -peerPublicKey<string>))

Parameters for configuring an IPSec profile

name

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

encAlgo

Encryption algorithm to be used in IPSec configuration for a CloudBridge. Possible values: AES, 3DES.

hashAlgo

Encryption algorithm to be used in IPSec configuration for a CloudBridge. Possible values: HMAC_SHA1, HMAC_SHA256, HMAC_MD5. Default: HMAC_SHA1.

lifetime

Time, in seconds, after which the security association expires. After expiration, new SAs are established, and new cryptographic keys are negotiated between the peers connected by the CloudBridge. Maximum value: 31536000. Default: 28800.

psk

Text string, called the pre-shared key, to be manually configured on each peer. The pre-shared keys of the peers are matched against each other for authentication before security associations are established. Therefore, for the authentication to be successful, you must configure the same pre-shared key on both of the peers of the CloudBridge. Maximum Length: 63 characters.

livenessCheckInterval

Time, in seconds, after which a notify payload is sent to check the status of the peer (UP or DOWN). Additional payloads are sent as specified by the retransmit interval setting. A value of zero disables liveliness checks.

retransmissiontime

Time, in seconds, after which an IKE retry message is sent to a peer. The retry message is sent upto three times. Each failure doubles the amount of time before sending another

retry message.

publickey

A local digital certificate to be used to authenticate the local CloudBridge appliance to the remote peer before establishing IPSec security associations. The same certificate should be present and set for the Peer Public Key parameter in the remote peer.

privatekey

Private key of the local digital certificate.

peerPublicKey

Digital certificate of the remote peer. This certificate is used to authenticate the remote peer to the local peer before establishing IPSec security associations. The same certificate should be present and set for the Public key parameter in the remote peer.

To create a GRE tunnel with IPSec profile by using the command line

At the CloudBridge instance (in the local data center) command prompt type:

add iptunnel <name><remoteIp><remoteSubnetMask><localIp>-type -protocol (GRE) -ipsecprofile<name>

Parameters for creating a GRE tunnel with an IPSec profile

name

Name of the IP Tunnel. This alphanumeric string is required and cannot be changed after the service group is created. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

remoteIp

A public IP address of the remote CloudBridge appliance, in the data center, used to set up the tunnel.

remoteSubnetMask

Subnet mask of the remote IP address of the tunnel.

localIp

A public address of the local CloudBridge instance used to set up the tunnel. Possible values: Auto, MIP, SNIP, and VIP. Default: Auto.

protocol

The protocol to be used in setting up the IP tunnel. Select GRE to set up a GRE tunnel.

ipsecProfileName

Name of the IPSec profile that is used for securing communication in the GRE tunnel. If this parameter is not specified, the default profile (ns_ipsec_default_profile) is

configured and, if this parameter is set to none, a GRE tunnel is created.

To bind an IPSec tunnel to the network bridge by using the command line

At the CloudBridge instance (in the local data center) command prompt, type:

bindnetbridge<name> [-tunnel<name>] [-vlan<id>] [-IPAddress<ip_addr|ipv6_addr>]

Parameters for binding IPSec tunnel to the network bridge

name

Name of the CloudBridge that you are configuring. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equal (=), and hyphen (-) characters.

tunnel

Name of the GRE tunnel to be associated with the CloudBridge.

VLAN

Identifier of the local VLAN that needs to be extended to the cloud.

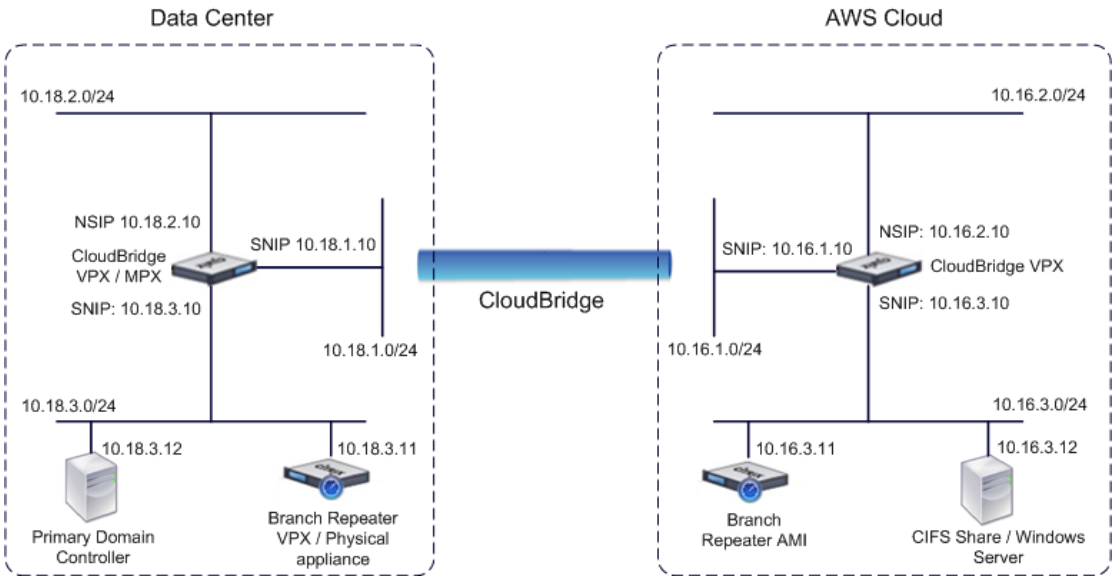
IPAddress

The IPV4 subnet that needs to be extended to the cloud.

WAN Optimization for CloudBridge tunnel

You should configure the CloudBridge appliances at both ends of the CloudBridge tunnel to send traffic through the Branch Repeater appliances.

Consider an example where a CloudBridge tunnel is configured between Amazon Web Services (AWS) cloud and a data center. For optimizing the traffic flow in CloudBridge tunnel, on the AWS end, you configure and launch a Branch Repeater virtual appliance (AMI) on AWS and pair it with a CloudBridge virtual appliance (VPX) on AWS. On the data center end, you configure a Branch Repeater virtual appliance (VPX)/physical appliance and pair it with a CloudBridge VPX/MPX appliance.



The following table lists the settings used in the AWS cloud end.

Entities	Settings
Subnets used for the CloudBridge tunnel setup	10.16.1.0/24
	10.16.2.0/24
	10.16.3.0/24
CloudBridge VPX settings	
Instance Name	CloudBridge-Cloud
SNIP	10.16.1.10
SNIP	10.16.3.10
NSIP	10.16.2.10

Branch Repeater AMI settings	
Instance Name	BranchRepeater-Cloud
IP Address	10.16.3.11

The following table lists the settings used in the data center end.

Entities	Settings
Subnets used for the CloudBridge tunnel setup	10.18.1.0/24
	10.18.2.0/24
	10.18.3.0/24
CloudBridge VPX/MPX settings	
SNIP	10.18.1.10
SNIP	10.18.3.10
NSIP	10.18.2.10
Branch Repeater VPX/physical appliance settings	
IP Address	10.18.3.11

You need to perform the following tasks for pairing Branch Repeaters appliances to the CloudBridge tunnel endpoints.

- **Instantiating a Branch Repeater virtual appliance (AMI) on AWS**. This task involves installing, configuring, and launching a Branch Repeater virtual appliance (AMI) on the AWS in the same AWS region where the CloudBridge VPX is running. After the Branch Repeater AMI is instantiated, you need to disable the Source/Destination check feature of the AMI instance from the AWS management interface. Then, you must enable SNMP Monitoring on the Branch Repeater AMI instance and grant SNMP monitoring access to the paired CloudBridge VPX on AWS by using the Branch Repeater management graphical user interface.

- **Setting up a Branch Repeater virtual appliance (VPX)/physical appliance in the data center**. This task involves deploying and configuring a Branch Repeater physical appliance or installing, configuring, and launching a Branch Repeater virtual appliance (VPX) in a virtualization platform in the datacenter.

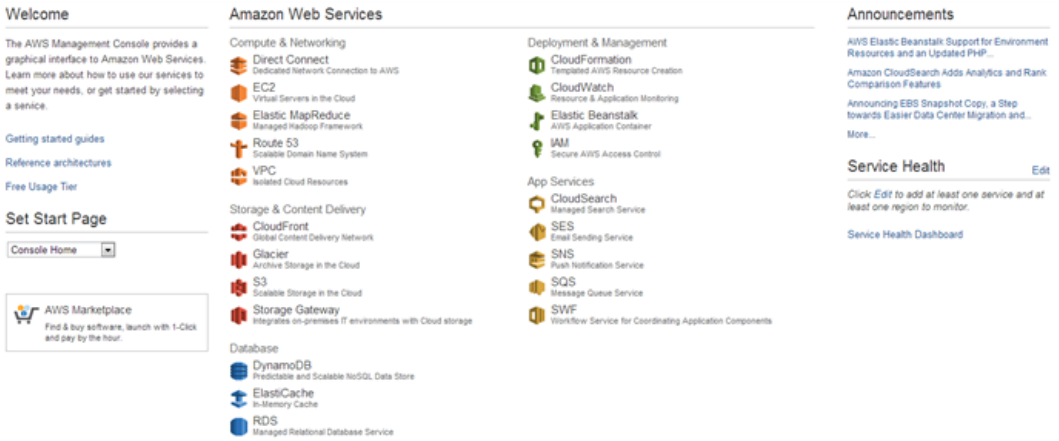
- **Redirecting traffic to the Branch Repeater appliances**. This task involves the use of Dynamic Load Balancing wizard for Citrix Branch Repeater on the CloudBridge appliance to pair with the respective Branch Repeater appliance at either ends of the CloudBridge.

Instantiating a Branch Repeater Virtual Appliance (AMI) on AWS

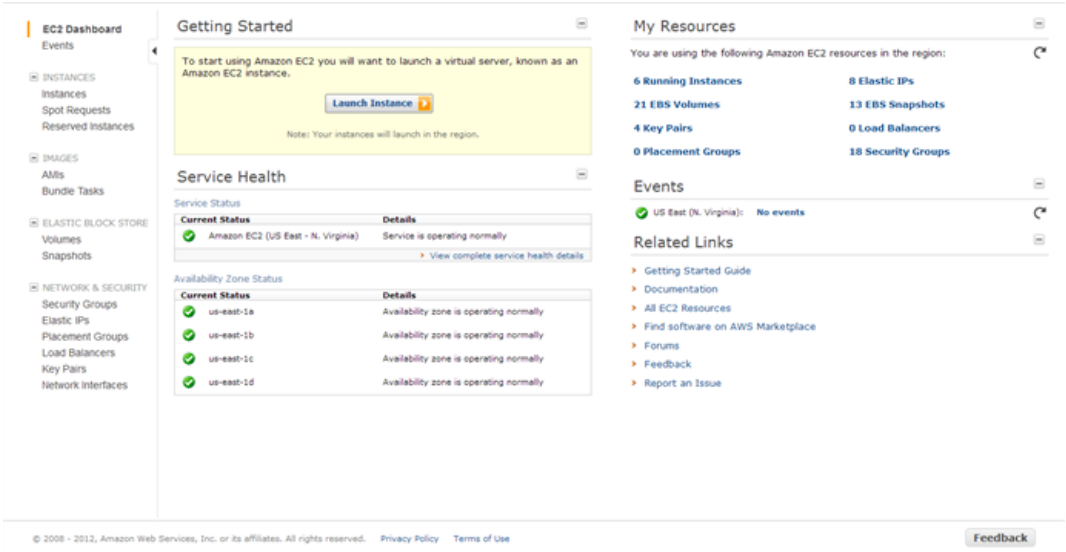
To install a Branch Repeater virtual appliance in an AWS VPC, you need an AWS account. You can create an AWS account at http://aws.amazon.com/. Branch Repeater is available as an Amazon Machine Image (AMI) in AWS Marketplace.

To instantiate a Branch Repeater virtual appliance (AMI) on AWS

1. In a web browser, type http://aws.amazon.com/.
2. Click My Account/Console, and then click My Account to open the Amazon Web Services Sign in page.
3. Use your Amazon account credentials to sign in.
4. On the Manage Your Account page, in the Account section, click the AWS Management Console link.
5. On the AWS Management Console page, click Sign in to the AWS Console to log on to the Management Console page.
6. On the Amazon Web Services page, click EC2 in the Compute & Networking section.



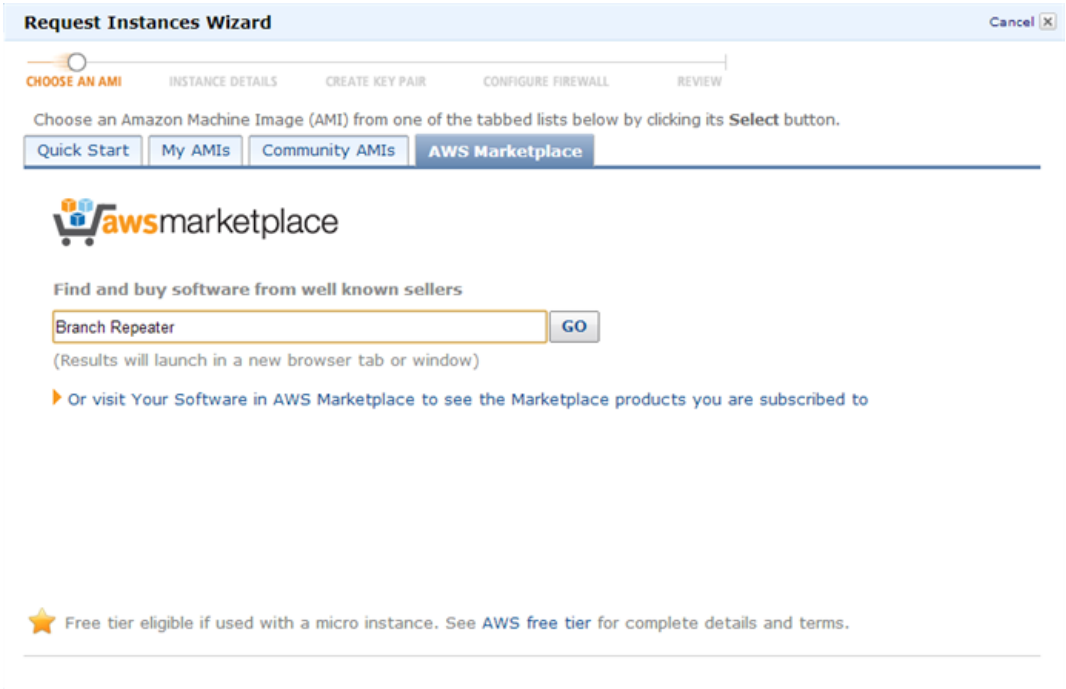
7. On the Amazon EC2 Console Dashboard page, in the Getting Started section, click Launch Instance.



8. In the Create a New Instance dialog box, select AWS Marketplace, and then click Continue to open the Request Instance Wizard.

9. In the Request Instance Wizard dialog box, click AWS Marketplace tab.

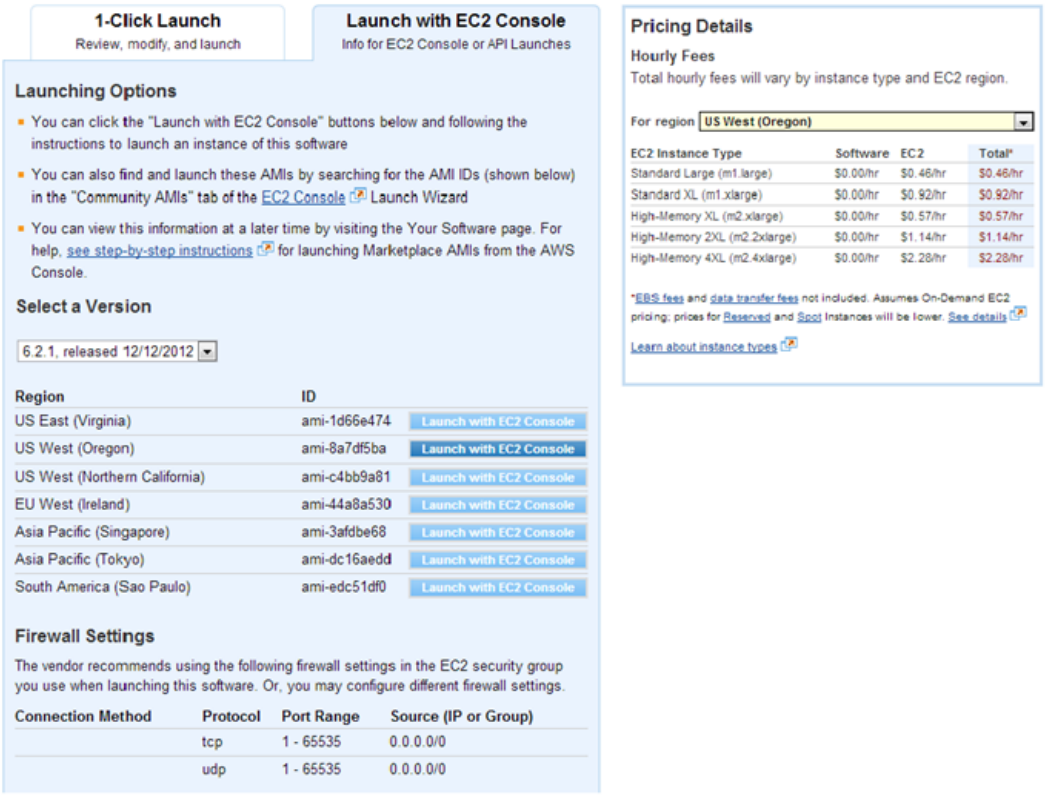
10. In the Search text field, type `Branch Repeater` to search for the Branch Repeater AMI, and click Go.



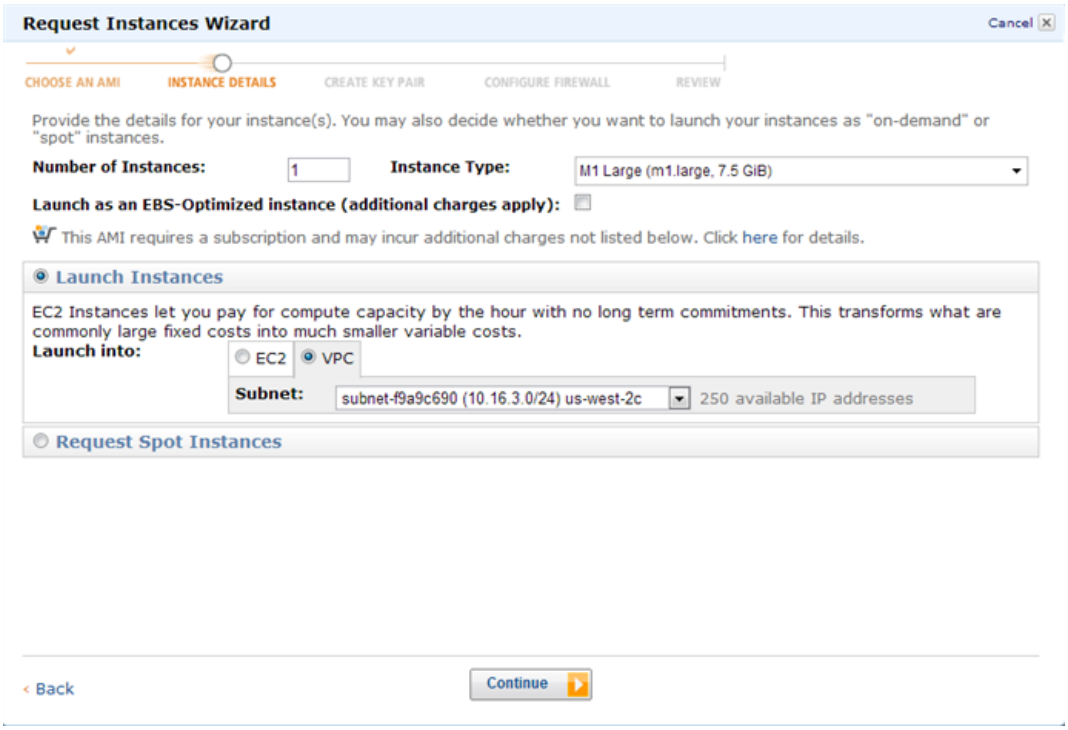
11. On the search result page, click Citrix Branch Repeater for CloudBridge.

12. On the Citrix Branch Repeater for CloudBridge page, click Continue.

13. On the Launch with EC2 Console tab, click Launch with EC2 Console for the region where you want to launch Citrix Branch Repeater AMI.



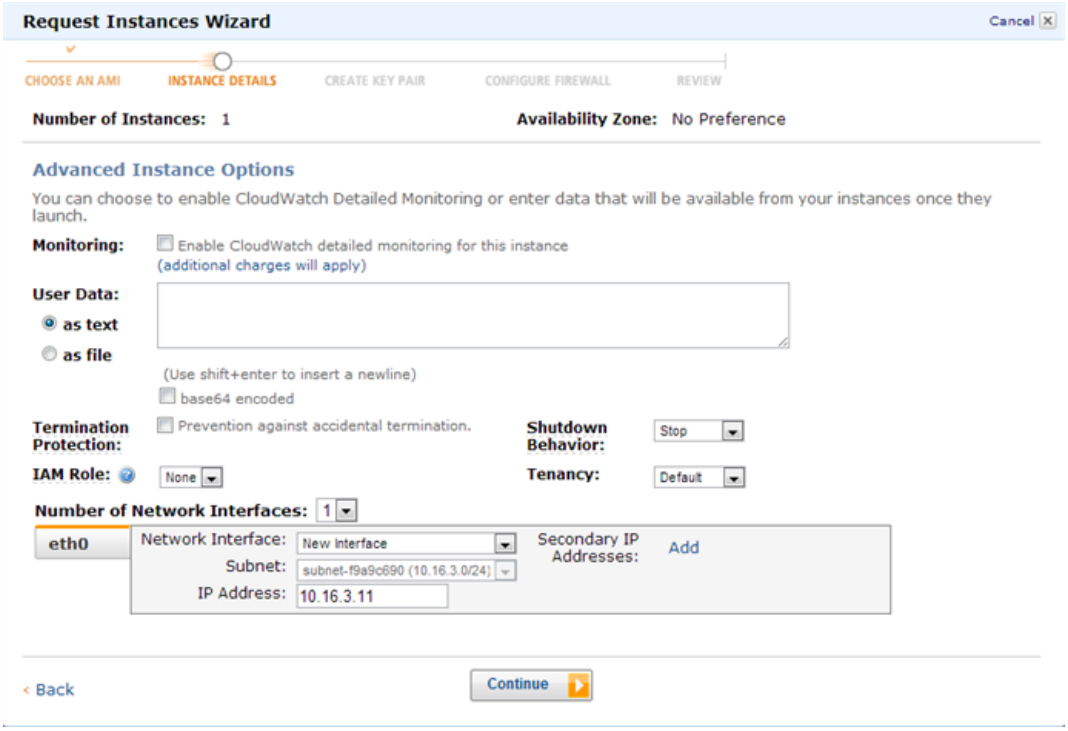
14. On the Request Instance Wizard page, type 1 in the Number of Instances text box, and from the Instance Type drop-down list, select Large (m1.large, 7.5GIB).



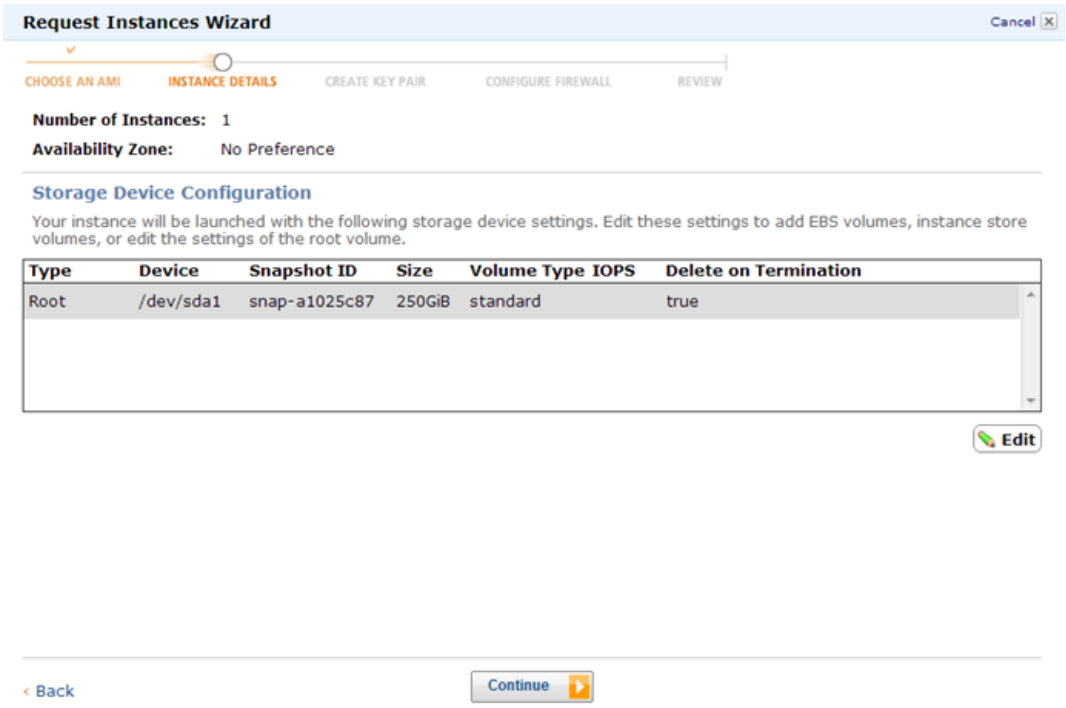
15. In the Launch Instances section, click the VPC tab. Then, from the Subnet drop-down list, select the private network subnet, and then click Continue.

16. On the next page, in the Advanced Instance Options section, verify the value for Number of Network Interfaces and eth0 details, such as Network Interface, Subnet, and IP Address, and then click Continue.

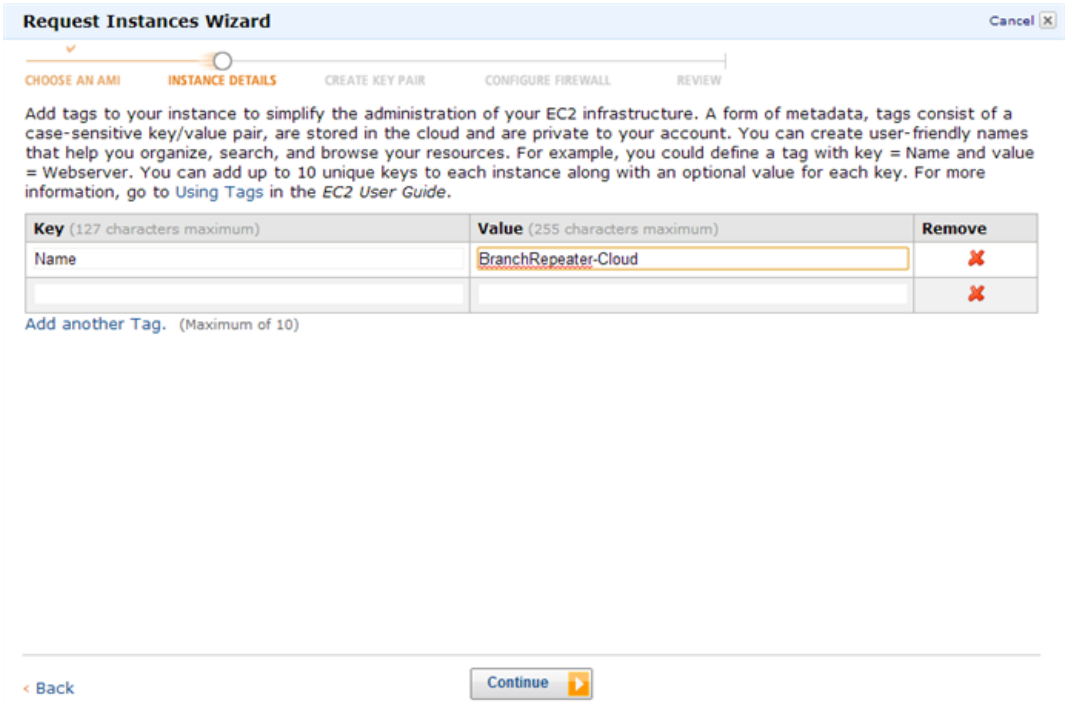
    Note: Branch Repeater AMI is not supported with more than one network interface. Therefore, the value of Number of Network Interfaces field should be set only to 1.



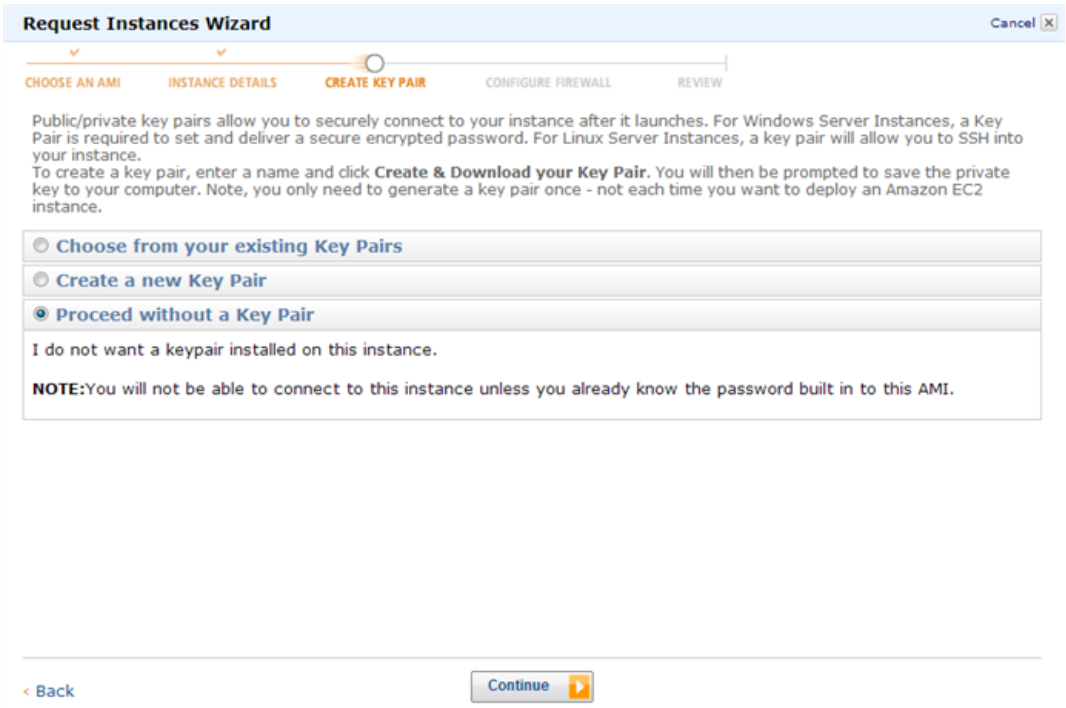
17. On the Request Instances Wizard page, verify the storage device configuration information and click Continue.



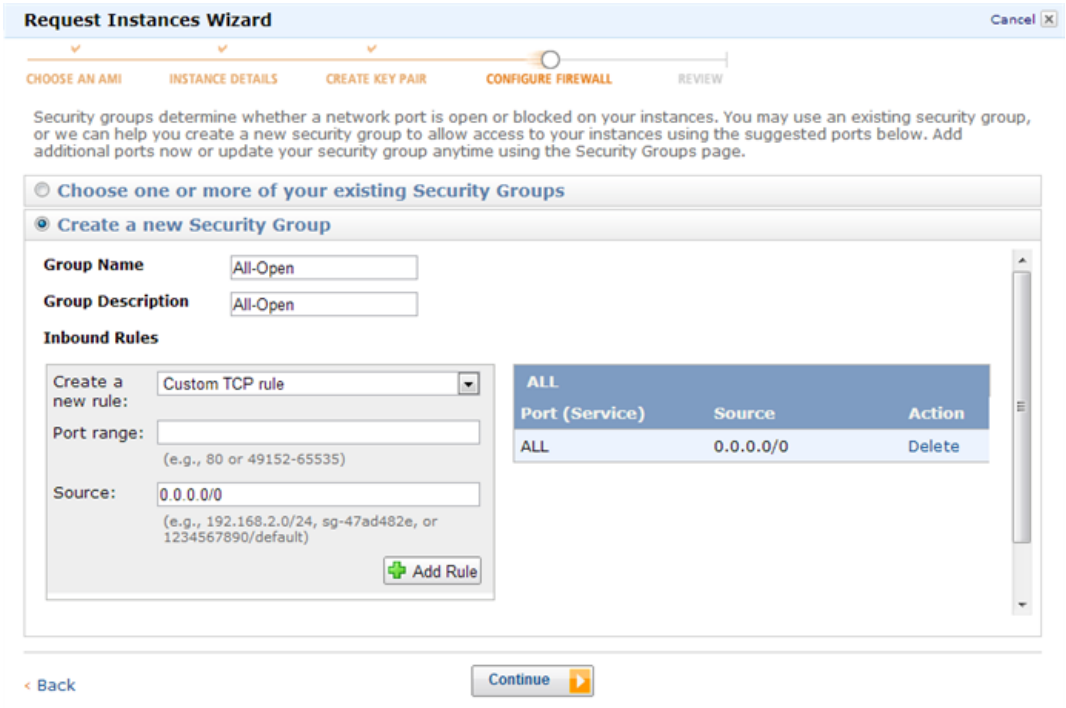
18. On the Request Instances Wizard page, enter a name for the EC2 instance in the Value text box, and then click Continue.



19. On the Request Instances Wizard page, select Proceed without a Key Pair, and then click Continue.

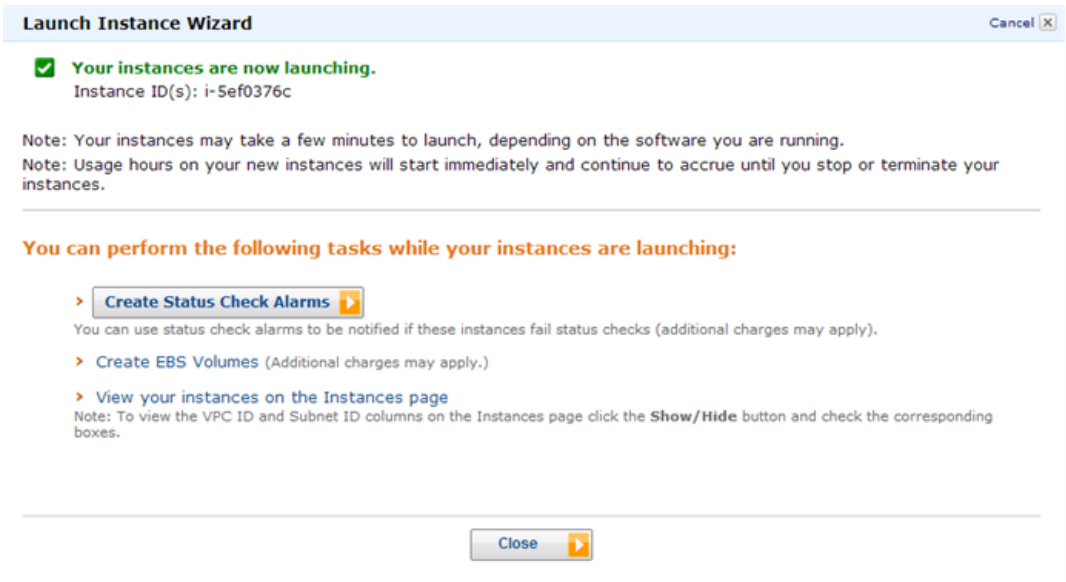


20. On the Request Instances Wizard page, select Create a new Security Group, then create a group that allows all the traffic to pass from the list, and then click Continue.



21. On the Request Instances Wizard page, verify the EC2 instance configuration details, and then click Launch to launch the EC2 instance.

22. Click Close to close the Launch Instance Wizard dialog box. The new EC2 instance is launched successfully.



Disabling the Source/Destination Check Feature

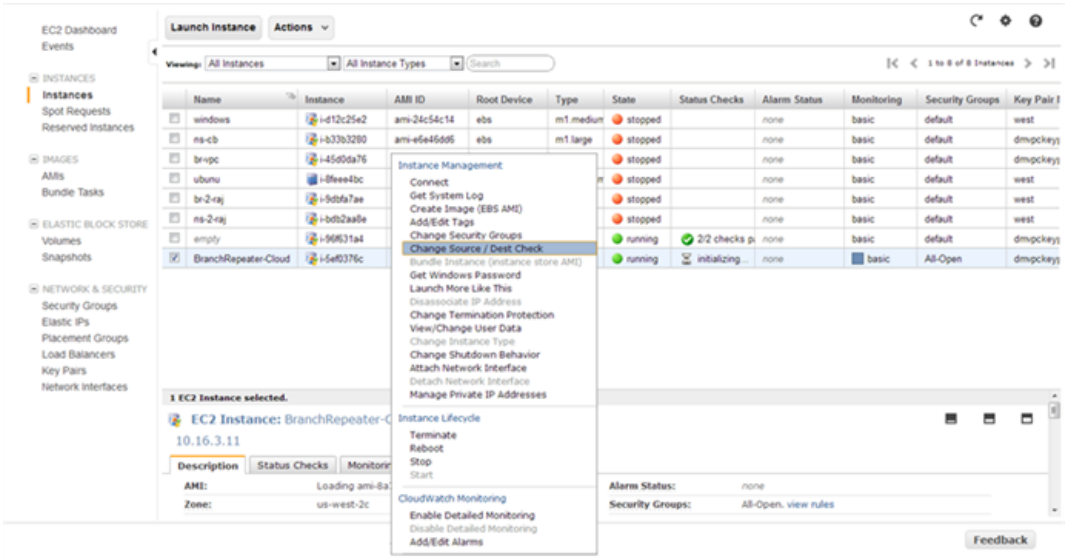
You must disable the Source/Destination check feature of Branch Repeater AMI instance for it to work properly on AWS.

To disable the Source/Destination check feature

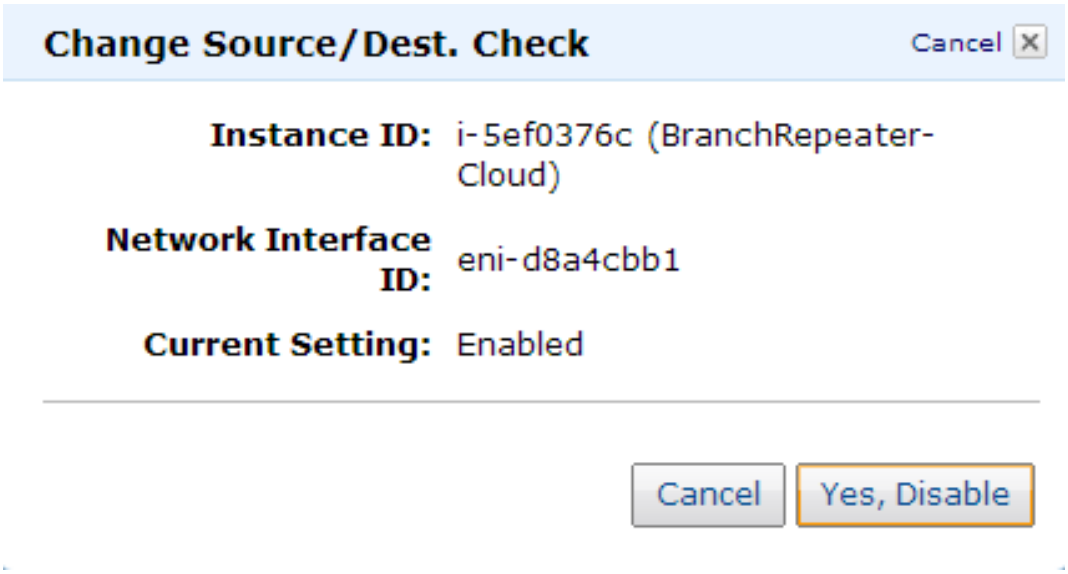
1. On the Amazon EC2 Console Dashboard page, in the navigation pane, click instances. The new EC2 instance should appear in the My Instances list.

2. Select the new EC2 instance. The instance details appear in the EC2 Instances pane.

3. Right-click the new EC2 instance and then select Change Source/Dest Check from the popup menu.



4. In the Change Source / Dest. Check dialog box, click Yes, Disable to disable the feature.

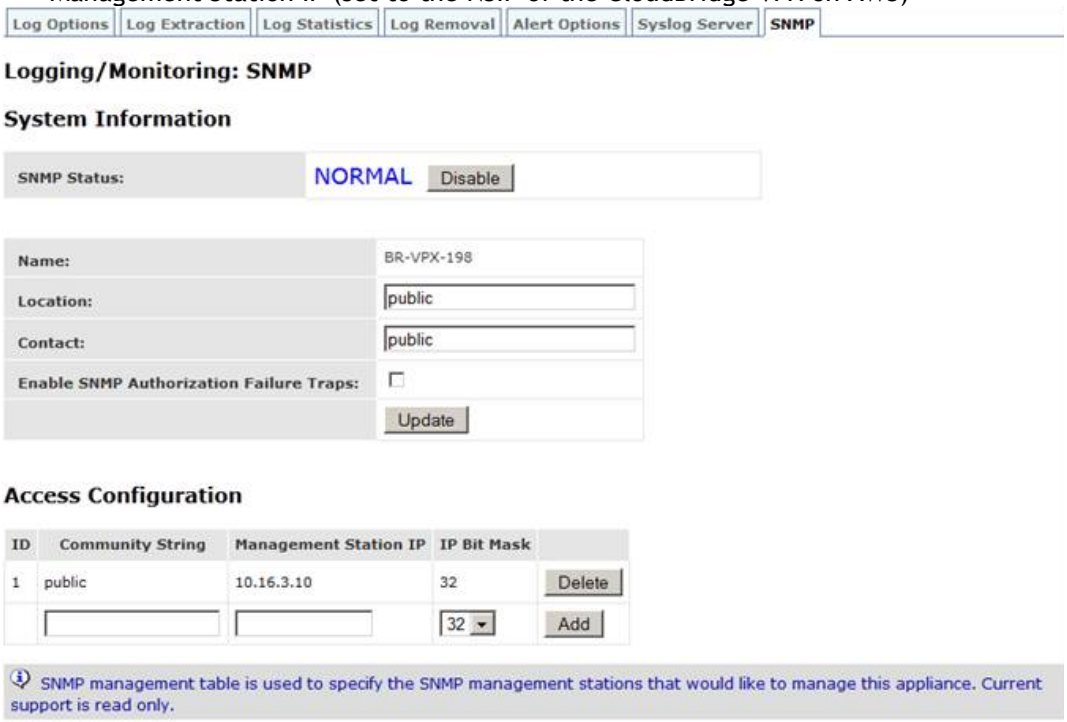


Configuring SNMP Monitoring on the Branch Repeater AMI on AWS

You must enable SNMP monitoring on the Branch Repeater AMI on AWS. Also, you must grant SNMP monitoring access to the paired CloudBridge VPX on AWS by adding its NSIP on the Branch Repeater AMI instance.

To configure SNMP monitoring on the Branch Repeater AMI by using the Branch Repeater graphical user interface

1. In the navigation pane, expand Configuration, and then click Logging/Monitoring.
2. In the details pane, click the SNMP tab.
3. In the System Information section, in the SNMP Status row, click Enable. This action enables SNMP monitoring on the Branch Repeater AMI instance.
4. In the Access Configuration section, add SNMP monitoring access to CloudBridge VPX appliance by setting the following parameters:
   - Community String (set to the string public)
   - Management Station IP (set to the NSIP of the CloudBridge VPX on AWS)



5. Click Add.

Limitations and Usage Guidelines for Branch Repeater AMI Instances on AWS

- High Availability setup for Branch Repeater AMI instances is not supported.
- Branch Repeater AMI instance in Group Mode is not supported.
- Branch Repeater plug-ins are not supported.
- Tagged VLAN is not supported because of the inherent limitation of AWS.
- Traffic shaping is not supported.
- You may create only an m1.large Branch Repeater AMI instance on AWS.
- IP address/gateway/subnet assignment using the Branch Repeater management user interface is not supported.
- Console access is not available for Branch Repeater AMI instance on AWS.
- It is not possible to install licenses on a Branch Repeater AMI instance on AWS. The Branch Repeater AMI instance is automatically licensed and rate limiting is controlled by the CloudBridge instance, which is paired with the Branch Repeater AMI instance.
- While configuring the Branch Repeater instance, you may not change the disk size, which has a default value of 250 GB. A higher capacity disk does not increase the available Disk Based Compression (DBC) cache size.

Setting up the Branch Repeater Appliance in the Datacenter

Before you set up a Branch Repeater virtual appliance (VPX) or physical appliance in the datacenter, provision the virtual appliance or rack mount the hardware appliance.

For instructions for rack mounting a Branch Repeater physical appliance, or provisioning a Branch Repeater VPX instance, see Branch Repeaters.

These setup instructions assume that the Branch Repeater in the datacenter is deployed in one-arm mode. References to an *appliance* apply to virtual appliances (VPX) as well as physical appliances.

After you have installed and completed the initial configuration of the Branch Repeater appliance, configure the interfaces on the NetScaler and Branch Repeater appliances so that they can communicate with each other. Also configure the virtual inline and TCP Maximum Segment Size (MSS) settings on the Branch Repeater appliance.

Configuring the Network at the Datacenter

By default, the first and second interfaces on the Branch Repeater appliance are bridged. Configure one network interface on the NetScaler appliance and the first network interface on the Branch Repeater appliance to be part of the client subnet. For the second interface on the Branch Repeater appliance, do the following (assuming a one-arm configuration):

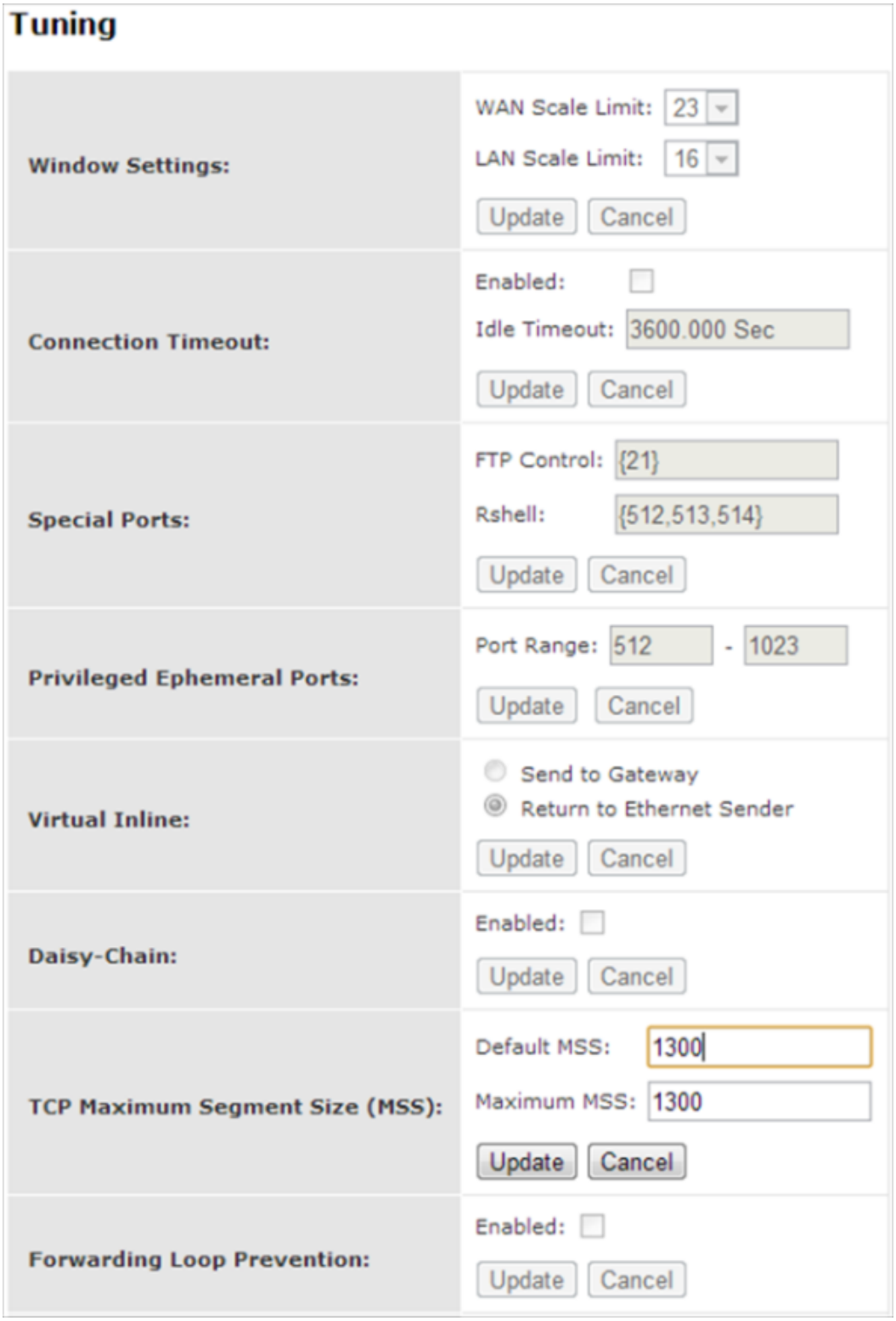
- If the Branch Repeater appliance is a physical appliance, do not connect the interface to the network.
- If the Branch Repeater appliance is a virtual appliance, configure a dummy internal network. Make sure that the second of the bridged ports is the only interface in the dummy internal network.

Configuring the TCP MSS and Virtual Inline Settings on the Branch Repeater

The configuration on the Branch Repeater appliance (either a physical appliance or a virtual appliance) in the datacenter must match the configuration on the Branch Repeater instance in the Amazon VPC. Branch Repeater AMI instances on AWS have a preconfigured value of 1300 for both the default and maximum values of TCP Maximum Segment Size (MSS). Additionally, the Virtual Inline option should be set to Return to Ethernet Sender, so that packets are returned to the CloudBridge appliance. Therefore, you must configure these settings on the datacenter Branch Repeater appliance.

To configure the TCP MSS and Virtual Inline settings on a Branch Repeater appliance in the datacenter

1. Log on to the Branch Repeater appliance in the datacenter.
2. From the Configuration menu, click Tuning.



3. On the Tuning page, do the following:

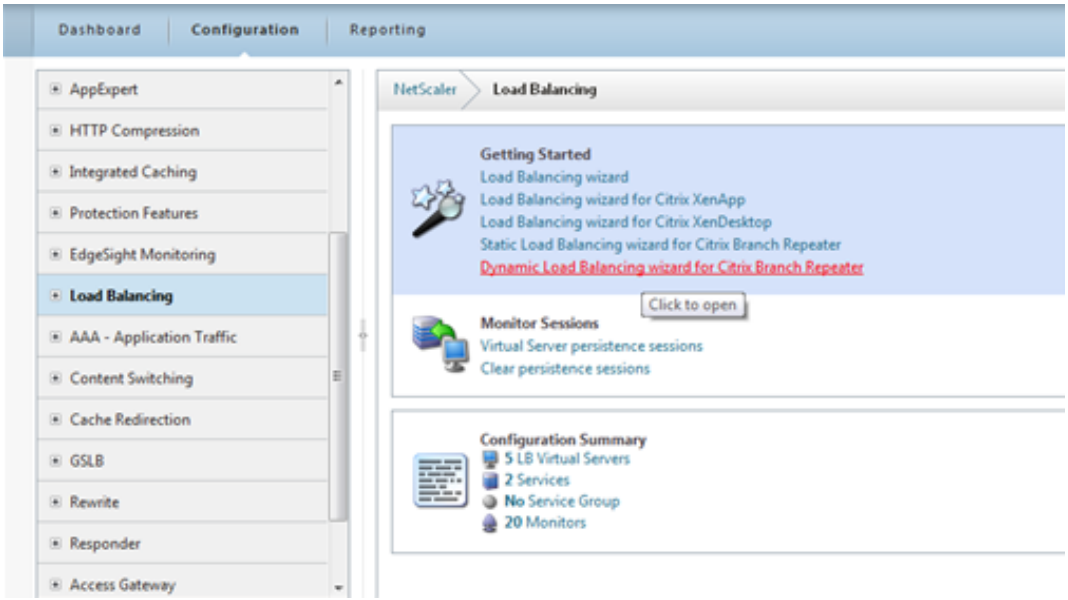
   - In the Virtual Inline row, select Return to Ethernet Sender, and then click Update.
   - In the TCP Maximum Segment Size (MSS) row, in the Default MSS and Maximum MSS boxes, enter 1300, and then click Update.

Redirecting Traffic to the Branch Repeater Appliances from the CloudBridge Appliance

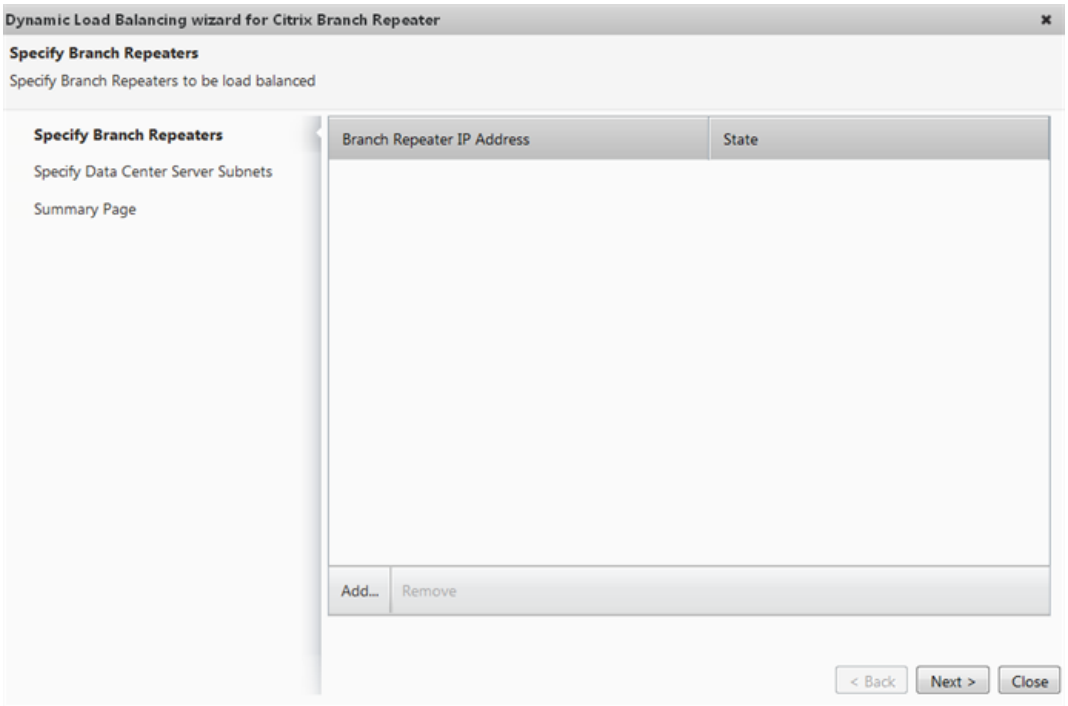
On the CloudBridge appliances in the datacenter and in the Amazon VPC, specify the Branch Repeater appliance as a service by using the Dynamic Load Balancing wizard for Citrix Branch Repeater. The wizard automatically creates a service and two virtual servers on the CloudBridge appliance.

To configure redirection of traffic to Branch Repeater appliances by using the CloudBridge configuration utility

1. In the left pane, click Load Balancing. Then, in the right pane, click Dynamic Load Balancing wizard for Citrix Branch Repeater.

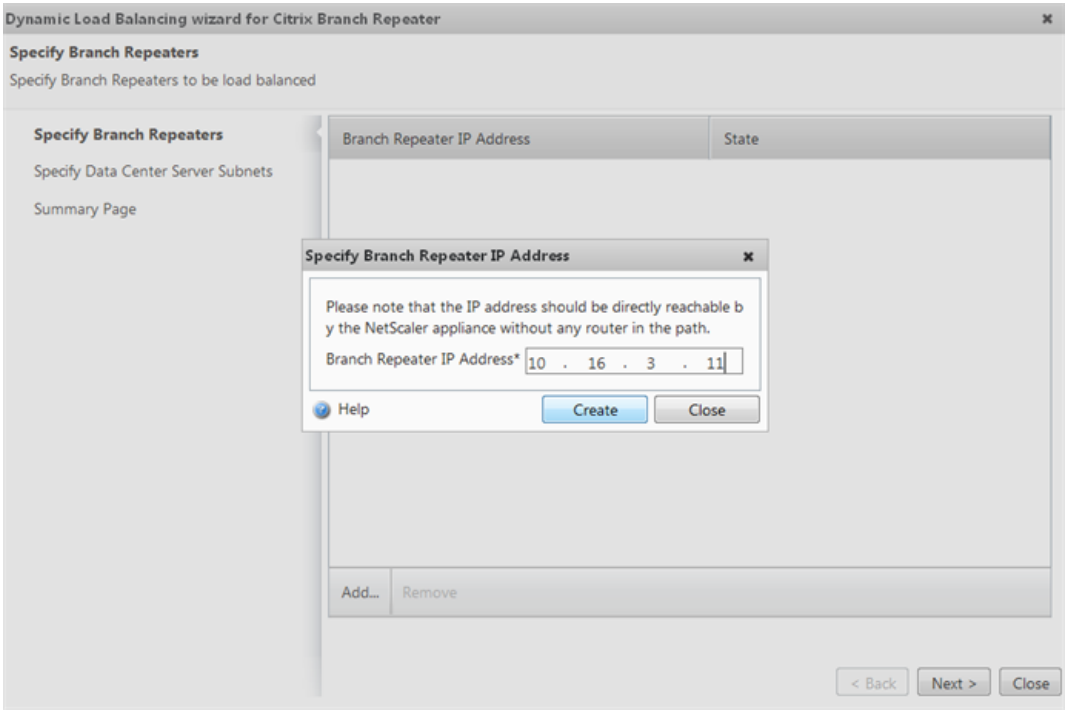


The Dynamic Load Balancing wizard for Citrix Branch Repeater appears.



2. In the wizard, on the Specify Branch Repeaters page, click Add.

3. In the Specify IP Address dialog box, enter the IP address of a Branch Repeater appliance, click Create, and then click Close.

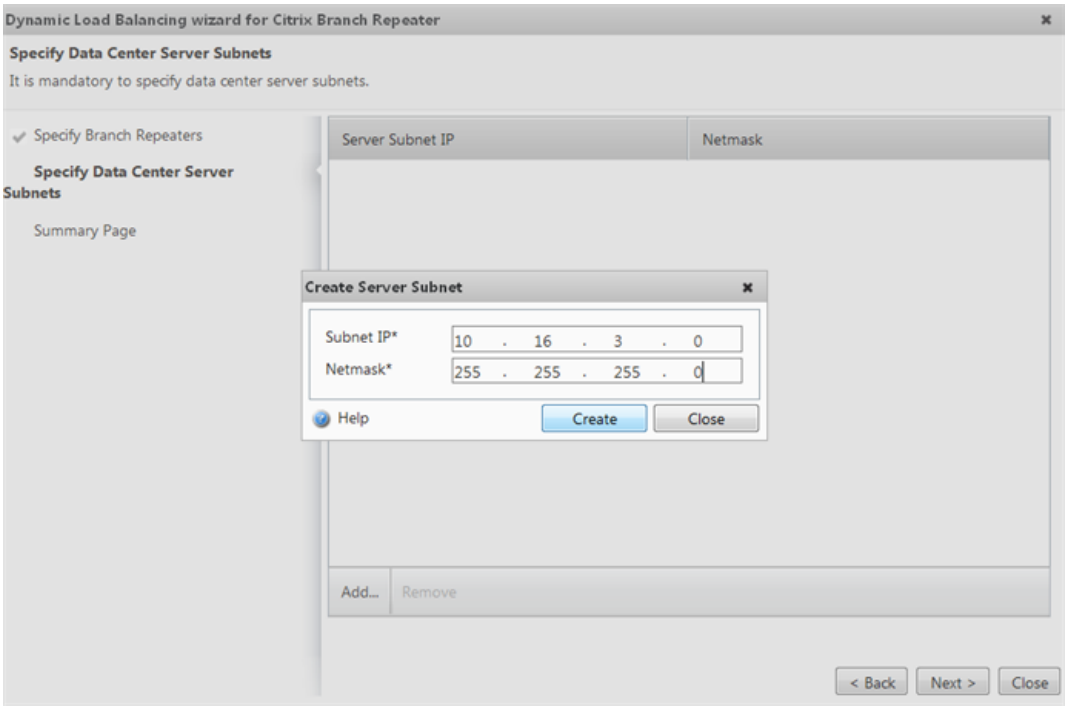


4. Click Next.

5. On the Specify Data Center Server Subnets page, click Add. In the Create Server Subnet dialog box, set the following parameters:

   - Subnet IP – The IP address of the subnet in which the servers reside.

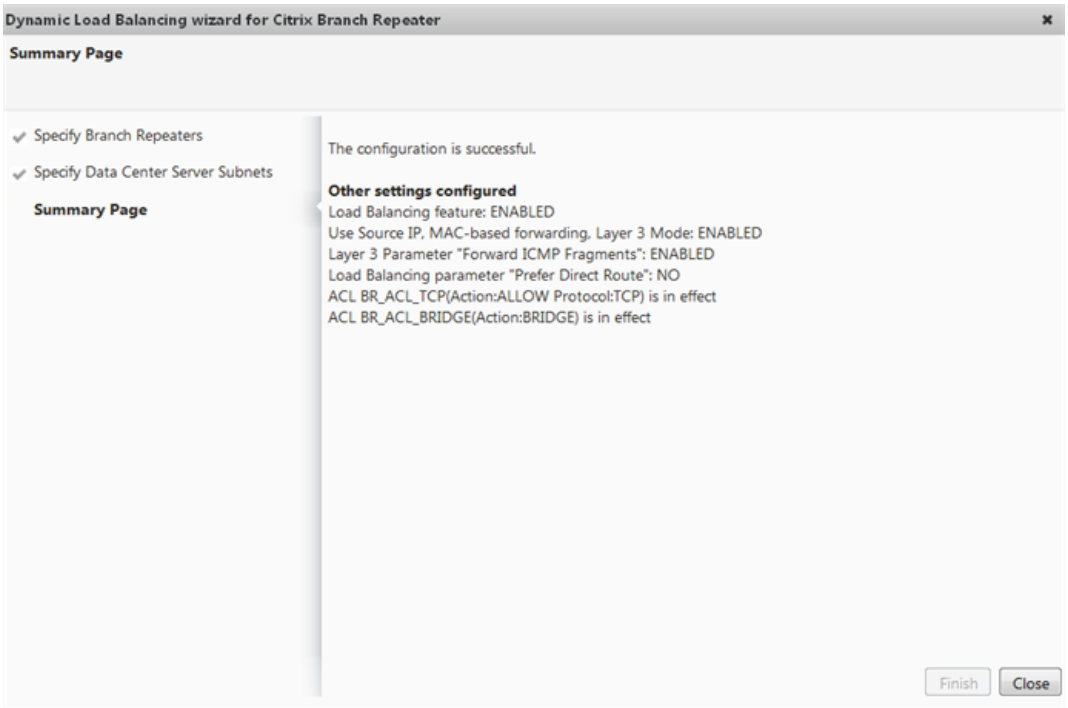
   - Mask – The subnet mask.



6. Repeat steps 5-6 until you have added all of the server subnets, and then click Close.

7. Click Next and click Finish.

8. The Summary page displays additional settings that are added automatically to complete the Branch Repeater load balancing configuration on the CloudBridge appliance.



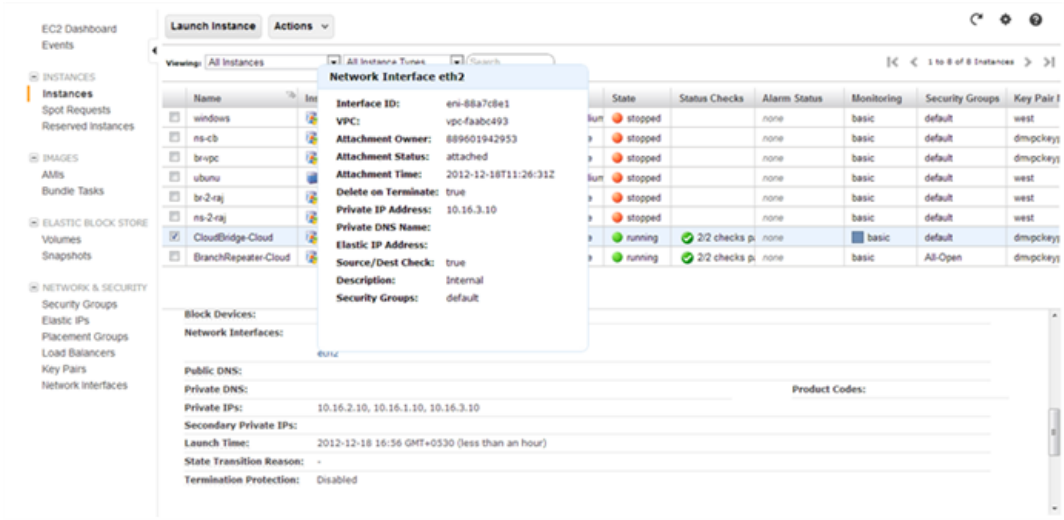
9. Click Close.

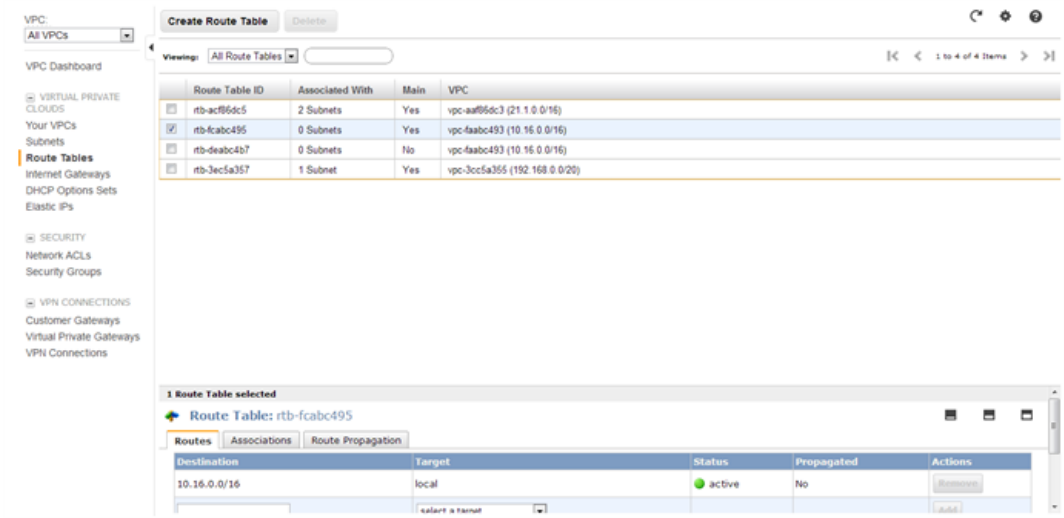
(Advanced Configuration) Accelerating Encrypted MAPI, Signed SMB, SSL Traffic and Branch Repeater Joining to Windows domain

To accelerate encrypted MAPI, signed SMB, and SSL traffic, you have to perform the following steps:

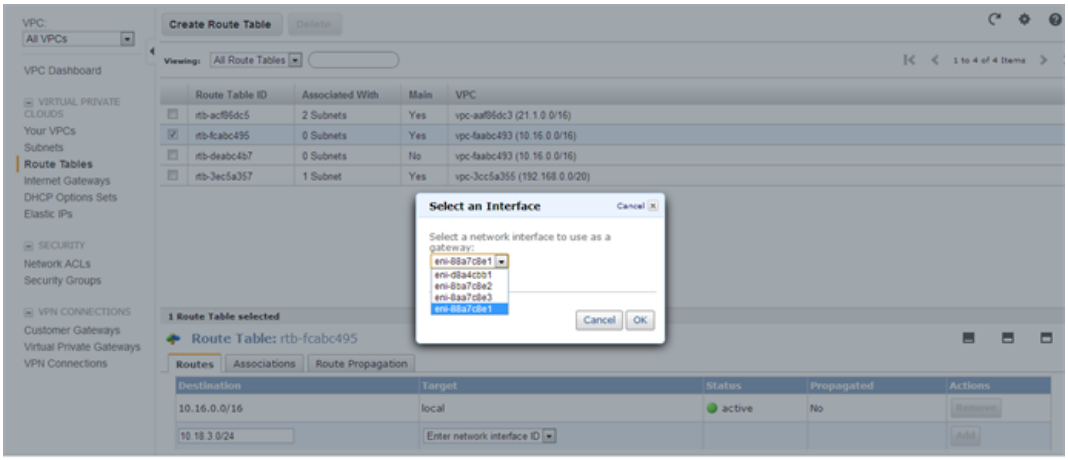
- Add a route to the server farm in the AWS VPC route table.
- Set listen policies for the virtual servers, which represent the Branch Repeater AMI, on the CloudBridge VPX on AWS.

To add a route to the server farm in the AWS VPC route table

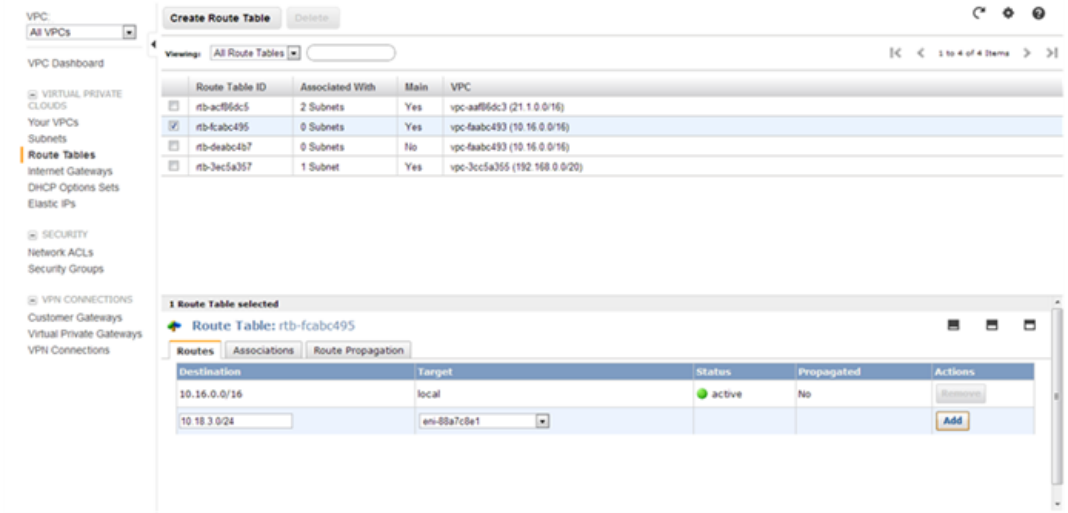
1. On the Amazon EC2 Console Dashboard page, in the navigation pane, click instances.
2. Select the CloudBridge VPX instance. The instance details are displayed in the EC2 Instances pane.
3. 

   In the EC2 Instances pane, select the CloudBridge VPX instance and then click edocs Interface (for example, eth2) that faces the Branch Repeater AMI on AWS, and note the Interface ID from the Network Interface pop-up window.
4. Click Services, and then click VPC.
5. 

   In the Navigation pane, click Route Tables to list all the VPC route tables. Select a VPC route table in the Route Tables pane to list the route table details in the Route Table Selected pane.
6. In the Route Table Selected pane, on the Routes tab, add a new row at the bottom of the table and, in the Destination column, type the subnet for the server farm.
7. From the select a target drop-down list, select Enter Network Interface Id.

8. 

   In the Select an Interface dialog box, select the network interface Id that you had noted earlier, and then click OK.

9. 

   Click Add to add the new route to the VPC route table.

Now, you need to set the following listen policies for the virtual servers BR_LB_VS_DYN_1 and BR_LB_VS_DYN_2.

Virtual servers	Parameters to be modified	Value to be set for the parameter
BR_LB_VS_DYN_1	Listen Policy	sys.vserver("BR_LB_VS_DYN_1").state.eq(up)&&client.tcp.repeater_option.exists&&client.ip.src.eq(<IP address of the Branch Repeater>).not For example, sys.vserver("BR_LB_VS_DYN_1").state.eq(up)&&client.tcp.repeater_option.exists&&client.ip.src.eq(10.16.3.11).not

BR_LB_VS_DYN_2	Listen Policy	sys.vserver("BR_LB_VS_DYN_2").state.eq(up)&&client.ip.src.eq(<IP address of the Branch Repeater appliance>).not For example, sys.vserver("BR_LB_VS_DYN_2").state.eq(up)&&client.ip.src.eq(10.16.3.11).not

To set listen policies for the virtual servers to which the Branch Repeater service is bound by using the CloudBridge command line

At the command prompt, type:

set lb vserver <name> -listenpolicy <expression>

Example

> set lb vserver BR_LB_VS_DYN_1 -listenpolicy sys.vserver("BR_LB_VS_DYN_1").state.eq(up)&&client.tcp.repe
Done

> set lb vserver BR_LB_VS_DYN_2 -listenpolicy sys.vserver("BR_LB_VS_DYN_2").state.eq(up)&&client.ip.src.e
Done

Note: On AWS, for pairing a Branch Repeater AMI with a CloudBridge VPX, you use the Dynamic Load Balancing wizard for Citrix Branch Repeater on the CloudBridge VPX. The wizard creates the following entities on the CloudBridge VPX:

Entity Name	Entity Type	Description
BR_LB_SVC_DYN_<IP address of the Branch Repeater appliance> For example, BR_LB_SVC_DYN _ 192.0.2.30	Service	A service representing the Branch Repeater appliance.
BR_LB_VS_DYN_1 and BR_LB_VS_DYN_2	Virtual server	Virtual servers to entertain different types of traffic for the Branch Repeater appliance. The service (for example, BR_LB_SVC_DYN_10.16.3.11) representing the Branch Repeater appliance is bound to both the virtual servers.

Parameter Descriptions (of commands listed in the CLI procedure)

set lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Troubleshooting Branch Repeaters in a CloudBridge tunnel Setup

The Branch Repeater Release Notes provides rough guidelines on the maximum number of connections and the optimized throughput for Branch Repeater in a CloudBridge tunnel deployment.

As Branch Repeater appliance approaches the limit, you may observe un-accelerated connections on the web console of the Branch Repeater on the client side. These connections bypass the Branch Repeater on the server side and do not show up on its web console.

On the server side, you need to perform the following steps on the CloudBridge appliance to which the Branch Repeater is paired. These settings should lead to reduced number of un-accelerated connections which in turn results in optimization of even more TCP traffic.

#	Steps	Entity Name	Parameters to be modified	Value to be set for the parameter
1	Modify the Retries and Failure Retries parameters of the default monitor named PING	PING	Retries	33
			Failure Retries	32
2	Bind the PING Monitor to the service (for example, BR_LB_SVC_DYN_192.0.2.30) representing the Branch Repeater appliance.	BR_LB_MONITOR_DYN BR_LB_SVC_DYN_<IP address of the Branch Repeater appliance> For example, BR_LB_MONITOR_DYN BR_LB_SVC_DYN_ 10.16.3.11	NA	NA
3	Unbind the monitor named BR_LB_MONITOR_DYN from the service (for example, BR_LB_SVC_DYN_10.16.3.11) representing the Branch Repeater appliance.	BR_LB_MONITOR_DYN BR_LB_SVC_DYN_<IP address of the Branch Repeater appliance> For example, BR_LB_MONITOR_DYN BR_LB_SVC_DYN_ 10.16.3.11	NA	NA

To set the Retries and Failure Retries parameters of the monitor PING by using the CloudBridge command line

At the command prompt, type:

set lb monitor <MonitorName> <MonitorType> -retries <integer> -failureRetries <integer>

Example

```
> set lb monitor PING ping -retries 33 -failureRetries 32
 Done
```

To bind the monitor PING to the Branch Repeater service by using the CloudBridge command line

At the command prompt, type:

bind service <name> -monitorName <string>

Example

```
> bind service BR_LB_SVC_DYN_10.16.3.11 -monitorName PING
 Done
```

To unbind the default Branch Repeater monitor from Branch Repeater service by using the CloudBridge command line

At the command prompt, type:

unbind service <name> -monitorName <string>

Example

```
> unbind service BR_LB_SVC_DYN_10.16.3.11 -monitorName BR_LB_MONITOR_DYN
 Done
```

Note: On AWS, for pairing a Branch Repeater AMI with a CloudBridge VPX, you use the Dynamic Load Balancing wizard for Citrix Branch Repeater on the CloudBridge VPX. The wizard creates the following entities on the CloudBridge VPX:

Entity Name	Entity Type	Description
BR_LB_SVC_DYN_<IP address of the Branch Repeater appliance> For example, BR_LB_SVC_DYN _ 192.0.2.30	Service	A service representing the Branch Repeater appliance.
BR_LB_MONITOR_DYN BR_LB_SVC_DYN_<IP address of the Branch Repeater appliance> For example, BR_LB_MONITOR_DYN BR_LB_SVC_DYN_ 192.0.2.30	Monitor	A monitor bound to the service (for example, BR_LB_SVC_DYN_10.16.3.11) representing the Branch Repeater appliance.

Parameter Descriptions (of commands listed in the CLI procedure)

set lb monitor

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind service

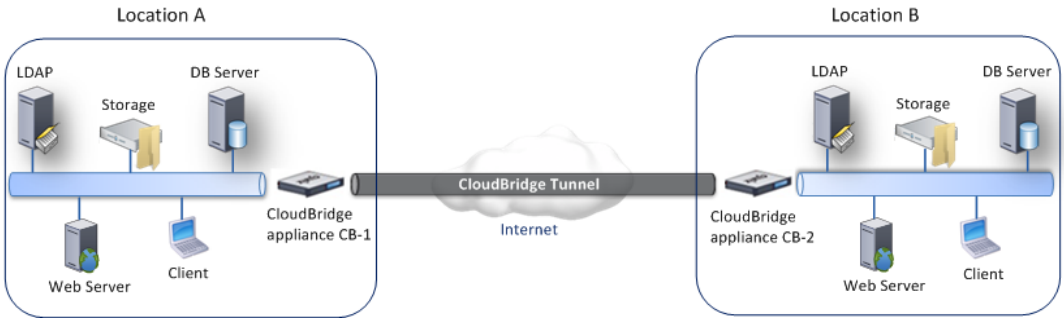
No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

unbind service

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

CloudBridge Tunnel Diagnostics and Troubleshooting

The following figure shows a CloudBridge tunnel between two CloudBridge appliances.



If you have problems with a CloudBridge tunnel configuration, make sure that all prerequisites were observed before the tunnel was set up. If they were, the problem might be with the tunnel end-point IP addresses, a NAT configuration, the way the tunnel was set up, or with the data traffic.

Prerequisites for Configuring a Cloudbridge Tunnel

Before you begin configuring a CloudBridge tunnel, make sure that you complete the following tasks:

- **Configure firewalls to allow UDP and ESP traffic** - Configure firewalls, deployed on the network edge of each of the CloudBridge tunnel end points, as follows:
  - If no NAT device is deployed before each of the CloudBridge tunnel end points, that is, the public IP addresses of both the tunnel end points are directly accessible to each other, you must configure the firewall to allow the following:
    - Any UDP packets for port 500
    - Any ESP (IP protocol number 50) packets
  - If a NAT device is deployed before any or each of the CloudBridge tunnel end points, that is, the public IP addresses of at least one tunnel end point is not directly accessible to the other, you must configure the firewall to allow the following:
    - Any UDP packets for port 500
    - Any UDP packets for port 4500
    - Any ESP (IP protocol number 50) packets
- **Test connectivity** - Before configuring the CloudBridge tunnel, make sure that the IP address of each CloudBridge tunnel end point is accessible from the other end point. If you have configured the firewalls to allow UDP packets for ports 500 and 4500, and ICMP traffic is allowed through the firewalls, you should be able to ping the IP address at one end point of the tunnel from the IP address at the other end point.

  On each of the tunnel end points, at the command line interface, type the following command:

  ping -**S** <LocalTunnelEndpoint-IP> <RemoteTunnelEndpoint-IP>

  If above ping is not successful, use any public IP address to verify Internet connectivity.

  ping -S <LocalTunnelEndPtIP> <PublicIP>

  If this ping is also unsuccessful, check your routing or Internet connectivity.

- **Enable the CloudBridge feature** - Make sure that the CloudBridge feature is enabled on NetScaler appliances, if they are used as tunnel end points, and that the license is active.

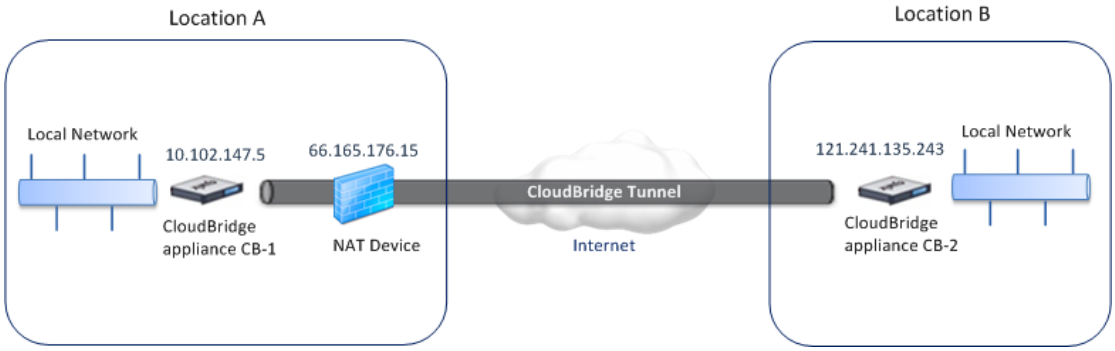
Points to Consider when Configuring a CloudBridge Tunnel with a NAT Device

For configuring a CloudBridge tunnel, consider the following points:

- You must not deploy any dynamic NAT device before a CloudBridge tunnel end point. At least one of the CloudBridge appliances must be directly connected or behind a static NAT device.
- Make sure that the IP tunnel entity configured on each CloudBridge appliance specifies the correct IP address of the appliance at the other end point. If one of the CloudBridge appliances is behind a static NAT device, the IP tunnel entity on the peer tunnel end point (the peer CloudBridge appliance) must specify the remote tunnel end-point IP as the IP address of the NAT device, not the IP address of the CloudBridge appliance that is behind the NAT device.

Examples

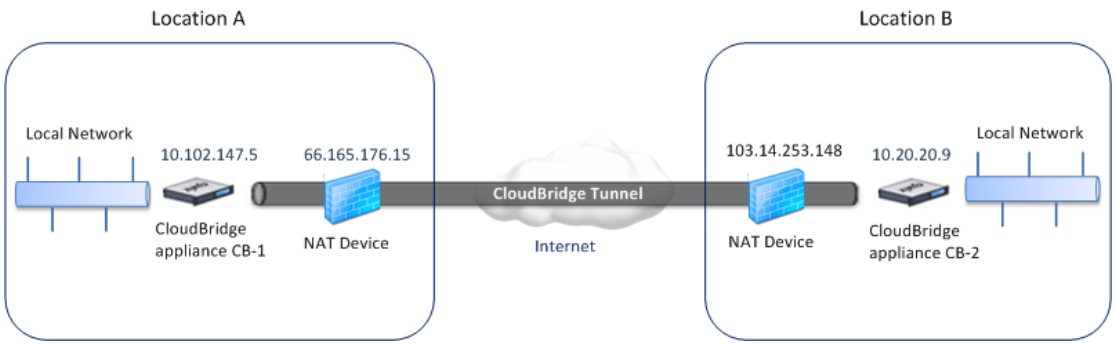
Consider the following deployment, where a NAT device is deployed in front of CloudBridge appliance CB-2:



The remote IP address and the local IP parameters of the IP tunnel entity configuration on CB-1 and CB-2 are as follows:

CloudBridge appliance	Remote IP	Local IP
CB-1	121.241.135.243	10.102.147.5
CB-2	66.165.176.15	121.241.135.243

Consider the following deployment, where a NAT device is deployed in front of both CloudBridge appliances CB-1 and CB-2:



The remote IP and the local IP parameters of the IP tunnel entity configuration on CB-1 and CB-2 are as follows:

CloudBridge appliance	Remote IP	Local IP
CB-1	103.14.253.148	10.102.147.5
CB-2	66.165.176.15	10.20.20.9

Troubleshooting a CloudBridge Tunnel

If your CloudBridge tunnel does not function properly, the issue could be with tunnel establishment or with the data traffic. If you are unsure which type of problem you have, look for an error message in the log file and see if the error message is in the list of tunnel-establishment issues. If you do not find your error message, check the list of possible issues related to data traffic.

Issues Related to Tunnel Establishment

After the requirements for configuring the IPSec tunnel are met and the CloudBridge tunnel is configured, if the status of the tunnel is not UP, look for debugging information in the iked.log file on one or both CloudBridge appliances configured as the tunnel end points.

On either appliance, type the following command at the CloudBridge shell prompt:

cat /tmp/iked.debug | tee /var/iked.log

The following table lists some common errors and their solutions.

Error Log Message	Possible Cause	Solution
retransmission count exceeded the limit **log message example** 2013-02-04 15:47:52 [PROTO_ERR]: ikev2.c:616:ikev2_timeout(): 3:5.5.5.2[500] - 5.5.5.1[500]:0x0:retransmission count exceeded the limit	The tunnel on the other end is not yet configured, or firewall routing issues are preventing the exchange of IKE related packets (UDP port 500/4500).	· If the tunnel on the other end point is not configured, configure it. · If the tunnel settings (IKE Version, Encryption/Hash Algorithm, PSK/certificates) on one end point do not match those on the other end point, no proposal is agreed upon between the end points. Specify the same settings on both end points. · After you configure a CloudBridge tunnel between two end points, if the IP tunnel entity in an end point does not enter the UP state within a few minutes, remove the IP tunnel entity and add it again. One minute is usually sufficient for tunnel establishment if both ends are Citrix CloudBridge appliances. · If none of the above measures correct the problem, configure, between the same end points, another CloudBridge that uses only the GRE protocol. Configure the firewalls on both ends to allow GRE (protocol number 47) packets. Verify that you are able to ping the network at one end of CloudBridge tunnel from the other end.

authentication failure **Log message example** *2013-02-04 16:05:16 [PROTO_ERR]: ikev2_auth.c:615:ikev2_verify(): 8:5.5.5.2[500] - 5.5.5.1[500]:0x8104290:authentication failure*	The IPSec authentication parameters (PSK or the public and private key) are set to incorrect values.	· Configure the authentication parameters correctly on both CloudBridge appliances.
failed to find a socket for retransmission or couldn't find configuration **Log message example** 2013-02-04 15:47:44 [INTERNAL_ERR]: isakmp.c:1844:isakmp_retransmit(): failed to find a socket for retransmission 2013-01-10 21:21:46 [PROTO_ERR]: ikev1.c:950:isakmp_ph1begin_r(): couldn't find configuration .	The tunnel IP address is not yet available for IKE purposes, or the tunnel does not exist.	· Remove the IP tunnel entities on both tunnel end points and add them again. · If another IP tunnel entity exists, with Local IP set to the same IP address but with IPSec profile set to NONE, remove these two tunnel entities and add them again. First add the one with a valid IPSec profile, and then add the one with IPSec profile NONE. · Verify that the IP address is available for IKE purposes, by typing the following commands at the CloudBridge shell prompt: · **ifconfig** -**a** | **grep**<LocalTunnelEndPoint-IP> **Example** root@ns# ifconfig -a | grep 5.5.5.2 *inet 5.5.5.2 netmask 0xffffff00 broadcast 5.5.5.255* · **netstat | grepudp | grep** <LocalTunnelEndPoint-IP> **Example** root@ns# netstat | grepudp | grep 5.5.5.2 *udp4 0 0 5.5.5.2.sae-urn *.* udp4 0 0 5.5.5.2.isakmp *.**

The source port and destination ports shown in the /tmp/iked.debug are other than port 500. That is: src=<srcip>[<srcPort != 500>] dst=<dst tip>[<dstPort != 500>]) **Log message example** 2013-02-04 16:08:59 [INFO]: ike_pfkey.c:490:sadb_log_add(): SADB_UPDATE ul_proto=255 src=5.5.5.1[4500] dst=5.5.5.2[4500] satype=ESP samode=transport spi=0x055fdd6d authtype=HMAC-SHA-256 enctype=AES-CBC lifetime soft time=25741 bytes=0 hard time=28800 bytes=0	At least one of the CloudBridge end points is deployed behind a NAT device	· See Points to Consider when Configuring a CloudBridge Tunnel with a NAT Device for proper IP configuration for configuring a CloudBridge tunnel. · Make sure that UDP traffic is unblocked and the IPSec tunnel configuration is correct on both CloudBridge instances, as described in Prerequisites and Points to Consider when Configuring a CloudBridge Tunnel with a NAT Device.

Issues Related to Data Traffic

If the data in the CloudBridge tunnel are not exchanged properly between the tunnel end points, do the following.

- For a CloudBridge tunnel that uses GRE and IPSec protocols:
  - Make sure that L2 mode is enabled on both of the CloudBridge tunnel end points. To enable L2 mode, type the following command at the CloudBridge command prompt.

    enable mode L2

  - If one of the CloudBridge tunnel end points is a CloudBridge virtual appliance (VPX) and is provisioned on a VMware ESXi hypervisor, make sure that **Promiscuous mode** is set to **Accept** for the vSwitch associated with the CloudBridge VPX appliance.

  - If a VLAN is extended through a CloudBridge tunnel, verify one-to-one mapping on the extended VLAN entity on each of the tunnel end points .

  - Make sure that the IP tunnel entity is bound to the correct netbridge entity in each of the tunnel end points.

  - Verify that the ARP entry for the peer CloudBridge tunnel end point exists on the local tunnel end point, by typing the following command at the CloudBridge command prompt.

    show arp

    If the output shows an incomplete ARP entry, bidirectional traffic is not flowing through the tunnel. If bidirectional traffic is flowing, the ARP entry shows the name of tunnel interface for the devices on the other side of the tunnel.

  - Remove the IP tunnel entities from both tunnel end points and add them again with the same parameters, but with the IPSec profile set to NONE, so that the tunnel uses only the GRE protocol.

    After verifying the following in the IP tunnel (that uses GRE protocol), configure the tunnel with IPSec parameters by specifying a valid IPSec profile to the respective IP tunnel entities on each of the tunnel end points.

    - Proper PING or TCP flow through the tunnel

    - Proper flow of data traffic through the tunnel

    After the configured tunnel (that uses GRE and IPSec protocols) is in UP state, if the data traffic does not flow properly through the tunnel, and if a NAT device was deployed in front of any or both of the tunnel end points, analyze the ingress and egress packets on the NAT devices
- If a CloudBridge appliance is used as Router or Gateway.
  - Make sure that L3 mode is enabled on the CloudBridge appliance. To enable L3 mode, run the following command in the CloudBridge command line.

enable mode L3

- If subnets are bound to a netbridge entity, make sure that correct IP tunnel entity is also bound to the netbridge.

- Run the following command in the CloudBridge command line to see where the packets (Input and Output)are getting dropped:

  stat ipsec counters

- Make sure that the correct routes are configured on both the tunnel end points.

- If no NAT device is deployed in front of the CloudBridge appliance, make sure that the firewalls are configured to allow any ESP (IP protocol number 50) packets and any UDP packets for port 4500.

If none of the above measures result in successful exchange of traffic between the tunnel end points, contact Citrix Technical Support.

Checklist before Contacting Citrix Technical Support

For a speedy resolution, make sure that you have the following items ready before contacting Citrix Technical Support.

- ·Details of the deployment and network topology.
- Log file collected by typing the following command at the CloudBridge shell prompt.

  cat /tmp/iked.debug | tee /var/log/iked.log
- Tech support bundle captured by typing the following command at the CloudBridge command prompt.

  show techsupport
- Packet traces captured on both CloudBridge tunnel end points. To start a packet trace, type the following command at the CloudBridge command prompt.

  start nstrace-size 0

  To stop packet trace, type the following command at the CloudBridge command prompt.

  stop nstrace
- Output of the following command typed at the CloudBridge command prompt.

  show arp

Known Issues

IKE re-keying, which is renegotiation of new cryptographic keys between the CloudBridge tunnel end points to establish new SAs, is not supported. When the Security Associations (SAs) expire, the tunnel goes into the DOWN state. Therefore, you must set a very large value for the lifetimes of SAs.

EdgeSight Monitoring for NetScaler

Citrix EdgeSight for NetScaler is an application to monitor end-user experience with Web applications served in a NetScaler environment. The EdgeSight Monitoring application uses the HTML Injection feature of the NetScaler to provide data with which you can compare the performance of various Web applications across geographical locations.

For EdgeSight monitoring, register the NetScaler appliance with EdgeSight and enable applications in the NetScaler. The EdgeSight application processes the data and displays the information after aggregating it. You can view the data as charts, graphs, or tables.

When EdgeSight monitoring is enabled on a virtual server, NetScaler injects scripts into the responses sent to the clients. Execution or insertion of these scripts does not affect the response to the client. Data injected by the NetScaler is collected by the EdgeSight server through data collector services.

EdgeSight is an agentless application. The EdgeSight server from which you can monitor the user-experience is referred to as *EdgeSight UI server*.

Use the wizard to register the NetScaler appliance with the EdgeSight UI server, select the data collector services, and configure the rate at which data is injected into the response. For more information on the wizard, see "Configuring EdgeSight Monitoring."

Note: The EdgeSight UI server has a data collector and a Web site. For better scalability, you can install multiple data collectors.

To use EdgeSight monitoring, enable EdgeSight monitoring on the load balancing or content switching virtual servers associated with the selected applications. For instructions, see "Enabling an Application for EdgeSight Monitoring. "

Configuring EdgeSight Monitoring for NetScaler

The configuration utility provides a wizard to assist you with configuration. The wizard for the configuration of EdgeSight monitoring for NetScaler guides you through the configuration procedure in simple steps. The wizard takes care of the following tasks:

- Enable the EdgeSight Monitoring (HTML Injection) feature.
- Specify the rate and frequency for injecting data.
- Bind the EdgeSight server/data collector services to the load balancing virtual server on the NetScaler.
- Enable the Web applications for EdgeSight monitoring.

Note: You can configure rate or frequency. If you specify the rate to be x, data is injected once after every x responses sent by the service. For example, if you specify the rate to be 500, NetScaler injects the data into the 1st response, 501st response, 1002nd response, and so on. If you specify frequency to be y, data is injected once in every y milliseconds.

To access the wizard from the NetScaler configuration utility and configure EdgeSight Monitoring

1. In the navigation pane, click EdgeSight Monitoring.
2. Click EdgeSight for NetScaler Wizard.
3. Follow the instructions presented by the wizard.

To configure EdgeSight monitoring from the command line interface and configure EdgeSight Monitoring

The following example shows the CLI commands executed for configuring EdgeSight monitoring for a NetScaler appliance.

Example

When the EdgeSight for NetScaler overview page link is clicked

Jun 9 22:46:21 <local0.info> 10.102.113.114 06/10/2011:02:46:21 GMT ns PPE-2 : UI CMD_EXECUTED 247 : User nsroot - Remote_ip 10.101.254.143 - Command "show filter action" - Status "Success"

Jun 9 22:46:33 <local0.info> 10.102.113.114 06/10/2011:02:46:33 GMT ns PPE-2 : UI CMD_EXECUTED 248 : User nsroot - Remote_ip 10.101.254.143 - Command "show filter postbodyInjection" - Status "Success"

Jun 9 22:46:33 <local0.info> 10.102.113.114 06/10/2011:02:46:33 GMT ns PPE-2 : UI CMD_EXECUTED 249 : User nsroot - Remote_ip 10.101.254.143 - Command "show filter htmlinjectionparameter" - Status "Success"

Jun 9 22:46:33 <local0.info> 10.102.113.114 06/10/2011:02:46:33 GMT ns PPE-2 : UI CMD_EXECUTED 250 : User nsroot - Remote_ip 10.101.254.143 - Command "show filter htmlinjectionvariable EDGESIGHT_SERVER_IP" - Status "Success"

Jun 9 22:46:33 <local0.info> 10.102.113.114 06/10/2011:02:46:33 GMT ns PPE-2 : UI CMD_EXECUTED 251 : User nsroot - Remote_ip 10.101.254.143 - Command "show lb vserver __ESNS_LBVSERVER" - Status "Success"

Jun 9 22:46:34 <local0.info> 10.102.113.114 06/10/2011:02:46:34 GMT ns PPE-2 : UI CMD_EXECUTED 252 : User nsroot - Remote_ip 10.101.254.143 - Command "show lb vserver __ESNS_LBVSERVER" - Status "Success"

Jun 9 22:46:34 <local0.info> 10.102.113.114 06/10/2011:02:46:34 GMT ns PPE-2 : UI CMD_EXECUTED 253 : User nsroot - Remote_ip 10.101.254.143 - Command "show service" - Status "Success"

When the Register Appliance link is clicked

Jun 9 22:47:52 <local0.info> 10.102.113.114 06/10/2011:02:47:52 GMT ns PPE-2 : UI CMD_EXECUTED 254 : User nsroot - Remote_ip 10.101.254.143 - Command "show ns hostName" - Status "Success"

On completion of the wizard

Jun 9 22:50:01 <local0.info> 10.102.113.114 06/10/2011:02:50:01 GMT ns PPE-2 : UI CMD_EXECUTED 255 : User nsroot - Remote_ip 10.101.254.143 - Command "set filter htmlinjectionvariable EDGESIGHT_SERVER_IP -value 10.102.31.147" - Status "Success"

Jun 9 22:50:01 <local0.info> 10.102.113.114 06/10/2011:02:50:01 GMT ns PPE-2 : UI CMD_EXECUTED 256 : User nsroot - Remote_ip 10.101.254.143 - Command "set lb vserver __ESNS_LBVSERVER -IPAddress 0.0.0.0 -IPPattern 0.0.0.0 -IPMask * -weight 1 essvc -persistenceType NONE -timeout 2 -persistenceBackup NONE -backupPersistenceTimeout 2 -lbMethod LEASTCONNECTION -persistMask 255.255.255.255 -v6persistmasklen 128 -pq OFF -sc OFF -rtspNat OFF -m IP -dataOffset 0 -sessionless DISABLED -connfailover DISABLED -cltTimeout 180 -soMethod NONE -soPersistence DISABLED -soPersistenceTimeOut 2 -redirectPortRewrite DISABLED -downStateFlush DISABLED -gt2GB DISABLED -insertVs" - Status "Success"

Jun 9 22:50:02 <local0.info> 10.102.113.114 06/10/2011:02:50:02 GMT ns PPE-2 : UI CMD_EXECUTED 257 : User nsroot - Remote_ip 10.101.254.143 - Command "set filter prebodyInjection "/netscaler/htmlinjection/ens/prebody.js"" - Status "Success"

Jun 9 22:50:02 <local0.info> 10.102.113.114 06/10/2011:02:50:02 GMT ns PPE-2 : UI CMD_EXECUTED 258 : User nsroot - Remote_ip 10.101.254.143 - Command "set filter

postbodyInjection "/netscaler/htmlinjection/ens/postbody.js"" - Status "Success"

Enabling an Application for EdgeSight Monitoring

EdgeSight monitoring makes it possible to monitor the performance of an application from the end user's perspective.

Note: To enable an application to be monitored, EdgeSight monitoring must be enabled on the virtual servers.

EdgeSight monitoring is possible only if the response from the physical server is not compressed. Therefore, make sure that Compression is enabled globally on the NetScaler. When you use the wizard to configure EdgeSight monitoring, the wizard takes care of enabling compression and other necessary processing.

Note: Before enabling EdgeSight monitoring on a virtual server, make sure that you completed the configuration of EdgeSight monitoring through the wizard.

To enable EdgeSight monitoring on a load balancing or content switching virtual server by using the NetScaler configuration utility

1. In the navigation pane, expand Load Balancing and click Virtual Servers.
2. Select the virtual server, or multiple virtual servers, and then click Enable EdgeSight Monitoring.
3. If you want the NetScaler to compress responses after receiving them from the server, select the Compress response at NetScaler before sending it to the client check box.
4. Select the Export EdgeSight statistics to AppFlow check box.
5. From the Appflow Action drop-down list, select the AppFlow action.

   The AppFlow action defines the list of AppFlow collectors to which it exports EdgeSight Monitoring statistics. If you have selected multiple load balancing virtual servers, the same AppFlow action will be configured in the responder policies bound to them.

   Note: You can later change the AppFlow action configured for each of the selected Load Balancing virtual server individually, if required.
6. Click OK.

To enable EdgeSight monitoring on a load balancing or content switching virtual server by using the command line interface

The following example shows the CLI commands executed for enabling EdgeSight monitoring on a virtual server.

Example

Jun 9 22:56:13 <local0.info> 10.102.113.114 06/10/2011:02:56:13 GMT ns PPE-2 : UI CMD_EXECUTED 266 : User nsroot - Remote_ip 10.101.254.143 - Command "show lb vserver guilb" - Status "Success"

Jun 9 22:56:13 <local0.info> 10.102.113.114 06/10/2011:02:56:13 GMT ns PPE-2 : UI CMD_EXECUTED 267 : User nsroot - Remote_ip 10.101.254.143 - Command "show lb vserver guilb" - Status "Success"

Jun 9 22:56:14 <local0.info> 10.102.113.114 06/10/2011:02:56:14 GMT ns PPE-2 : UI CMD_EXECUTED 268 : User nsroot - Remote_ip 10.101.254.143 - Command "show lb vserver guilb" - Status "Success"

Jun 9 22:56:14 <local0.info> 10.102.113.114 06/10/2011:02:56:14 GMT ns PPE-2 : UI CMD_EXECUTED 269 : User nsroot - Remote_ip 10.101.254.143 - Command "show lb vserver guilb" - Status "Success"

Jun 9 22:56:14 <local0.info> 10.102.113.114 06/10/2011:02:56:14 GMT ns PPE-2 : UI CMD_EXECUTED 270 : User nsroot - Remote_ip 10.101.254.143 - Command "bind lb vserver guilb -weight 1 -policyName __ESNS_PREBODY_POLICY" - Status "Success"

Jun 9 22:56:15 <local0.info> 10.102.113.114 06/10/2011:02:56:15 GMT ns PPE-2 : UI CMD_EXECUTED 271 : User nsroot - Remote_ip 10.101.254.143 - Command "bind lb vserver guilb -weight 1 -policyName __ESNS_POSTBODY_POLICY" - Status "Success"

Jun 9 22:56:15 <local0.info> 10.102.113.114 06/10/2011:02:56:15 GMT ns PPE-2 : UI CMD_EXECUTED 272 : User nsroot - Remote_ip 10.101.254.143 - Command "bind lb vserver guilb -weight 1 -policyName __ESNS_RESPONDER_POLICY -priority 2147483647 -gotoPriorityExpression END" - Status "Success"

Jun 9 22:56:15 <local0.info> 10.102.113.114 06/10/2011:02:56:15 GMT ns PPE-2 : UI CMD_EXECUTED 273 : User nsroot - Remote_ip 10.101.254.143 - Command "bind lb vserver guilb -weight 1 -policyName __ESNS_REWRITE_POLICY -priority 2147483647 -gotoPriorityExpression END -type REQUEST" - Status "Success"

Jun 9 22:56:15 <local0.info> 10.102.113.114 06/10/2011:02:56:15 GMT ns PPE-2 : UI CMD_EXECUTED 274 : User nsroot - Remote_ip 10.101.254.143 - Command "show ns feature" - Status "Success"

Accessing the EdgeSight Monitoring Interface from NetScaler

You can view the data presented by the EdgeSight monitoring application from the NetScaler appliance. The configuration utility of the NetScaler displays a login screen to access the EdgeSight UI server and upon successful login, displays the data.

To access EdgeSight for NetScaler by using the NetScaler configuration utility

1. In the navigation pane, click EdgeSight Monitoring.
2. Click Access EdgeSight for NetScaler.
3. Enter the credentials for accessing the EdgeSight UI server. For more information on viewing the reports, see *EdgeSight Administration Guide* at "http://support.citrix.com/article/CTX126418"

Variables Injected for EdgeSight Monitoring for NetScaler

For monitoring the end-user experience in the NetScaler environment, NetScaler injects scripts into the responses sent to the clients. A predefined set of variables are used in the scripts and the variables are evaluated at runtime. The following table describes the variables.

Table 1. Variables for Monitoring the NetScaler Performance

Name	Type	JavaScript type	Comment
SYS.IID	128-bit GUID structure	Windows format GUID	This is a GUID that uniquely identifies each NetScaler. The value of this variable remains constant across reboots. It is valid in both prebody and postbody.
HTTP.XID	128-bit GUID structure	Windows format GUID	This is a GUID that uniquely identifies each HTTP transaction (request/response). This variable is guaranteed to be unique even if the NetScaler is rebooted. It is valid in both the prebody and postbody.
SYS.UPTIME	32-bit integer	10-digit number	Gives the time in seconds, offset to UTC, that the NetScaler has been up. It is valid in both prebody and postbody.
HTTP.REQ.RECEIVE_TIME_BEG	64-bit integer	20-digit number	Gives the time, in microseconds, when NetScaler received the first byte of a client request. It is valid in both prebody and postbody.

HTTP.REQ.RECEIVE_TIME_END	64-bit integer	20-digit number	Gives the time, in microseconds, when NetScaler received the last byte of a client request. It is valid in both the prebody and postbody.
HTTP.REQ.SEND_TIME_BEG	64-bit integer	20-digit number	Gives the time, in microseconds, when NetScaler forwarded the first byte of a request to the back-end server. It is valid in both prebody and postbody.
HTTP.REQ.SEND_TIME_END	64-bit integer	20-digit number	Gives the time, in microseconds, when NetScaler forwarded the last byte of a request to the back-end server. It is valid in both prebody and postbody.
HTTP.RES.RECEIVE_TIME_BEG	64-bit integer	20-digit number	Gives the time, in microseconds, when NetScaler received the first byte of a response from the back-end server. It is valid in both prebody and postbody.
HTTP.RES.RECEIVE_TIME_END	64-bit integer	20-digit number	Gives the time, in microseconds, when NetScaler received the last byte of a response from the back-end server. It is valid only in postbody.
HTTP.RES.SEND_TIME_BEG	64-bit integer	20-digit number	Gives the time, in microseconds, when NetScaler forwarded the first byte of response to the client. It is valid in both prebody and postbody.

HTTP.RES.SEND_TIME_END	64-bit integer	20-digit number	Gives the time, in microseconds, when NetScaler forwarded the last byte of a response to the client. It is valid only in postbody.
SYS.VSERVER	String (147 characters)	20-digit number	Gives the name, IP address, and port number of the virtual server that load balanced the request. It is valid in both prebody and postbody.
SYS.VSERVICE	String (147 characters)	20-digit number	Gives the name, IP address, and port number of the physical server that serviced the request. It is valid in both prebody and postbody.

Flex Tenancy

Flex Tenancy™ is a Citrix NetScaler methodology that allows you to tune a group of NetScaler VPX instances to the unique characteristics and needs of individual applications in a complex Web 2.0 setup.

As the Web becomes the de-facto way of delivering application services, the number of web applications that enterprises and service providers must support has been growing at a very fast pace. Not only are the technical requirements of each web application different, but also in most large environments, the applications are owned and controlled by different constituencies/organizations. This leads to the need to offer the Application Delivery Controller (ADC) functionality as a shared service to multiple tenants.

Understanding the Flex Tenancy Architecture

In a typical Flex Tenancy set-up, NetScaler physical and virtual appliances can be used together in a two-tier architecture with each tier dedicated to managing specific actions. This:

- provides flexibility for how application delivery services are deployed and managed
- makes it much easier to shuffle applications and their associated application delivery resources on-demand without risking the stability of the entire network
- reduces costs

The Flex Tenancy architecture segments web application delivery services into two tiers:

- shared-network-service flex tier
- application-specific tenant tier

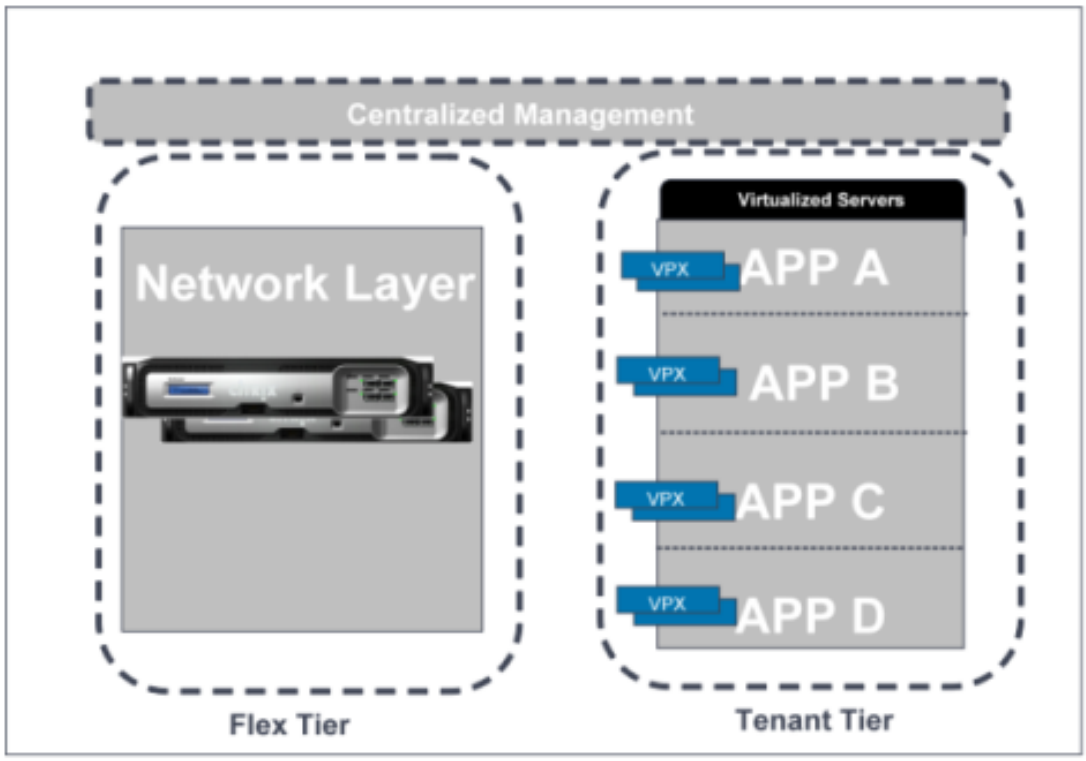


Figure 1. Flex Tenancy Architecture

The Flex Tier

The flex tier runs at the edge of the data center or an enterprise network. The flex tier generally performs application delivery services and associated policies that are common and applied to all applications. Examples of such services could include:

- SSL offload
- SSL VPN
- DoS mitigation
- GSLB
- Certain types of redirects
- Content Switching

Since the policies are common and shared, there is no reason to try and partition them across multiple NetScaler instances dedicated per specific application. Indeed, partitioning at the flex tier is counterproductive as it leads to duplication of effort and the associated possibility of configuration errors during change management. Therefore, the flex tier should be physically centralized on as few NetScaler instances as possible. In all but the smallest environments this will generally lead to NetScaler MPX physical appliances being used at the flex tier.

The Tenant Tier

The tenant tier runs logically close to the applications, with each tenant (whether a tenant is an application, a line of business, or a customer) getting its own NetScaler instance. The tenant tier isolates the application delivery needs that vary by application - like server load balancing, caching, compression and application firewall protection - per application.

Since the policies - and thus the NetScaler configurations - differ by application, there is no inherent configuration benefit to centralizing multiple applications onto a single NetScaler. In fact, there are significant configuration isolation, separation of duties and capacity planning benefits of dedicating appliances on an app-by-app basis.

Centralized Management

One potential downside to dedicating NetScaler instances to specific applications is "appliance sprawl". In Flex Tenancy architectures, the vast majority of most instances will be NetScaler VPX virtual appliances. Therefore, the physical challenges (e.g., racking, cabling) associated with appliance sprawl don't exist. Citrix Command Center is used to provide centralized FCAPS (fault, configuration, accounting, performance, security) management of both the flex and the tenant tiers.

Building a Flex Tenancy Solution

The Flex Tenancy architecture is applicable to any high volume environment where:

- multiple tenants share a common infrastructure
- there is a core set of shared application delivery services that are common to all tenants
- each tenant also has its own specific web application delivery needs and requirements

The two most prevalent examples of this kind of environment are:

- hosting/managed services providers that want to offer dedicated load balancing/application delivery services to their customers
- an enterprise IT organization that models itself as an “internal service provider” to support multiple lines-of-business and business applications.

In each case, the core architecture is similar. However, the deployment architecture and the management of the overall system will likely vary based upon the very different business needs of each case.

Enterprise IT as an Internal Service Provider

Many enterprise IT organizations model themselves as internal service providers supporting the different needs of the different lines-of-business. Building "private clouds" to support enterprise applications is the latest phase of this trend.

An enterprise typically hosts a variety of applications that may be independent of each other.

These applications:

- require their own application server pools
- typically need customized ADC policies and tuning
- have their own distinct change management requirements and windows

The challenge facing the groups managing the web application delivery infrastructure is to support different and increasingly complex applications and at the same time scale so that they can support an ever increasing number of applications.

Achieving application performance in this environment depends upon coordination between network teams and the various application teams. Application tuning requires knowledge of the application and in many cases should be responsibility of the application team. Maintaining network performance and availability requires knowledge of various networking protocols and hardware management and therefore becomes the responsibility of the network team.

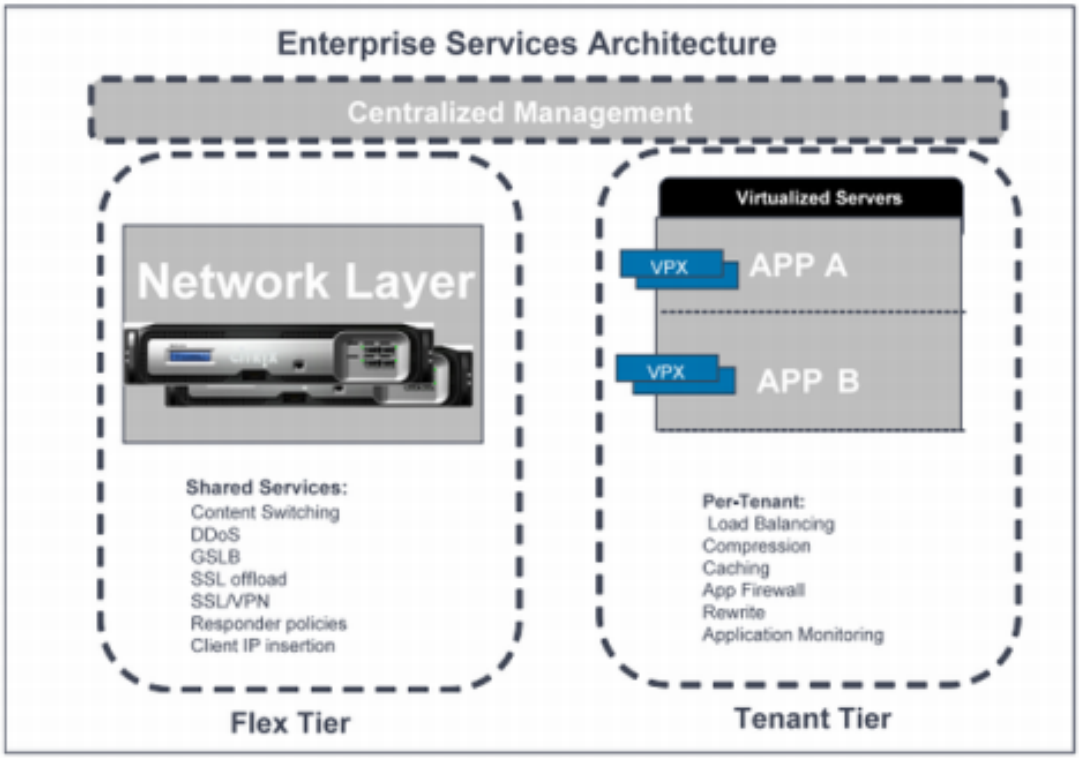
Sharing the same device between both teams creates manageability challenges for an organization. For example, consider an application administrator wanting to upgrade to upgrade the ADC take advantage of new functionality. If the ADC is shared by other applications, the administrator must coordinate with all these teams to initiate change control for his change.

Moreover, any changes to the ADC will need to be tested with every other application. As the number of applications grows, this model becomes exponentially complex.

The Flex Tenancy architecture addresses these issues. Since no other applications run on the tenant instance:

- it can be upgraded based solely on the needs of its hosted app
- there is no need to qualify the version upgrade against other applications
- there is no concern that using the new functionality will impact other app performance

Figure 1. Architecture of an enterprise service solution



There are three possible administrative approaches using Flex Tenancy:

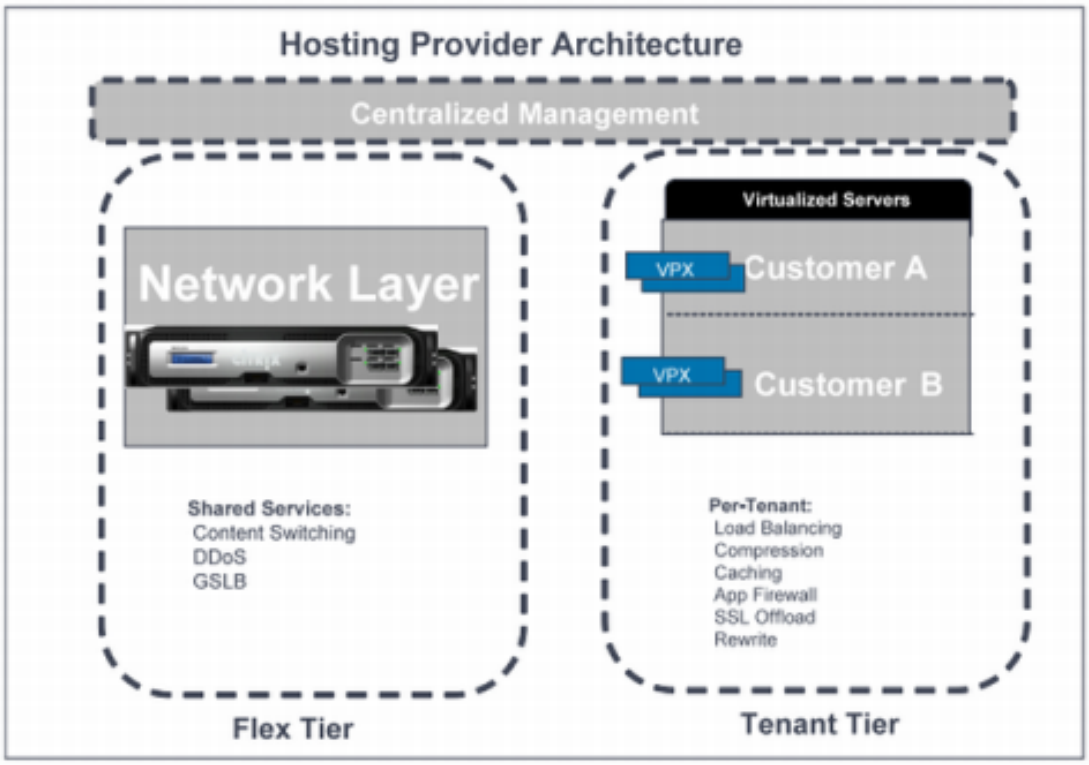
1. The central IT organization can retain full administrative control over both the flex and tenant tiers.

2. The central IT organization can retain full control over the flex tier, but delegate management rights of the tenant instances to individual app teams.

3. The central IT team can retain full control over the flex tier, retain control over certain elements of the tenant tier (e.g., certain IP addressing, ensuring it can retain “root access”) but delegate control of other functionality to app teams.

The ability to tune the application delivery fabric to individual applications enables IT organizations to maximize the performance of their applications and to scale the number of applications they provide to their stakeholders without significant increase in costs.

Hosting provider solution



A hosting provider provides space on a server they own and Internet connectivity for the applications hosted on that server. These servers are typically hosted in a data center. Load balancing is a frequently requested "add-on" services customers ask for. Additionally, advanced L7 services such as compression, application firewall and caching provide additional revenue opportunities for the hosting provider.Figure 1. Architecture of a hosting provider solution

The biggest challenge in this environment is managing and delivering application delivery services for a wide variety of customers, each with varying requirements. Trying to manage these services on a shared device can lead to performance bottlenecks, change management conflicts and ultimately a loss of business. Also, many customers will want admin rights to control the load balancing services used for their hosted back-end servers.

Flex Tenancy solution can be very useful in this scenario. A hosting provider can use the flex tier to run services common to the entire data center. These include global server load balancing (GSLB) which would provide data center redundancy, denial of service protection (DoS), and segregate traffic to the tenant tier using content switching policies.

At the tenant tier each tenant is provisioned, and can manage its own, dedicated NetScaler instances.

One of the primary services of this tier is to load balance requests to the backend servers. In addition, this tier may also perform SSL offload. This is usually a flex tier service, but in a hosting environment it may be offloaded to the tenant tier if the hosting business model

supports customers owning and managing their own certificates.

Tenant tier is also used to apply a variety of complex application policies to tune application performance. For example, a customer can define caching policies to cache objects of a certain application only for ten seconds while other application objects could be cached for a longer duration. Customers can also define rewrite policies, application firewall policies, compression policies and application level monitoring policies.

In this environment, flex tier can comprise of one or more MPX devices while the tenant tier could comprise of a combination of VPX and MPX devices. Citrix provides Command Center to manage these devices.

Since VPX is a virtual appliance, network administrators can easily create a workflow, using commercial or in-house data center automation tools, to bring up additional NetScaler VPX instances and servers online to support the increased load. NetScaler also provides extensive API that can be used to integrate into the work flow automation tools used in hosting/managed services infrastructures. Network administrators can also use the Citrix Command Center in conjunction to propagate the relevant NetScaler configurations to these newly started NetScaler VPX instances.

The division of services amongst the tiers and the ability to manage them through Command Center and NetScaler APIs enables a hosting provider to scale performance of his application delivery fabric and to streamline his operations.

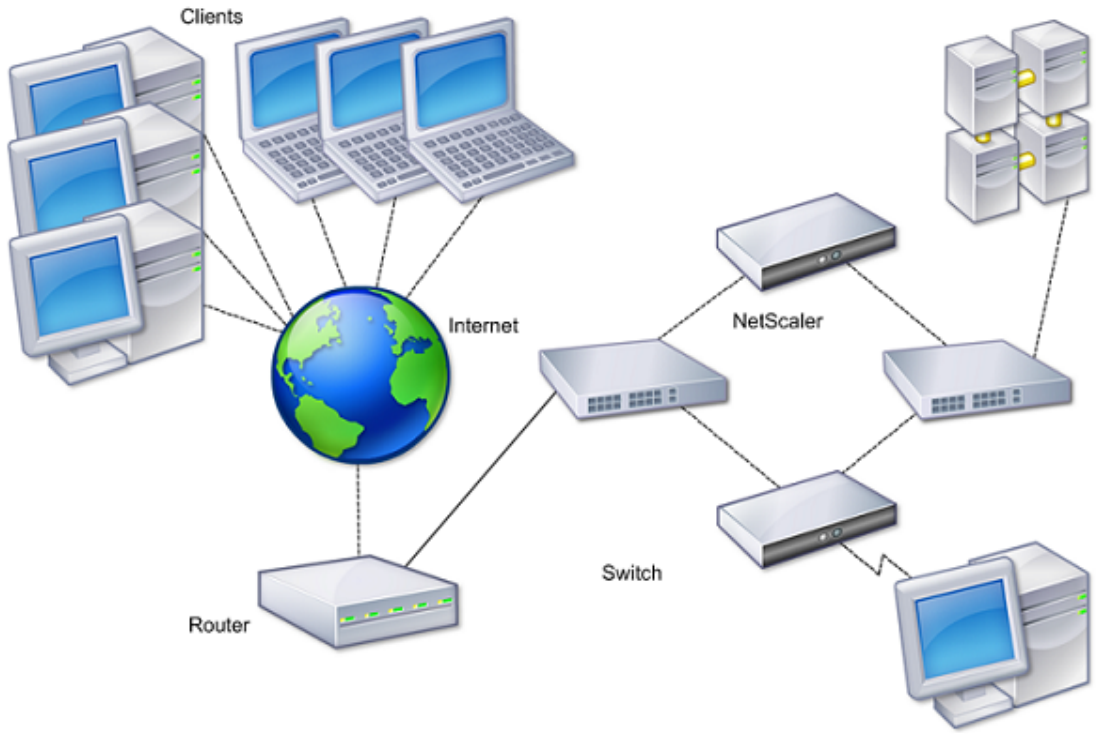
High Availability

A high availability (HA) deployment of two Citrix® NetScaler® appliances can provide uninterrupted operation in any transaction. With one appliance configured as the primary node and the other as the secondary node, the primary node accepts connections and manages servers while the secondary node monitors the primary. If, for any reason, the primary node is unable to accept connections, the secondary node takes over.

The secondary node monitors the primary by sending periodic messages (often called heartbeat messages or health checks) to determine whether the primary node is accepting connections. If a health check fails, the secondary node retries the connection for a specified period, after which it determines that the primary node is not functioning normally. The secondary node then takes over for the primary (a process called failover).

After a failover, all clients must reestablish their connections to the managed servers, but the session persistence rules are maintained as they were before the failover.

With Web server logging persistence enabled, no log data is lost due to the failover. For logging persistence to be enabled, the log server configuration must carry entries for both systems in the log.conf file.



The following figure shows a network configuration with an HA pair.Figure 1. NetScaler Appliances in a High Availability Configuration

To configure HA, you might want to begin by creating a basic setup, with both nodes in the same subnet. You can then customize the intervals at which the nodes communicate health-check information, the process by which nodes maintain synchronization, and the

propagation of commands from the primary to the secondary. You can configure fail-safe mode to prevent a situation in which neither node is primary. If your environment includes devices that do not accept NetScaler gratuitous ARP messages, you should configure virtual MAC addresses. When you are ready for a more complex configuration, you can configure HA nodes in different subnets.

To improve the reliability of your HA setup, you can configure route monitors and create redundant links. In some situations, such as when troubleshooting or performing maintenance tasks, you might want to force a node to fail over (assign primary status to the other node), or you might want to force the secondary node to stay secondary or the primary node to stay primary.

Considerations for a High Availability Setup

Note the following requirements for configuring systems in an HA setup:

- In an HA configuration, the primary and secondary NetScaler appliances should be of the same model. Different NetScaler models are not supported in an HA pair (for example, you cannot configure a 10010 model and a 7000 model as an HA pair).
- In an HA setup, both nodes must run the same version of NetScaler, for example, nCore/nCore or classic/classic. If the nodes are running NetScaler classic and you want to migrate to NetScaler nCore of the same NetScaler release, prop and sync are not supported during the migration process. Once migration is complete, prop and sync are auto-enabled. The same applies if you migrate from NetScaler nCore to NetScaler classic.
- Entries in the configuration file (ns.conf) on both the primary and the secondary system must match, with the following exceptions:
  - The primary and the secondary systems must each be configured with their own unique NetScaler IP addresses (NSIPs.)
  - In an HA pair, the node ID and associated IP address of one node must point to the other node. For example, if you have nodes NS1 and NS2, you must configure NS1 with a unique node ID and the IP address of NS2, and you must configure NS2 with a unique node ID and the IP address of NS1.
- If you create a configuration file on either node by using a method that does not go directly through the GUI or the CLI (for example, importing SSL certificates, or changing to startup scripts), you must copy the configuration file to the other node or create an identical file on that node.
- Initially, all NetScaler appliances are configured with the same RPC node password. RPC nodes are internal system entities used for system-to-system communication of configuration and session information. For security, you should change the default RPC node passwords.

  One RPC node exists on each NetScaler. This node stores the password, which is checked against the password provided by the contacting system. To communicate with other systems, each NetScaler requires knowledge of those systems, including how to authenticate on those systems. RPC nodes maintain this information, which includes the IP addresses of the other systems, and the passwords they require for authentication.

  RPC nodes are implicitly created when adding a node or adding a Global Server Load Balancing (GSLB) site. You cannot create or delete RPC nodes manually.

  Note: If the NetScaler appliances in a high availability setup are configured in one-arm mode, you must disable all system interfaces except the one connected to the switch or hub.
- For an IPv6 HA configuration, the following considerations apply:

- You must install the IPv6PT license on both NetScaler appliances.
- After installing the IPv6PT license, enable the IPv6 feature by using the configuration utility or the command line interface.
- Both NetScaler appliances require a global NSIP IPv6 address. In addition, network entities (for example, switches and routers) between the two nodes must support IPv6.

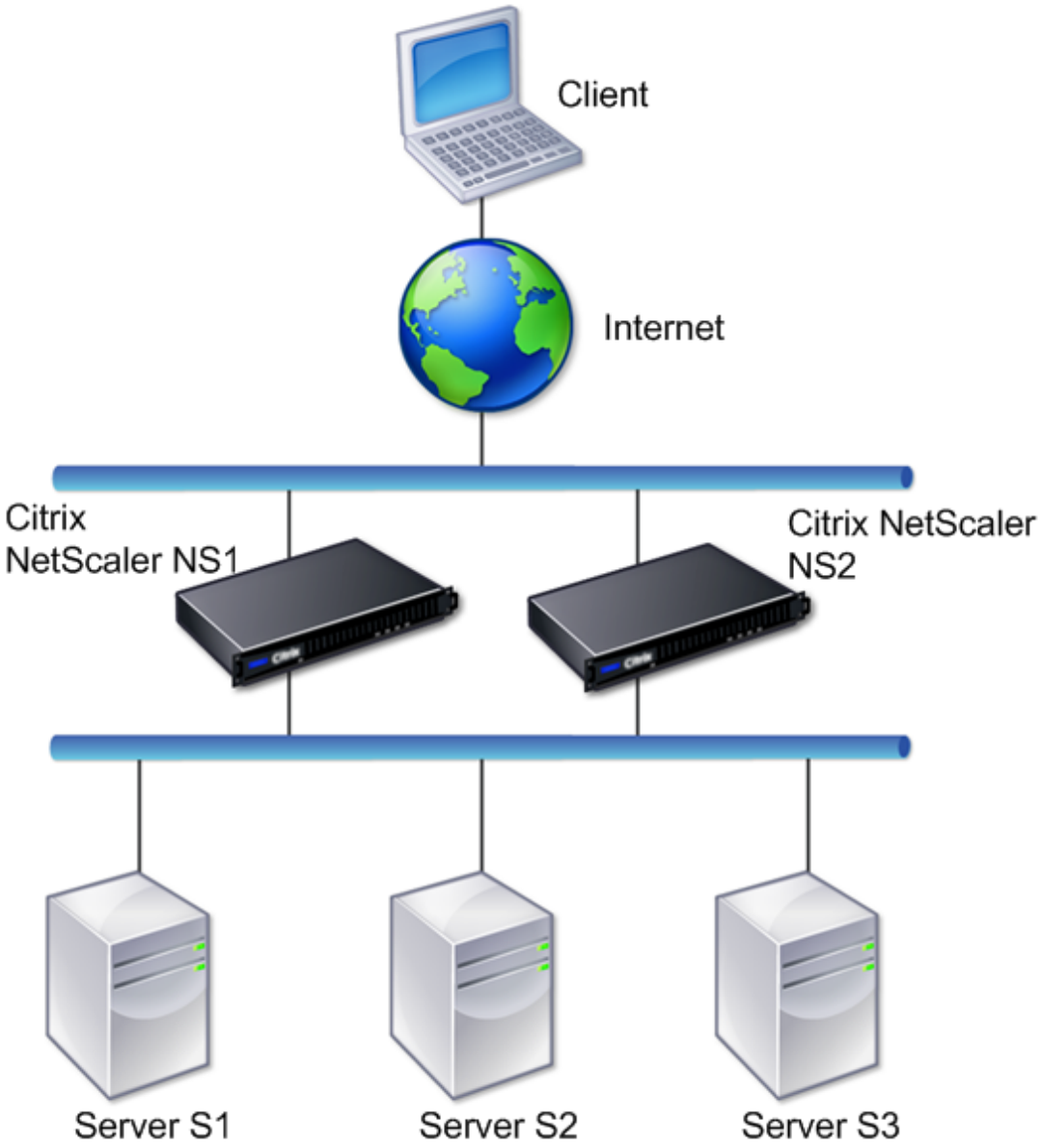
Configuring High Availability

To set up a high availability configuration, you create two nodes, each of which defines the other's NetScaler IP (NSIP) address as a remote node. Begin by logging on to one of the two NetScaler appliances that you want to configure for high availability, and add a node. Specify the other appliance's NetScaler IP (NSIP) address as the address of the new node. Then, log on to the other appliance and add a node that has the NSIP address of the first appliance. An algorithm determines which node becomes primary and which becomes secondary.

Note: The configuration utility provides an option that avoids having to log on to the second appliance.

The following figure shows a simple HA setup, in which both nodes are in same subnet.

Figure 1. Two NetScaler Appliances Connected in a High Availability Configuration


Client
Internet
Citrix
NetScaler NS1
Citrix NetScaler
NS2
Server S1
Server S2
Server S3

Adding a Remote Node

To add a remote NetScaler appliance as a node in a high availability setup, you specify a unique node ID and the appliance's NSIP. The maximum number of node IDs in an HA setup is 64. When you add an HA node, you must disable the HA monitor for each interface that is not connected or not being used for traffic. For CLI users, this is a separate procedure.

Note: To ensure that each node in the high availability configuration has the same settings, you should synchronize your SSL certificates, startup scripts, and other configuration files with those on the primary node.

To add a node by using the command line interface

At the command prompt, type:

- add ha node <id> <IPAddress>
- show ha node

Example

```
> add ha node 3 1000:0000:0000:0000:0005:0600:700a:888b
```

To disable an HA monitor by using the command line interface

At the command prompt, type:

- set interface <ifNum> [-haMonitor (**ON** | **OFF**)]
- show interface <ifNum>

Example

```
> set interface 1/3 -haMonitor OFF
 Done
```

To add a remote node by using the configuration utility

Navigate to System > High Availability and, on the Nodes tab, add a new remote node, or edit an existing node.

Parameter Descriptions (of commands listed in the CLI procedure)

add ha node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ha node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

set interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Disabling or Enabling a Node

You can disable or enable only a secondary node. When you disable a secondary node, it stops sending heartbeat messages to the primary node, and therefore the primary node can no longer check the status of the secondary. When you enable a node, the node takes part in the high availability configuration.

To disable or enable a node by using the command line interface

At the command prompt, type one of the following commands:

- set ha node -hastatus DISABLED
- set ha node -hastatus ENABLED

To disable or enable a node by using the configuration utility

1. Navigate to System > High Availability and, on the Nodes tab, open the node.
2. In the High Availability Status list, select ENABLED (Actively Participate in HA) or DISABLED (Do not participate in HA).

Parameter Descriptions (of commands listed in the CLI procedure)

set ha node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Removing a Node

If you remove a node, the nodes are no longer in high availability configuration.

To remove a node by using the command line interface

At the command prompt, type:

rm ha node <id>

Example

```
> rm ha node 2
  Done
```

To remove a node by using the configuration utility

Navigate to System > High Availability and, on the Nodes tab, delete the node.

Note: You can use the Network Visualizer to view the NetScaler appliances that are configured as a high availability (HA) pair and perform high availability configuration tasks. For more information, see " Using the Network Visualizer."

Parameter Descriptions (of commands listed in the CLI procedure)

rm ha node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring the Communication Intervals

The hello interval is the interval at which the heartbeat messages are sent to the peer node. The dead interval is the time interval after which the peer node is marked DOWN if heartbeat packets are not received. The heartbeat messages are UDP packets sent to port 3003 of the other node in an HA pair.

To set the hello and dead intervals by using the command line interface

At the command prompt, type:

- set HA node [-helloInterval <msecs>] [-deadInterval <secs>]
- show HA node <id>

To set the hello and dead intervals by using the configuration utility

1. Navigate to System > High Availability and, on the Nodes tab, open the node.
2. Set the following parameters:
    - Hello Interval (msecs)
    - Dead Interval (secs)

Parameter Descriptions (of commands listed in the CLI procedure)

set HA node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show HA node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Synchronization

Synchronization is a process of duplicating the configuration of the primary node on the secondary node. The purpose of synchronization is to ensure that there is no loss of configuration information between the primary and the secondary nodes, regardless of the number of failovers that occur. Synchronization uses port 3010.

Synchronization is triggered by either of the following circumstances:

- The secondary node in an HA setup comes up after a restart.
- The primary node becomes secondary after a failover.

Automatic synchronization is enabled by default. You can also force synchronization.

Disabling or Enabling Synchronization

Automatic HA synchronization is enabled by default on each node in an HA pair. You can enable or disable it on either node.

To disable or enable automatic synchronization by using the command line interface

At the command prompt, type:

- set HA node -haSync DISABLED
- set HA node -haSync ENABLED

To disable or enable synchronization by using the configuration utility

1. Navigate to System > High Availability and, on the Nodes tab, open the node.
2. Under HA Synchronization, clear or select the Secondary node will fetch the configuration from Primary option.

Parameter Descriptions (of commands listed in the CLI procedure)

set HA node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Forcing the Secondary Node to Synchronize with the Primary Node

In addition to automatic synchronization, the NetScaler supports forced synchronization. You can force the synchronization from either the primary or the secondary node. When you force synchronization from the secondary node, it starts synchronizing its configuration with the primary node.

However, if synchronization is already in progress, forced synchronization fails and the system displays a warning. Forced synchronization also fails in any of the following circumstances:

- You force synchronization on a standalone system.
- The secondary node is disabled.
- HA synchronization is disabled on the secondary node.

To force synchronization by using the command line interface

At the command prompt, type:

force HA sync

To force synchronization by using the configuration utility

1. Navigate to System > High Availability.
2. On the Nodes tab, click Force Synchronization.

Parameter Descriptions (of commands listed in the CLI procedure)

force HA sync

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Synchronizing Configuration Files in a High Availability Setup

In a high availability setup, you can synchronize various configuration files from the primary node to the secondary node.

To perform the synchronization, you can use the command line interface or the configuration utility at either the primary or the secondary node. Files located on the secondary that are specific to the secondary (not present on the primary) are not deleted during the synchronization.

To synchronize files in a high availability setup by using the command line interface

At the command prompt, type:

sync HA files <mode>

Example

```
> sync HA files all
 Done
```

To synchronize files in a high availability setup by using the configuration utility

Navigate to System > Diagnostics and, in the Utilities group, click Start HA files synchronization.

Parameter Descriptions (of commands listed in the CLI procedure)

sync HA files

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Command Propagation

In an HA setup, any command issued on the primary node propagates automatically to, and is executed on, the secondary before it is executed on the primary. If command propagation fails, or if command execution fails on the secondary, the primary node executes the command and logs an error. Command propagation uses port 3010.

In an HA pair configuration, command propagation is enabled by default on both the primary and secondary nodes. You can enable or disable command propagation on either node in an HA pair. If you disable command propagation on the primary node, commands are not propagated to the secondary node. If you disable command propagation on the secondary node, commands propagated from the primary are not executed on the secondary node.

Note: After reenabling propagation, remember to force synchronization.

If synchronization occurs while you are disabling propagation, any configuration-related changes that you make before the disabling of propagation takes effect are synchronized with the secondary node. This is also true for cases where propagation is disabled while synchronization is in progress.

To disable or enable command propagation by using the command line interface

At the command prompt, type:

- set HA node -haProp DISABLED
- set HA node -haProp ENABLED

To disable or enable command propagation by using the configuration utility

1. Navigate to System > High Availability and, on the Nodes tab, open the node.
2. Clear or select the Primary node will propagate configuration to the Secondary option.

Parameter Descriptions (of commands listed in the CLI procedure)

set HA node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Fail-Safe Mode

In an HA configuration, fail-safe mode ensures that one node is always primary when both nodes fail the health check. This is to ensure that when a node is only partially available, backup methods are enabled to handle traffic as best as possible. The HA fail-safe mode is configured independently on each node.

The following table shows some of the fail-safe cases. The NOT_UP state means that the node failed the health check yet it is partially available. The UP state means that the node passed the health check.

Table 1. Fail-Safe Mode Cases

Node A (Primary) Health State	Node B (Secondary) Health State	Default HA Behavior	Fail-Safe Enabled HA Behavior	Description
NOT_UP(failed last)	NOT_UP (failed first)	A (Secondary), B (Secondary)	A (Primary), B (Secondary)	If both nodes fail, one after the other, the node that was the last primary remains primary.
NOT_UP (failed first)	NOT_UP(failed last)	A (Secondary), B (Secondary)	A(Secondary), B(Primary)	If both nodes fail, one after the other, the node that was the last primary remains primary.
UP	UP	A (Primary), B (Secondary)	A (Primary), B (Secondary)	If both nodes pass the health check, no change in behavior with fail-safe enabled.
UP	NOT_UP	A(Primary), B(Secondary)	A (Primary), B (Secondary)	If only the secondary node fails, no change in behavior with fail-safe enabled.
NOT_UP	UP	A(Secondary), B(Primary)	A(Secondary), B(Primary)	If only the primary fails, no change in behavior with fail-safe enabled.
NOT_UP	UP (STAYSECONDARY)	A (Secondary), B (Secondary)	A (Primary), B (Secondary)	If the secondary is configured as STAYSECONDARY, the primary remains primary even if it fails.

To enable fail-safe mode by using the command line interface

At the command prompt, type:

set HA node [-failSafe (**ON** | **OFF**)]

Example

set ha node -failsafe ON

To enable fail-safe mode by using the configuration utility

1. Navigate to System > High Availability and, on the Nodes tab, open the node.
2. Under Fail-Safe Mode, select the Maintain one Primary node even when both nodes are unhealthy option.

Parameter Descriptions (of commands listed in the CLI procedure)

set HA node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Virtual MAC Addresses

A Virtual MAC address (VMAC) is a floating entity shared by the primary and the secondary nodes in an HA setup.

In an HA setup, the primary node owns all of the floating IP addresses, such as the MIPs, SNIPs, and VIPs. The primary node responds to Address Resolution Protocol (ARP) requests for these IP addresses with its own MAC address. As a result, the ARP table of an external device (for example, an upstream router) is updated with the floating IP address and the primary node's MAC address.

When a failover occurs, the secondary node takes over as the new primary node. It then uses Gratuitous ARP (GARP) to advertise the floating IP addresses that it acquired from the primary. However, the MAC address that the new primary advertises is the MAC address of its own interface.

Some devices (notably a few routers) do not accept the GARP messages generated by the NetScaler appliance. As a result, some external devices retain the old IP to MAC mapping advertised by the old primary node. This can result in a site going down.

You can overcome this problem by configuring a VMAC on both nodes of an HA pair. Both nodes then possess identical MAC addresses. Therefore, when failover occurs, the MAC address of the secondary node remains unchanged, and the ARP tables on the external devices do not need to be updated.

To create a VMAC, you need to first create a Virtual Router ID (VRID) and bind it to an interface. (In an HA setup, you need to bind the VRID to the interfaces on both nodes.) Once the VRID is bound to an interface, the system generates a VMAC with the VRID as the last octet.

Configuring IPv4 VMACs

When you create a IPv4 VMAC address and bind it to a interface, any IPv4 packet sent from the interface uses the VMAC address that is bound to the interface. If there is no IPv4 VMAC bound to an interface, the interface's physical MAC address is used.

The generic VMAC is of the form 00:00:5e:00:01:<VRID>. For example, if you create a VRID with a value of 60 and bind it to an interface, the resulting VMAC is 00:00:5e:00:01:3c, where 3c is the hex representation of the VRID. You can create 255 VRIDs with values from 1 to 255.

Creating or Modifying an IPv4 VMAC

You create an IPv4 virtual MAC by assigning it a virtual router ID. You can then you bind the VMAC to an interface. You cannot bind multiple VRIDs to the same interface. To verify the VMAC configuration, you should display and examine the VMACs and the interfaces bound to the VMACs.

To add a VMAC by using the command line interface

At the command prompt, type:

- add vrID <id>
- bind vrid <id> -ifnum <interface_name>
- show vrID

Example

```
> add vrID 100
 Done
> bind vrid 100 -ifnum 1/1 1/2 1/3
 Done
```

To unbind interfaces from a VMAC by using the command line interface

At the command prompt, type:

- unbind vrid <id> -ifnum <interface_name>
- show vrID

To configure a VMAC by using the configuration utility

Navigate to Network > VMAC and, on the VMAC tab, add a new VMAC, or edit an existing VMAC.

Parameter Descriptions (of commands listed in the CLI procedure)

add vrID

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind vrid

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show vrID

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

unbind vrid

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Removing an IPv4 VMAC

To remove an IPv4 virtual MAC, you delete its virtual router ID.

To remove an IPv4 VMAC by using the command line interface

At the command prompt, type:

rm vrid <id>

Example

rm vrid 100s

To remove an IPv4 VMAC by using the configuration utility

Navigate to Network > VMAC and, on the VMAC tab, delete the IPv4 VMAC.

Parameter Descriptions (of commands listed in the CLI procedure)

rm vrid

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring IPv6 VMAC6s

The NetScaler supports VMAC6 for IPv6 packets. You can bind any interface to a VMAC6, even if an IPv4 VMAC is bound to the interface. Any IPv6 packet sent from the interface uses the VMAC6 bound to that interface. If there is no VMAC6 bound to an interface, an IPv6 packet uses the physical MAC.

Creating or Modifying a VMAC6

You create an IPv6 virtual MAC by assigning it an IPv6 virtual router ID. You can then you bind the VMAC to an interface. You cannot bind multiple IPv6 VRIDs to an interface. To verify the VMAC6 configuration, you should display and examine the VMAC6s and the interfaces bound to the VMAC6s.

To add a VMAC6 by using the command line interface

At the command prompt, type:

- add vrID6 <id>
- bind vrID6 <id> -ifnum <interface_name>
- show vrID6

Example

```
> add vrID6 100
Done
> bind vrID6 100 -ifnum 1/1 1/2 1/3
 Done
```

To unbind interfaces from a VMAC6 by using the command line interface

At the command prompt, type:

- unbind vrID6 <id> -ifnum <interface_name>
- show vrID6

To configure a VMAC6 by using the configuration utility

Navigate to Network > VMAC and, on the VMAC6 tab, add a new VMAC6, or edit an existing VMAC6.

Parameter Descriptions (of commands listed in the CLI procedure)

add vrID6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind vrID6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show vrID6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

unbind vrID6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Removing a VMAC6

To remove an IPv4 virtual MAC, you delete its virtual router ID.

To remove a VMAC6 by using the command line interface

At the command prompt, type:

rm vrid6 <id>

Example

rm vrid6 100s

To remove a VMAC6 by using the configuration utility

Navigate to System > Network > VMAC and, on the VMAC6 tab, delete the virtual router ID.

Parameter Descriptions (of commands listed in the CLI procedure)

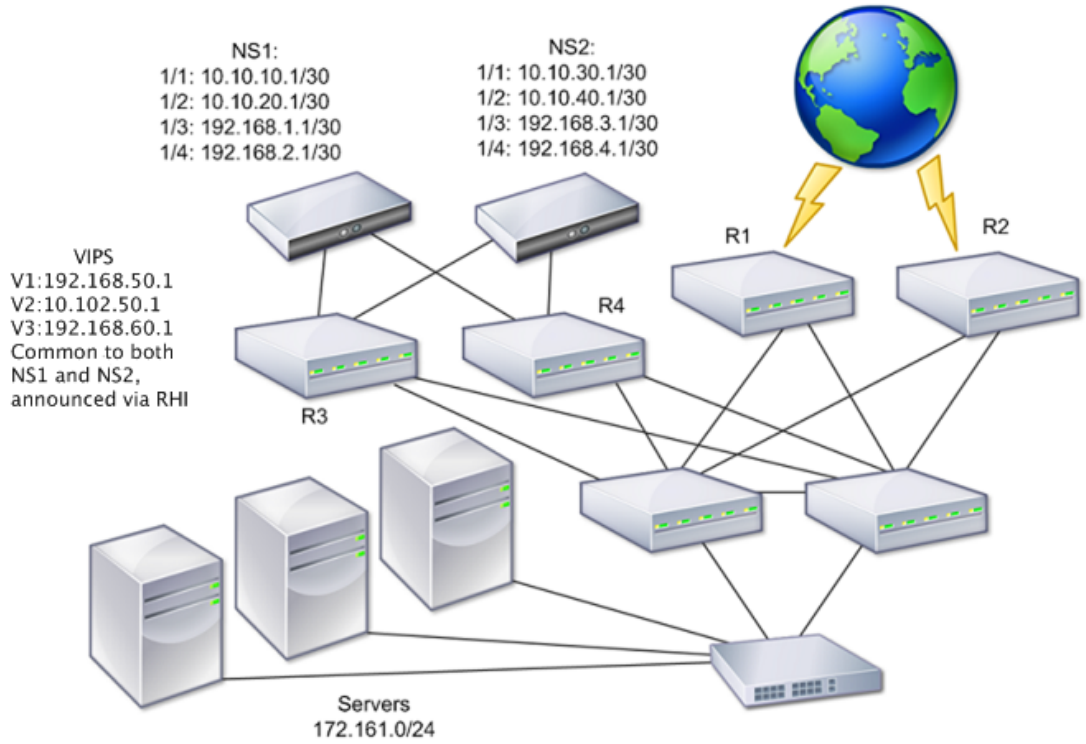
rm vrid6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring High Availability Nodes in Different Subnets

The following figure shows an HA deployment with the two systems located in different subnets:

Figure 1. High Availability over a Routed Network



In the figure, the systems NS1 and NS2 are connected to two separate routers, R3 and R4, on two different subnets. The NetScaler appliances exchange heartbeat packets through the routers. This configuration could be expanded to accommodate deployments involving any number of interfaces.

Note: If you use static routing on your network, you must add static routes between all the systems to ensure that heartbeat packets are sent and received successfully. (If you use dynamic routing on your systems, static routes are unnecessary.)

If the nodes in an HA pair reside on two separate networks, the primary and secondary node must have independent network configurations. This means that nodes on different networks cannot share entities such as MIPs, SNIPs, VLANs, and routes. This type of configuration, where the nodes in an HA pair have different configurable parameters, is known as Independent Network Configuration (INC) or Symmetric Network Configuration (SNC).

The following table summarizes the configurable entities and options for an INC, and shows how they must be set on each node.

Table 1. Behavior of NetScaler Entities and Options in an Independent Network Configuration

NetScaler entities	Options
IPs (NSIP/MIP/SNIPs)	Node-specific. Active only on that node.
VIPs	Floating.
VLANs	Node-specific. Active only on that node.
Routes	Node-specific. Active only on that node. Link load balancing routes are floating.
ACLs	Floating (Common). Active on both nodes.
Dynamic routing	Node-specific. Active only on that node. The secondary node should also run the routing protocols and peer with upstream routers.
L2 mode	Floating (Common). Active on both nodes.
L3 mode	Floating (Common). Active on both nodes.
Reverse NAT (RNAT)	Node-specific. RNAT with VIP, because NATIP is floating.

As in configuring HA nodes in the same subnet, to configure HA nodes in different subnets, you log on to each of the two NetScaler appliances and add a remote node representing the other appliance.

Adding a Remote Node

When two nodes of an HA pair reside on different subnets, each node must have a different network configuration. Therefore, to configure two independent systems to function as an HA pair, you must specify INC mode during the configuration process.

When you add an HA node, you must disable the HA monitor for each interface that is not connected or not being used for traffic. For CLI users, this is a separate procedure.

To add a node by using the command line interface

At the command prompt, type:

- add ha node <id> <IPAddress> -inc ENABLED
- show ha node

Example

```
> add ha node 3 10.102.29.170 -inc ENABLED
 Done
> add ha node 3 1000:0000:0000:0000:0005:0600:700a:888b
  Done
```

To disable an HA monitor by using the command line interface

At the command prompt, type:

- set interface <ifNum> [-haMonitor (**ON** | **OFF**)]
- show interface <ifNum>

Example

```
> set interface 1/3 -haMonitor OFF
 Done
```

To add a remote node by using the configuration utility

1. Navigate to System > High Availability and, on the Nodes tab, add a new remote node.
2. Make sure to select the Turn off HA monitor on interfaces/channels that are down and Turn on INC (Independent Network Configuration) mode on self mode options.

Parameter Descriptions (of commands listed in the CLI procedure)

add ha node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ha node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

set interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Removing a Node

If you remove a node, the nodes are no longer in high availability configuration.

To remove a node by using the command line interface

At the command prompt, type:

rm ha node <id>

Example

```
> rm ha node 2
  Done
```

To remove a node by using the configuration utility

Navigate to System > High Availability and, on the Nodes tab, delete the node.

Note: You can use the Network Visualizer to view the NetScaler appliances that are configured as a high availability (HA) pair and perform high availability configuration tasks. For more information, see " Using the Network Visualizer."

Parameter Descriptions (of commands listed in the CLI procedure)

rm ha node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Route Monitors

You can use route monitors to make the HA state dependent on the internal routing table, whether or not the table contains any dynamically learned or static routes. In an HA configuration, a route monitor on each node watches the internal routing table to make sure that a route entry for reaching a particular network is always present. If the route entry is not present, the state of the route monitor changes to DOWN.

When a NetScaler appliance has only static routes for reaching a network, and you want to create a route monitor for the network, you must enable monitored static routes (MSR) for the static routes. MSR removes unreachable static routes from the internal routing table. If MSR is disabled on static routes, an unreachable static route can remain in the internal routing table, defeating the purpose of having the route monitor.

Route Monitors are supported both in non-INC and INC mode.

Route Monitors in HA in non-INC mode	Route Monitors in HA in INC mode
Route monitors are propagated by nodes and exchanged during synchronization.	Route monitors are neither propagated by nodes nor exchanged during synchronization.
Route monitors are active only in the current primary node.	Route monitors are active on both the primary and the secondary node.
The NetScaler appliance always displays the state of a route monitor as UP irrespective of the whether the route entry is present or not in the internal routing table.	The NetScaler appliance displays the state of the route monitor as DOWN if the corresponding route entry is not present in the internal routing table.

A route monitor starts monitoring its route after 180 seconds in the following cases [This is done to allow dynamic routes to get learnt, which may take 180 secs]: · reboot · failover · set route6 command for v6 routes · set route msr enable/disable command for v4 routes. · adding a new route monitor	-

Route monitors are useful in a non-INC mode HA configuration where you want the non-reachability of a gateway from a primary node to be one of the conditions for HA failover.

Consider an example of a non-Inc mode HA setup in a two-arm topology that has NetScaler appliances NS1 and NS2 in the same subnet, with router R1 and switches SW1, SW2, and SW3.

Because R1 is the only router in this setup, you want the HA setup to failover whenever R1 is not reachable from the current primary node. You can configure a route monitor (say, RM1 and RM2, respectively) on each of the nodes to monitor the reachability of R1 from that node.

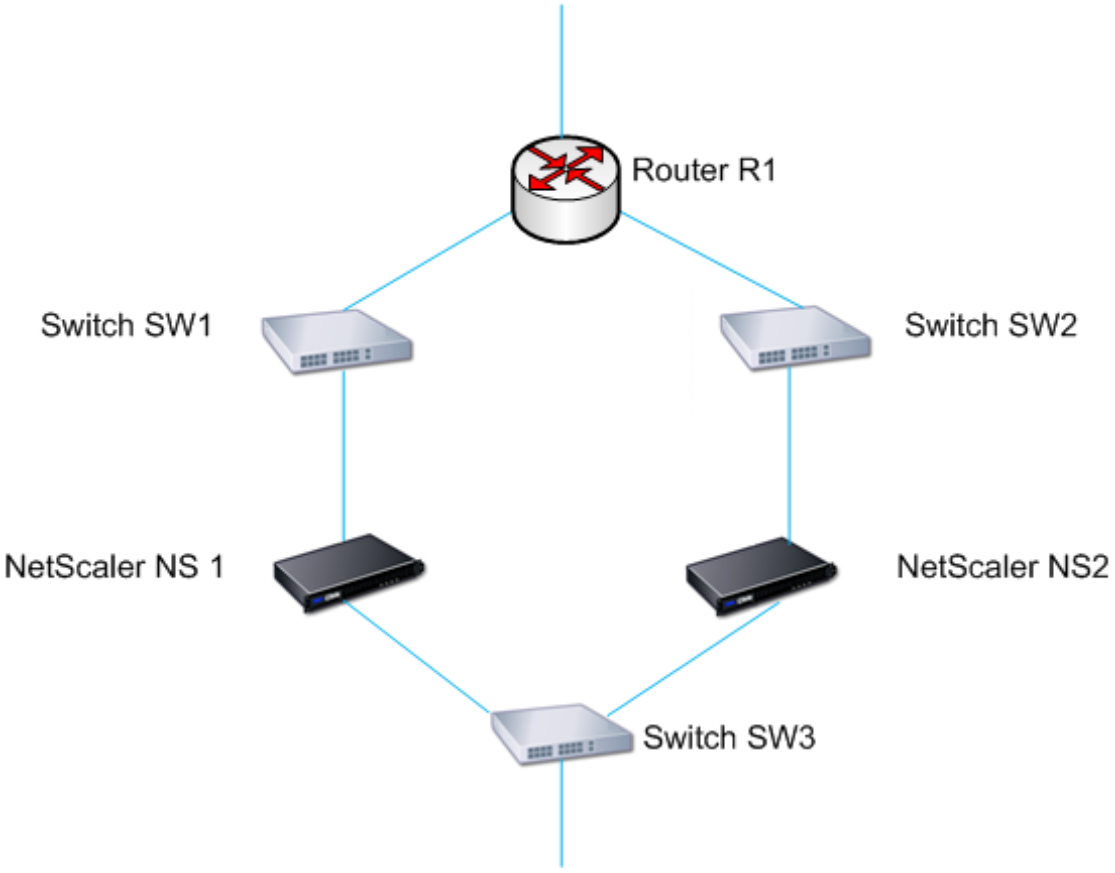


Figure 1.

With NS1 as the current primary node, the execution flow is as follows:

1. Route monitor RM1 on NS1 monitors NS1's internal routing table for the presence of a route entry for router R1. NS1 and NS2 exchange heartbeat messages through switch SW1 or SW3 at regular intervals.

2. If switch SW1 goes down, the routing protocol on NS1 detects that R1 is not reachable and therefore removes the route entry for R1 from the internal routing table. NS1 and NS2 exchanges heartbeat messages through switch SW3 at regular intervals.

3. Detecting that the route entry for R1 is not present in the internal routing table, RM1 initiates a failover. If route to R1 is down from both NS1 and NS2, failover happens every 180 seconds till one of the appliances is able to reach R1 and restore the connectivity.

Adding a Route Monitor to a High Availability Node

A single procedure creates a route monitor and binds it to an HA node.

To add a route monitor by using the command line interface

At the command prompt, type:

- bind HA node <id> (-routeMonitor <ip_addr|ipv6_addr> [<netmask>])
- show HA node

Example

```
> bind HA node 0 -routeMonitor 10.102.71.0 255.255.255.0
 Done
> bind HA node 0 -routeMonitor 1000:0000:0000:0000:0005:0600:700a:888b
 Done
```

To add a route monitor by using the configuration utility

Navigate to System > High Availability and, on the Route Monitors tab, click Configure.

Parameter Descriptions (of commands listed in the CLI procedure)

bind HA node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show HA node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Removing Route Monitors

To remove a route monitor by using the command line interface

At the command prompt, type:

- unbind HA node <id> (-routeMonitor <ip_addr|ipv6_addr> [<netmask>])
- show ha node

Example

unbind HA node 3 -routeMonitor 10.102.71.0 255.255.255.0
unbind HA node 3 -routeMonitor 1000:0000:0000:0000:0005:0600:700a:888b

To remove a route monitor by using the configuration utility

Navigate to System > High Availability and, on the Route Monitors tab, delete the route monitor.

Parameter Descriptions (of commands listed in the CLI procedure)

unbind HA node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ha node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Limiting Failovers Caused by Route Monitors in non-INC mode

In an HA configuration in non-INC mode, if route monitors fail on both nodes, failover happens every 180 seconds until one of the nodes is able to reach all of the routes monitored by the respective route monitors.

However, for a node, you can limit the number of failovers for a given interval by setting the Maximum Number of Flips and Maximum Flip Time parameters on the nodes. When either limit is reached, no more failovers occur, and the node is assigned as primary even if any route monitor fails on that node. If the node is then able to reach all of the monitored routes, the next monitor failure triggers resetting of the Maximum Number of Flips and Maximum Flip Time parameters on the node and starting the time specified in the Maximum Flip Time parameter.

These parameters are set independently on each node and therefore are neither propagated nor synchronized.

Note: This feature is supported only on NetScaler 9.3.e.

Parameters for limiting the number of failovers

Maximum Number of Flips (maxFlips)

Maximum number of failovers allowed, within the Maximum Flip Time interval, for the node in HA in non INC mode, if the failovers are caused by route-monitor failure.

Maximum Flip Time (maxFlipTime)

Amount of time, in seconds, during which failovers resulting from route-monitor failure are allowed for the node in HA in non INC mode.

To limit the number of failovers by using the command line interface

At the command prompt, type:

- `set HA node [-maxFlips < positive_integer>] [-maxFlipTime <positive_integer>]`
- `show HA node [< id>]`

Example

```
> set ha node -maxFlips 30 -maxFlipTime 60
 Done
> sh ha node
1) Node ID: 0
 IP: 10.102.169.82 (NS)
 Node State: UP
 Master State: Primary
 Fail-Safe Mode: OFF
```

```
 INC State: DISABLED
 Sync State: ENABLED
 Propagation: ENABLED
 Enabled Interfaces : 1/1
 Disabled Interfaces : None
 HA MON ON Interfaces : 1/1
 Interfaces on which heartbeats are not seen :None
 Interfaces causing Partial Failure:None
 SSL Card Status: NOT PRESENT
 Hello Interval: 200 msecs
 Dead Interval: 3 secs
 Node in this Master State for: 0:4:24:1
 (days:hrs:min:sec)
2) Node ID: 1
 IP: 10.102.169.81
 Node State: UP
 Master State: Secondary
 Fail-Safe Mode: OFF
 INC State: DISABLED
 Sync State: SUCCESS
 Propagation: ENABLED
 Enabled Interfaces : 1/1
 Disabled Interfaces : None
 HA MON ON Interfaces : 1/1
 Interfaces on which heartbeats are not seen : None
 Interfaces causing Partial Failure: None
 SSL Card Status: NOT PRESENT

Local node information:
 Configured/Completed Flips: 30/0
 Configured Flip Time: 60
 Critical Interfaces: 1/1

Done
```

To limit the number of failovers by using the configuration utility

1. Navigate to System > High Availability and, on the Nodes tab, open the local node.
2. Set the following parameters:
   - Maximum Number of Flips
   - Maximum Flip Time

Configuring FIS

Link redundancy is a way to prevent failover by grouping interfaces so that, when one interface fails, other functioning interfaces are still available. The link redundancy feature allows you to group the two interfaces into a failover interface set (FIS), which prevents the failure of a single link from causing failover to the secondary system unless all of the interfaces on the primary system are nonfunctional.

Each interface in an FIS maintains independent bridge entries. HA MON interfaces that are not bound to an FIS are known as critical interfaces (CI) because if any of them fails, failover is triggered.

Creating or Modifying an FIS

To add an FIS and bind interfaces to it by using the command line interface

At the command prompt, type:

- add fis <name>
- bind fis <name> <ifnum> ...
- show fis <name>

Example

```
> add fis fis1
 Done
> bind fis fis1 1/3 1/5
 Done
```

An unbound interface becomes a critical interface (CI) if it is enabled and HA MON is on.

To unbind an interface from an FIS by using the command line interface

At the command prompt, type:

- unbind fis <name> <ifnum> ...
- show fis <name>

Example

```
> unbind fis fis1 1/3
 Done
```

To configure an FIS by using the configuration utility

Navigate to System > High Availability and, on the Failover Interface Set tab, add a new FIS, or edit an existing FIS.

Parameter Descriptions (of commands listed in the CLI procedure)

add fis

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind fis

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show fis

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

unbind fis

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Removing an FIS

When the FIS is removed, its interfaces are marked as critical interfaces.

To remove an FIS by using the command line interface

At the command prompt, type:

rm fis <name>

Example

```
> rm fis fis1
  Done
```

To remove an FIS by using the configuration utility

Navigate to System > High Availability and, on the Failover Interface Set tab, delete the FIS.

Parameter Descriptions (of commands listed in the CLI procedure)

rm fis

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Understanding the Causes of Failover

The following events can cause failover in an HA configuration:

1. If the secondary node does not receive a heartbeat packet from the primary for a period of time that exceeds the dead interval set on the secondary. (See Note: 1.)
2. The primary node experiences a hardware failure of its SSL card.
3. The primary node does not receive any heartbeat packets on its network interfaces for three seconds.
4. On the primary node, a network interface that is not part of a Failover Interface Set (FIS) or a Link Aggregation (LA) channel and has the HA Monitor (HAMON) enabled, fails. (See Note: 2.)
5. On the primary node, all interfaces in an FIS fail. (See Note: 2.)
6. On the primary node, an LA channel with HAMON enabled fails. (See Note: 2.)
7. On the primary node, all interfaces fail (see Note: 2). In this case, failover occurs regardless of the HAMON configuration.
8. On the primary node, all interfaces are manually disabled. In this case, failover occurs regardless of the HAMON configuration.
9. You force a failover by issuing the force failover command on either node.
10. A route monitor that is bound to the primary node goes DOWN.

Note: 1. For more information about setting the dead interval, see Configuring the Communication Intervals. Possible causes for a node not receiving heartbeat packets from a peer node include:

- A network configuration problem prevents heartbeats from traversing the network between the HA nodes.
- The peer node experiences a hardware or software failure that causes it to freeze (hang), reboot, or otherwise stop processing and forwarding heartbeat packets.

Note: 2. In this case, fail means that the interface was enabled but goes to the DOWN state, as can be seen from the show interface command or from the configuration utility. Possible causes for an enabled interface to be in the DOWN state are LINK DOWN and TXSTALL.

Forcing a Node to Fail Over

You might want to force a failover if, for example, you need to replace or upgrade the primary node. You can force failover from either the primary or the secondary node. A forced failover is not propagated or synchronized. To view the synchronization status after a forced failover, you can view the status of the node.

A forced failover fails in any of the following circumstances:

- You force failover on a standalone system.
- The secondary node is disabled.
- The secondary node is configured to remain secondary.

The NetScaler appliance displays a warning message if it detects a potential issue when you run the force failover command. The message includes the information that triggered the warning, and requests confirmation before proceeding.

You can force a failover on a primary node, secondary node, and when nodes are in listen mode.

- **Forcing Failover on the Primary Node**.

  If you force failover on the primary node, the primary becomes the secondary and the secondary becomes the primary. Forced failover is possible only when the primary node can determine that the secondary node is UP.

  If the secondary node is DOWN, the force failover command returns the following error message: "Operation not possible due to invalid peer state. Rectify and retry."

  If the secondary system is in the claiming state or inactive, it returns the following error message: "Operation not possible now. Please wait for system to stabilize before retrying."

- **Forcing Failover on the Secondary Node**.

  If you run the force failover command from the secondary node, the secondary node becomes primary and the primary node becomes secondary. A force failover can occur only if the secondary node’s health is good and it is not configured to stay secondary.

  If the secondary node cannot become the primary node, or if secondary node was configured to stay secondary (using the STAYSECONDARY option), the node displays the following error message: "Operation not possible as my state is invalid. View the node for more information."

- **Forcing Failover When Nodes Are in Listen Mode**.

  When the two nodes of an HA pair are running different versions of the system software, the node running the higher version switches to the listen mode. In this mode, neither command propagation nor synchronization works.

Before upgrading the system software on both nodes, you should test the new version on one of the nodes. To do this, you need to force a failover on the system that has already been upgraded. The upgraded system then takes over as the primary node, but neither command propagation or synchronization occurs. Also, all connections need to be re-established.

To force failover on a node by using the command line interface

At the command prompt, type:

force HA failover

To force failover on a node by using the configuration utility

Navigate to System > High Availability and, on the Nodes tab, click Force Failover.

Parameter Descriptions (of commands listed in the CLI procedure)

force HA failover

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Forcing the Secondary Node to Stay Secondary

In an HA setup, the secondary node can be forced to stay secondary regardless of the state of the primary node.

For example, suppose the primary node needs to be upgraded and the process will take a few seconds. During the upgrade, the primary node may go down for a few seconds, but you do not want the secondary node to take over; you want it to remain the secondary node even if it detects a failure in the primary node.

When you force the secondary node to stay secondary, it will remain secondary even if the primary node goes down. Also, when you force the status of a node in an HA pair to stay secondary, it does not participate in HA state machine transitions. The status of the node is displayed as STAYSECONDARY.

Forcing the node to stay secondary works on both standalone and secondary nodes. On a standalone node, you must use this option before you can add a node to create an HA pair. When you add the new node, the existing node continues to function as the primary node, and the new node becomes the secondary node.

Note: When you force a system to remain secondary, the forcing process is not propagated or synchronized. It affects only the node on which you run the command.

To force the secondary node to stay secondary by using the command line interface

At the command prompt, type:

set ha node -hastatus STAYSECONDARY

To force the secondary node to stay secondary by using the configuration utility

Navigate to System > High Availability, on the Nodes tab, open the local node, and select STAY SECONDARY.

Parameter Descriptions (of commands listed in the CLI procedure)

set ha node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Forcing the Primary Node to Stay Primary

In an HA setup, you can force the primary node to remain primary even after a failover. You can enable this option either on a primary node in an HA pair or on a standalone system.

On a standalone system, you must run this command before you can add a node to create an HA pair. When you add the new node, it becomes the primary node. The existing node stops processing traffic and becomes the secondary node in the HA pair.

To force the primary node to stay primary by using the command line interface

At the command prompt, type:

set ha node -hastatus STAYPRIMARY

To force the primary node to stay primary by using the configuration utility

Navigate to System > High Availability, on the Nodes tab, open the local node, and select STAY PRIMARY.

Parameter Descriptions (of commands listed in the CLI procedure)

set ha node

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Understanding the High Availability Health Check Computation

The following table summarizes the factors examined in a health check computation:

- State of the CIs
- State of the FISs
- State of the route monitors

The following table summarizes the health check computation.

Table 1. High Availability Health Check Computation

FIS	CI	Route monitor	Condition
N	Y	N	If the system has any CIs, all of those CIs must be UP.
Y	Y	N	If the system has any FISs, all of those FISs must be UP.
Y	Y	Y	If the system has any route monitors configured, all monitored routes must be present in the FIS.

Troubleshooting High Availability Issues

Certain conditions can cause improper synchronization between nodes or incorrect configuration on the secondary node.

- **Improper synchronization of VLAN configuration in high availability systems**. In HA pairs, synchronization does not work properly if only one node has a VLAN configured. To prevent this problem, configure your VLANs after you configure your appliances as an HA pair, and be sure to configure them both.

- **Retrieving a lost configuration**. If the primary node is unable to send the configuration to the secondary node due to a network error, the secondary node may not have an accurate configuration and may not behave correctly if a failover occurs. If this happens, you can retrieve the current configuration from the configuration backup on the hard disk of the primary appliance. The operating system saves the last four copies of the ns.conf file in the /nsconfig directory as ns.conf.0, ns.conf.1, ns.conf.2, and ns.conf.3. The ns.conf.0 file contains the current configuration.

To retrieve the current system configuration

1. Exit the CLI to FreeBSD by typing the following command and pressing the Enter key:

   > shell

   The FreeBSD shell prompt appears, as shown below.

   #

2. Copy the latest backup file to /nsconfig/ns.conf by using the following command:

   ```
   # cp ‘ls -t /nsconfig/ns.conf.? | head -1` /nsconfig/ns.conf
   ```

If you perform a configuration using the NSConfig utility, it is not propagated. If you create a configuration using NSconfig, you must repeat the configuration steps separately for each node in an HA pair.

High Availability

What are the various ports used to exchange the HA-related information between the nodes in an HA configuration?

In an HA configuration, both nodes use the following ports to exchange HA related information:

- UDP Port 3003, to exchange heartbeat packets.
- Port 3010, for synchronization and command propagation.

What are the conditions that trigger synchronization?

Synchronization is triggered by any of the following conditions:

- The incarnation number of the primary node, received by the secondary, does not match that of the secondary node.

  Note: Both nodes in an HA configuration maintain a counter called *incarnation number*, which counts the number of configurations in the node's configuration file. Each node sends its incarnation number to each other node in the heartbeat messages. The incarnation number is not incremented for the following commands:

  1. All HA configuration related commands. For example, add ha node, set ha node, and bind ha node.
  2. All Interface related commands. For example, set interface and unset interface.
  3. All channel-related commands. For example, add channel, set channel, and bind channel.
- The secondary node comes up after a restart.
- The primary node becomes secondary after a failover.

What configurations are not synced or propagated in an HA configuration in INC or non-INC mode?

The following commands are neither propagated nor synced to the secondary node:

- All node specific HA configuration commands. For example, add ha node, set ha node, and bind ha node.
- All Interface related configuration commands. For example, set interface and unset interface.
- All channel related configuration commands. For example, add channel, set channel, and bind channel.

What configurations are not synced nor propagated in an HA configuration in INC mode?

The following configurations are not synced or propagated. Each node has its own.

- MIPs

- SNIPs
- VLANs
- Routes (except LLB routes)
- Route monitors
- RNAT rules (except any RNAT rule with VIP as the NAT IP)
- Dynamic routing configurations.

Does a configuration added to the secondary node get synchronized on the primary?

No, a configuration added to the secondary node is not synchronized to the primary.

What could be the reason for both nodes claiming to be the primary in an HA configuration?

The most likely reason is that the primary and secondary nodes are both healthy but the secondary does not receive the heartbeat packets from the primary. The problem could be with the network between the nodes.

Does an HA configuration run into any issues if you deploy the two nodes with different system clock settings?

Different system-clock settings on the two nodes can cause the following issues:

- The time stamps in the log file entries do not match. This situation makes it difficult to analyze the log entries for any issues.
- After a failover, you might have problems with any type of cookie based persistence for load balancing. A significant difference between the times can cause a cookie to expire sooner than expected, resulting in termination of the persistence session.
- Similar considerations apply to any time related decisions on the nodes.

What are the conditions for failure of the *force HA sync* command?

Forced synchronization fails in any of the following circumstances:

- You force synchronization when synchronization is already in progress.
- You force synchronization on a standalone NetScaler appliance.
- The secondary node is disabled.
- HA synchronization is disabled on the current secondary node.
- HA propagation is disabled on the current primary node and you force synchronization from the primary.

What are the conditions for failure of the *sync HA files* command?

Synchronizing configuration files fail in either of the following circumstances:

- On a standalone system.

- With the secondary node disabled.

In an HA configuration, if the secondary node takes over as the primary, does it switch back to secondary status if the original primary comes back online?

No. After the secondary node takes over as the primary, it remains as primary even if the original primary node comes back online again. To interchange the primary and secondary status of the nodes, run the *force failover* command.

What are the conditions for failure of the *force failover* command?

A forced failover fails in any of the following circumstances:

- You force failover on a standalone system.
- The secondary node is disabled.
- The secondary node is configured to remain secondary.
- The primary node is configured to remain primary.
- The state of the peer node is unknown.

Networking

The following topics provide a conceptual reference and instructions for configuring the various networking components on the NetScaler appliance.

IP Addressing	Learn the various types of NetScaler-owned IP addresses and how to create, customize, and remove them.
Interfaces	Configure some of the basic network configurations that must be done to get started.
Access Control Lists (ACLs)	Configure the different types of Access Control Lists and how to create, customize, and remove them.
IP Routing	Learn and configure the routing functionality of the NetScaler appliance, both static and dynamic.
Internet Protocol version 6 (IPv6)	Learn how the NetScaler appliance supports IPv6.
Traffic Domains	Learn and configure traffic domains to segment network traffic for different applications.

IP Addressing

Before you can configure the NetScaler appliance, you must assign the NetScaler IP Address (NSIP), also known as the Management IP address. You can also create other NetScaler-owned IP addresses for abstracting servers and establishing connections with the servers. In this type of configuration, the appliance serves as a proxy for the abstracted servers. You can also proxy connections by using network address translations (INAT and RNAT). When proxying connections, the appliance can behave either as a bridging (Layer 2) device or as a packet forwarding (Layer 3) device. To make packet forwarding more efficient, you can configure static ARP entries. For IPv6, you can configure neighbor discovery (ND).

Configuring NetScaler-Owned IP Addresses

The NetScaler-owned IP Addresses—NetScaler IP Address (NSIP), Virtual IP Addresses (VIPs), Subnet IP Addresses (SNIPs), Mapped IP Addresses (MIPs), and Global Server Load Balancing Site IP Addresses (GSLBIPs)—exist only on the NetScaler appliance. The NSIP uniquely identifies the NetScaler on your network, and it provides access to the appliance. A VIP is a public IP address to which a client sends requests. The NetScaler terminates the client connection at the VIP and initiates a connection with a server. This new connection uses a SNIP or a MIP as the source IP address for packets forwarded to the server. If you have multiple data centers that are geographically distributed, each data center can be identified by a unique GSLBIP.

You can configure some NetScaler-owned IP addresses to provide access for management applications.

Configuring the NetScaler IP Address (NSIP)

The NetScaler IP (NSIP) address is the IP address at which you access the NetScaler for management purposes. The NetScaler can have only one NSIP, which is also called the Management IP address. You must add this IP address when you configure the NetScaler for the first time. If you modify this address, you must reboot the NetScaler. You cannot remove an NSIP address. For security reasons, NSIP should be a non-routable IP address on your organization's LAN.

Note: Configuring the NetScaler IP address is mandatory.

To create the NetScaler IP address by using the command line interface

At the command prompt, type:

- set ns config [-IPAddress <ip_addr> -netmask <netmask>]
- show ns config

Example

```
> set ns config -ipaddress 10.102.29.170 -netmask 255.255.255.0
 Done
```

To configure the NetScaler IP address by using the configuration utility

1. In the navigation pane, click System.
2. On the System Information tab, click Setup Wizard.
3. In the Setup Wizard dialog box, click Next.
4. Under System Configuration, set the following parameters:
   - IP Address
   - Netmask
5. Follow the instructions in the Setup Wizard to complete the configuration.

Parameter Descriptions (of commands listed in the CLI procedure)

set ns config

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns config

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring and Managing Virtual IP (VIP) Addresses

Configuration of a virtual server IP (VIP) address is not mandatory during initial configuration of the NetScaler ADC. When you configure load balancing, you assign VIP addresses to virtual servers.

For more information about configuring a load balancing setup, see "Load Balancing."

In some situations, you need to customize VIP attributes or enable or disable a VIP address. A VIP address is usually associated with a virtual server, and some of the VIP attributes are customized to meet the requirements of the virtual server. You can host the same virtual server on multiple NetScaler appliances residing on the same broadcast domain, by using ARP and ICMP attributes. After you add a VIP (or any IP address), the NetScaler sends, and then responds to, ARP requests. VIPs are the only NetScaler-owned IP addresses that can be disabled. When a VIP address is disabled, the virtual server using it goes down and does not respond to ARP, ICMP, or L4 service requests.

As an alternative to creating VIP addresses one at a time, you can specify a consecutive range of VIP addresses.

To create a VIP address by using the command line interface

At the command prompt, type:

- add ns ip <IPAddress> <netmask> -type <type>
- show ns ip <IPAddress>

Example

```
> add ns ip 10.102.29.59 255.255.255.0 -type VIP
 Done
```

To create a range of VIP addresses by using the command line interface

At the command prompt, type:

- add ns ip <IPAddress> <netmask> -type <type>

- show ns ip <IPAddress>

Example

```
> add ns ip 10.102.29.[60-64] 255.255.255.0 -type VIP
ip "10.102.29.60" added
ip "10.102.29.61" added
ip "10.102.29.62" added
ip "10.102.29.63" added
ip "10.102.29.64" added
 Done
```

Parameters for configuring VIP addresses

ipAddress (IP Address)

Unique identification used to represent an entity. This is a required parameter.

netmask (Netmask)

Subnet mask associated with the IP address. This is a required parameter.

type (Type)

Type of the IP address. Specify **VIP**.

arp (ARP)

Use Address Resolution Protocol (ARP) to map IP addresses to the corresponding hardware addresses. Possible values: Enabled, Disabled. Default: Enabled.

icmpresponse (ICMP Response)

NetScaler sends ICMP responses to PING requests according to this value. The user network applications that use ICMP are PING and TRACEROUTE. This parameter can be set only if type is set as VIP. Possible values: NONE, ONE_VSERVER, ALL_VSERVERS, and VSVR_CNTRLD. Default value: NONE.

- When you select NONE, NetScaler always responds (even when the virtual server is DOWN).
- When you select ONE_VSERVER, NetScaler responds if at least one virtual server on this IP address is UP.
- When you select ALL_VSERVERS, NetScaler responds only if all the virtual servers on this IP address are UP.
- When you select VSVR_CNTRLD, the behavior depends on the ICMP VSERVER RESPONSE setting on the virtual server.

The following settings can be made on a virtual server:

- When you set ICMP VSERVER RESPONSE to PASSIVE on all virtual servers, NetScaler always responds.
- When you set ICMP VSERVER RESPONSE to ACTIVE on all virtual servers, NetScaler responds even if one virtual server is UP.
- When you set ICMP VSERVER RESPONSE to ACTIVE on some and PASSIVE on others, NetScaler responds even if one virtual server set to ACTIVE is UP.

arpresponse (ARP Response)

NetScaler appliance sends ARP responses according to this value. This parameter can be set only if type is set as VIP. Possible values: NONE, ONE_VSERVER. Default value: NONE.

- When you select NONE, NetScaler always responds (even when the virtual server is DOWN).
- When you select ONE_VSERVER, NetScaler responds if at least one virtual server on this IP address is UP.
- When you select ALL_VSERVERS, NetScaler responds only if all the virtual servers on this IP address are UP.

vServer (Virtual Server)

Apply the vserver attribute to this IP address. Possible values: Enabled, Disabled. Default: Enabled.

state (State)

State of the VIP. Possible values: Enabled, Disabled. Default: Enabled.

To configure a VIP address by using the configuration utility

Navigate to Network > IPs > IPV4s, and add a new IP address or edit an existing address.

To create a range of VIP addresses by using the configuration utility

1. Navigate to Network > IPs > IPV4s.
2. Click Add Range.

To enable or disable an IPv4 VIP address by using the command line interface

At the command prompt, type one of the following sets of commands to enable or disable a VIP and verify the configuration:

- enable ns ip <IPAddress>
- show ns ip <IPAddress>
- disable ns ip <IPAddress>
- show ns ip <IPAddress>

Example

```
> enable ns ip 10.102.29.79
 Done
> show ns ip 10.102.29.79

        IP: 10.102.29.79
        Netmask: 255.255.255.255
        Type: VIP
        state: Enabled
        arp: Enabled
        icmp: Enabled
        vserver: Enabled
        management access: Disabled
          telnet: Disabled
          ftp: Disabled
          ssh: Disabled
          gui: Disabled
          snmp: Disabled
        Restrict access: Disabled
        dynamic routing: Disabled
        hostroute: Disabled
 Done
> disable ns ip 10.102.29.79
 Done
> show ns ip 10.102.29.79

        IP: 10.102.29.79
        Netmask: 255.255.255.255
        Type: VIP
        state: Disabled
        arp: Enabled
        icmp: Enabled
        vserver: Enabled
        management access: Disabled
          telnet: Disabled
          ftp: Disabled
          ssh: Disabled
          gui: Disabled
          snmp: Disabled
        Restrict access: Disabled
        dynamic routing: Disabled
        hostroute: Disabled

 Done
```

To enable or disable a VIP address by using the configuration utility

1. Navigate to Network > IPs > IPV4s.
2. Select the VIP address, and click Enable or Disable.

Configuring ARP response Suppression for Virtual IP addresses (VIPs)

You can configure the NetScaler appliance to respond or not respond to ARP requests for a Virtual IP (VIP) address on the basis of the state of the virtual servers associated with that VIP.

For example, if virtual servers V1, of type HTTP, and V2, of type HTTPs, share VIP address 10.102.29.45 on a NetScaler appliance, you can configure the appliance to not respond to any ARP request for VIP 10.102.29.45 if both V1 and V2 are in the DOWN state.

The following three options are available for configuring ARP-response suppression for a virtual IP address.

- **NONE**. The NetScaler appliance responds to any ARP request for the VIP address, irrespective of the state of the virtual servers associated with the address.
- **ONE VSERVER**. The NetScaler appliance responds to any ARP request for the VIP address if at least one of the associated virtual servers is in UP state.
- **ALL VSERVER**. The NetScaler appliance responds to any ARP request for the VIP address if all of the associated virtual servers are in UP state.

Following table shows the sample behavior of NetScaler appliance for a VIP configured with two virtual servers:

Associated virtual servers for a VIP	**STATE 1**	**STATE 2**	**STATE 3**	**STATE 4**
NONE				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN
Respond to an ARP request for this VIP?	Yes	Yes	Yes	Yes
ONE VSERVER				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN
Respond to an ARP request for this VIP?	Yes	Yes	Yes	No
ALL VSERVER				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN

Respond to an ARP request for this VIP?	Yes	No	No	No

Consider an example where you want to test the performance of two virtual servers, V1 and V2, which have the same VIP address but are of different types and are each configured on NetScaler appliances NS1 and NS2. Let's call the shared VIP address *VIP1*.

V1 load balances servers S1, S2, and S3. V2 load balances servers S4 and S5.

On both NS1 and NS2, for VIP1, the ARP suppression parameter is set to ALL_VSERVER. If you want to test the performance of V1 and V2 on NS1, you must manually disable V1 and V2 on NS2, so that NS2 does not respond to any ARP request for VIP1.

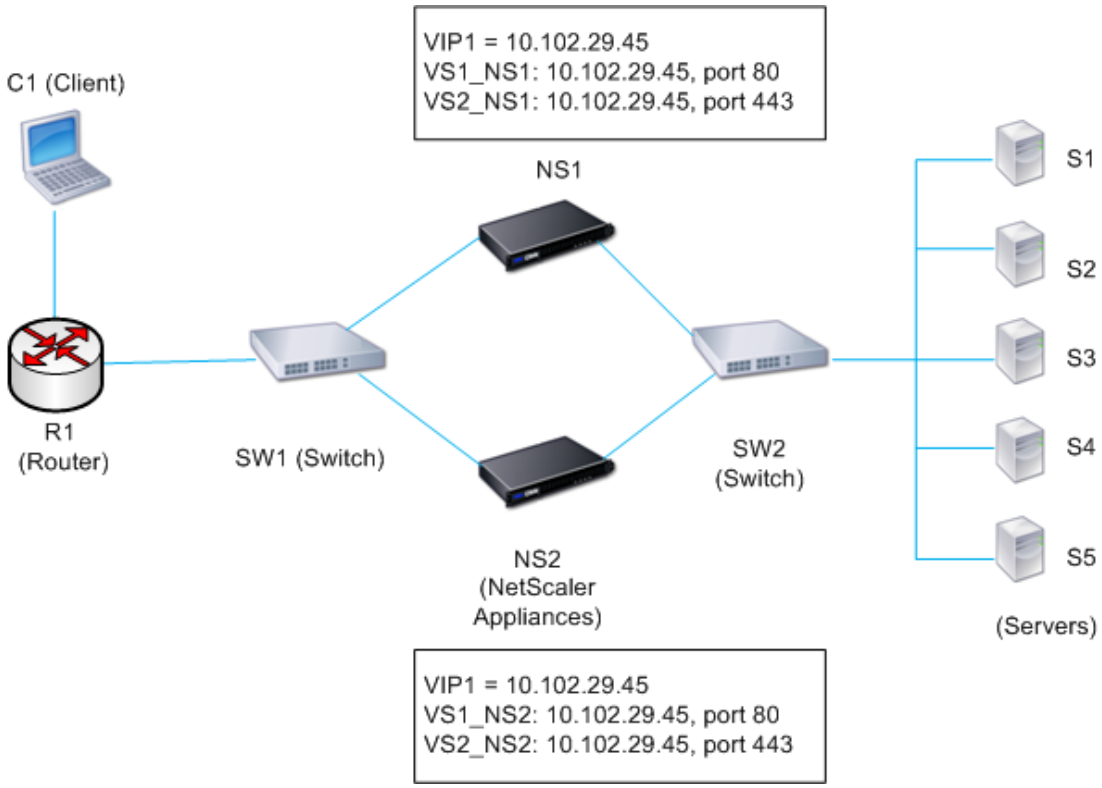


Figure 1.

The execution flow is as follows:

1. Client C1 sends a request to V1. The request reaches R1.
2. R1 does not have an APR entry for the IP address (VIP1) of V1, so R1 broadcasts an ARP request for VIP1.
3. NS1 replies with source MAC address MAC1 and source IP address VIP1. NS2 does not reply to the ARP request.
4. SW1 learns the port for VIP1 from the ARP reply and updates its bridge table, and R1 updates the ARP entry with MAC1 and VIP1.
5. R1 forwards the packet to address VIP1 on NS1.

6. NS1's load balancing algorithm selects server S2, and NS1 opens a connection between one of its SNIP or MIP addresses and S2. When S2 sends a response to the client, the response returns by the same path.

7. Now you want to test the performance of V1 and V2 on NS2, so you enable V1 and V2 on NS2 and disable them on NS1. NS2 now broadcasts an ARP message for VIP1. In the message, MAC2 is the source MAC address and VIP1 is the source IP address.

8. SW1 learns the port number for reaching MAC2 from the ARP broadcast and updates its bridge table to send subsequent client requests for VIP1 to NS2. R1 updates its ARP table.

9. Now suppose the ARP entry for VIP1 times out in the ARP table of R1, and client C1 sends a request for V1. Because R1 does not have an APR entry for VIP1, it broadcasts an ARP request for VIP1.

10. NS2 replies with a source MAC address and VIP1 as the source IP address. NS1 does not reply to the ARP request.

To configure ARP response suppression by using the command line interface

At the command prompt, type:

- set ns ip -arpResponse <arpResponse>]
- show ns ip <IPAddress>

Example

```
> set ns ip 10.102.29.96 -arpResponse ALL_VSERVERS
 Done
```

To configure ARP response suppression by using the configuration utility

1. Navigate to Network > IPs > IPV4s.

2. Open an IP address entry and select the type of ARP Response.

Parameter Descriptions (of commands listed in the CLI procedure)

set ns ip

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns ip

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Subnet IP Addresses (SNIPs)

A subnet IP address (SNIP) is a NetScaler owned IP address that is used by the NetScaler ADC to communicate with the servers.

The NetScaler ADC uses the subnet IP address as a source IP address to proxy client connections to servers. It also uses the subnet IP address when generating its own packets, such as packets related to dynamic routing protocols, or to send monitor probes to check the health of the servers.

Depending on your network topology, you might have to configure one or more SNIPs for different scenarios. Following are three typical scenarios in which you have to configure SNIPs:

- Using SNIPs for a Directly Connected Server Subnet
- Using SNIPs for Server Subnets Connected through a Router
- Using SNIPs for Multiple Server Subnets (VLANs) on an L2 Switch

To configure a SNIP address on a NetScaler ADC, you add the SNIP address and then enable global Use Subnet IP (USNIP) mode.

As an alternative to creating SNIPs one at a time, you can specify a consecutive range of SNIPs.

To configure a SNIP address by using the command line interface

At the command prompt, type:

- add ns ip <IPAddress> <netmask> -type SNIP
- show ns ip <IPAddress>

Example

```
> add ns ip 10.102.29.203 255.255.255.0 -type SNIP
 Done
```

To create a range of SNIP addresses by using the command line interface

At the command prompt, type:

- add ns ip <IPAddress> <netmask> -type SNIP
- show ns ip <IPAddress>

Example

```
> add ns ip 10.102.29.[205-209] 255.255.255.0 -type SNIP
ip "10.102.29.205" added
ip "10.102.29.206" added
ip "10.102.29.207" added
ip "10.102.29.208" added
ip "10.102.29.209" added
 Done
```

To enable or disable USNIP mode by using the command line interface

At the command prompt, type one of the following commands:

- enable ns modeUSNIP
- disable ns modeUSNIP

To configure a SNIP address by using the configuration utility

Navigate to Network > IPs > IPV4s, and add a new SNIP address or edit an existing address.

To create a range of SNIP addresses by using the configuration utility

1. Navigate to Network > IPs > IPV4s.
2. Click Add Range.

To enable or disable USNIP mode by using the command line interface

At the command prompt, type one of the following commands:

- enable ns mode `USNIP`
- disable ns mode `USNIP`

To enable or disable USNIP mode by using the configuration utility

1. Navigate to System > Settings, in Modes and Features group, click Change modes.
2. Select or clear the Use Subnet IP option.

Parameter Descriptions (of commands listed in the CLI procedure)

add ns ip

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns ip

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

enable ns mode

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable ns mode

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Using SNIPs for a Directly Connected Server Subnet

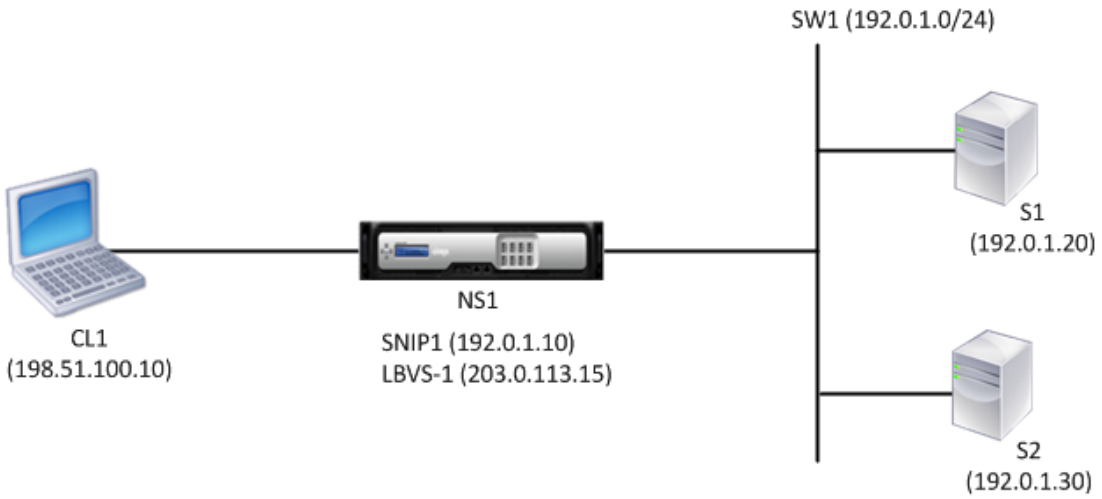
To enable communication between the NetScaler and a server that is either connected directly to the NetScaler or connected through only an L2 switch, you must configure a subnet IP address that belongs to the subnet of the server. You must configure at least one subnet IP address for each directly connected subnet, except for the directly connected management subnet that is connected through NSIP.

Consider an example of a load balancing setup in which load balancing virtual server LBVS1 on NetScaler ADC NS1 is used to load balance servers S1 and S2, which are connected to NS1 through L2 switch SW1. S1 and S2 belong to the same subnet.

SNIP address SNIP1, which belongs to the same subnet as S1 and S2, is configured on NS1. As soon as SNIP1 is configured, NS1 broadcasts ARP packets for SNIP1.

Services SVC-S1 and SVC-S2 on NS1 represent S1 and S2. As soon as these services are configured, NS1 broadcasts ARP requests for S1 and S2 to resolve IP-to-MAC mapping. After S1 and S2 respond, NS1 sends them monitoring probes at regular intervals, from address SNIP1, to check their health.

For more information about configuring load balancing on a NetScaler ADC, see Load Balancing.



Following is the traffic flow in this example:

1. Client C1 sends a request packet to LBVS-1. The request packet has:
    - Source IP = IP address of the client (198.51.100.10)
    - Destination IP = IP address of LBVS-1 (203.0.113.15)
2. LBVS1 of NS1 receives the request packet.

3. LBVS1's load balancing algorithm selects server S2.

4. Because S2 is directly connected to NS1, and SNIP1 (192.0.1.10) is the only IP address on NS1 that belongs to the same subnet as S2, NS1 opens a connection between SNIP1 and S2.

5. NS1 sends the request packet to S2 from SNIP1. The request packet has:

   - Source IP = SNIP1 (192.0.1.10)

   - Destination IP = IP address of S2 (192.0.1.30)
6. S2’s response returns by the same path.

Using SNIPs for Server Subnets Connected through a Router

To enable communication between the NetScaler ADC and servers in subnets connected through a router, you must configure at least one subnet IP address that belongs to the subnet of the directly connected interface to the router. The ADC uses this subnet IP address to communicate with servers in subnets that can be reached through the router.

Consider an example of a load balancing setup in which load balancing virtual server LBVS1 on NetScaler ADC NS1 is used to load balance servers S1, S2, S3, and S4, which are connected to NS1 through router R1.

S1 and S2 belong to same subnet, 192.0.2.0/24, and are connected to R1 through L2 switch SW1. S3 and S4 belong to a different subnet, 192.0.3.0/24, and are connected to R1 through L2 switch SW2.

NetScaler ADC NS1 is connected to router R1 through subnet 192.0.1.0/24. SNIP address SNIP1, which belongs to the same subnet as the directly connected interface to the router (192.0.1.0/24), is configured on NS1. NS1 uses this address to communicate with servers S1 and S2, and with servers S3 and S4.

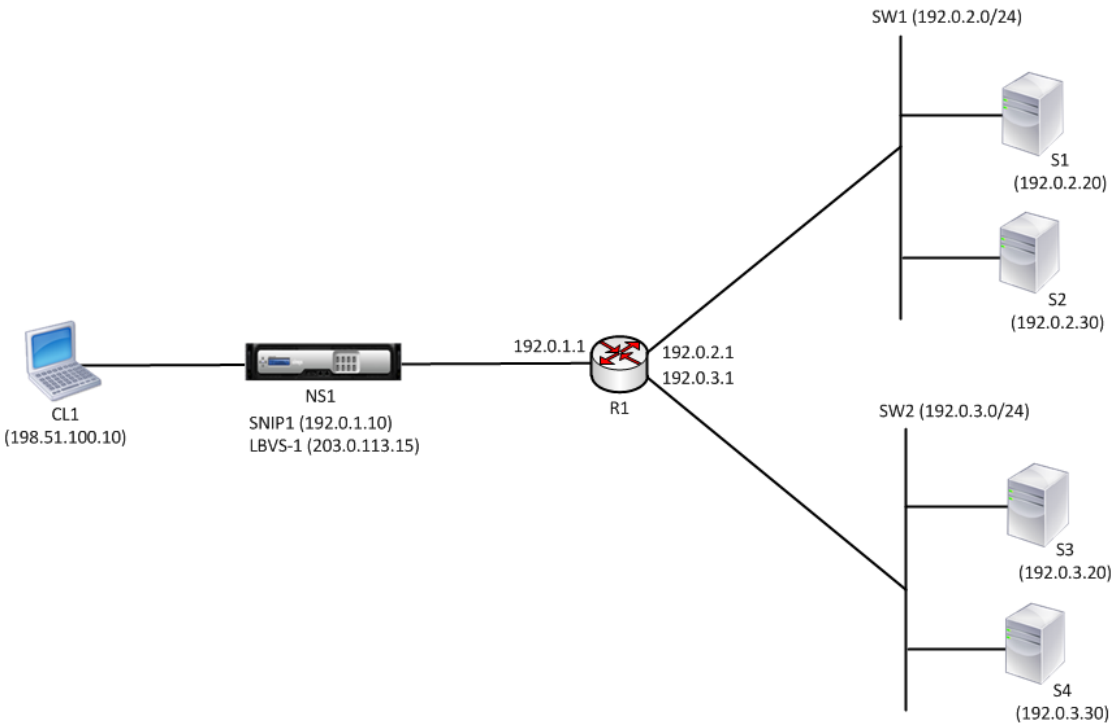
For more information about configuring load balancing on a NetScaler ADC, see Load Balancing.

As soon as address SNIP1 is configured, NS1 broadcasts ARP announcement packets for SNIP1.

NS1's routing table consists of route entries for S1, S2, S3, and S4 through R1. These route entries are either static route entries or advertised by R1 to NS1, using dynamic routing protocols.

Services SVC-S1, SVC-S2, SVC-S3, and SVC-S4 on NS1 represent servers S1, S2, S3, and S4. NS1 finds, in its routing tables, that these servers are reachable through R1. NS1 sends them monitoring probes at regular intervals, from address SNIP1, to check their health.

For more information about IP routing on a NetScaler ADC, see IP Routing.



Following is the traffic flow in this example:

1. Client C1 sends a request packet to LBVS-1. The request packet has:
   - Source IP = IP address of the client (198.51.100.10)
   - Destination IP = IP address of LBVS-1 (203.0.113.15)
2. LBVS1 of NS1 receives the request packet.
3. LBVS1's load balancing algorithm selects server S3.
4. NS1 checks its routing table and finds that S3 is reachable through R1. SNIP1 (192.0.1.10) is the only IP address on NS1 that belongs to the same subnet as router R1, NS1 opens a connection between SNIP1 and S3 through R1.
5. NS1 sends the request packet to R1 from SNIP1. The request packet has:
   - Source IP address = SNIP1 (192.0.1.10)
   - Destination IP address = IP address of S3 (192.0.3.20)
6. The request reaches R1, which checks its routing table and forwards the request packet to S3.
7. S3’s response returns by the same path.

Using SNIPs for Multiple Server Subnets (VLANs) on an L2 Switch

When you have multiple server subnets (VLANs) on an L2 switch that is connected to a NetScaler ADC, you must configure at least one SNIP address for each of the server subnets, so that the NetScaler ADC can communicate with these server subnets.

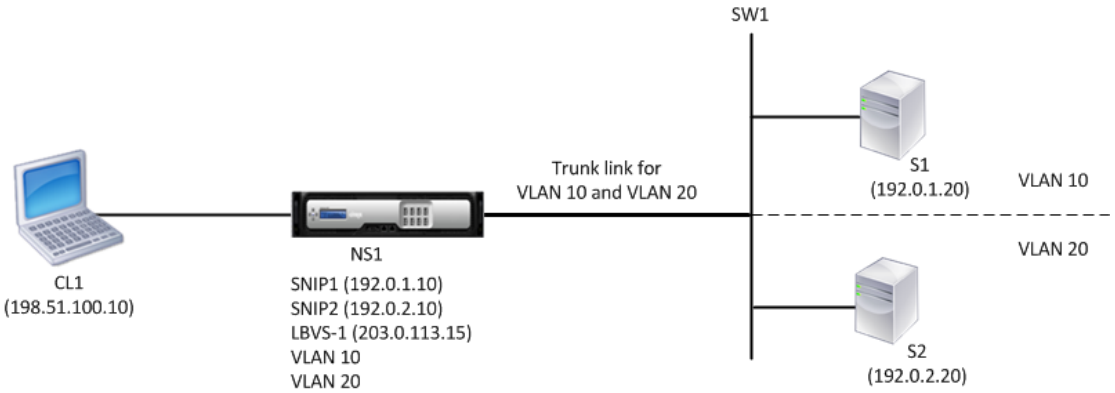
Consider an example of a load balancing setup in which load balancing virtual server LBVS1 on NetScaler ADC NS1 is used to load balance servers S1 and S2, which are connected to NS1 through L2 switch SW1. S1 and S2 belong to different subnets and are part of VLAN 10 and VLAN20, respectively. The link between NS1 and SW1 is a trunk link and is shared by VLAN10 and VLAN20.

For more information about configuring load balancing on a NetScaler ADC, see Load Balancing.

Subnet IP addresses SNIP1 (for reference purposes only) and SNIP2 (for reference purposes only) are configured on NS1. NS1 uses SNIP1 (on VLAN 10) to communicate with server S1, and SNIP2 (on VLAN 20) to communicate with S2. As soon as SNIP1 and SNIP2 are configured, NS1 broadcasts ARP announcement packets for SNIP1 and SNIP2.

For more information about configuring VLANs on a NetScaler ADC, see Configuring VLANs.

Services SVC-S1 and SVC-S2 on NS1 represent servers S1 and S2. As soon as these services are configured, NS1 broadcasts ARP requests for them. After S1 and S2 respond, NS1 sends them monitoring probes at regular intervals to check their health. NS1 sends monitoring probes to S1 from address SNIP1, and to S2 from address SNIP2.



Following is the traffic flow in this example:

1. Client C1 sends a request packet to LBVS-1. The request packet has:
    - Source IP = IP address of the client (198.51.100.10)
    - Destination IP = IP address of LBVS-1 (203.0.113.15)
2. LBVS1 of NS1 receives the request packet.

3. LBVS1's load balancing algorithm selects server S2.

4. Because S2 is directly connected to NS1, and SNIP2 (192.0.2.10) is the only IP address on NS1 that belongs to the same subnet as S2, NS1 opens a connection between SNIP2 and S2.

   Note: If S1 is selected, NS1 opens a connection between SNIP1 and S1.

5. NS1 sends the request packet to S2 from SNIP2. The request packet has:

   - Source IP = SNIP1 (192.0.2.10)

   - Destination IP = IP address of S2 (192.0.2.20)
6. S2’s response returns by the same path.

Configuring Mapped IP Addresses (MIPs)

Mapped IP addresses (MIP) are used for server-side connections. A MIP can be considered a default Subnet IP (SNIP) address, because MIPs are used when a SNIP is not available or Use SNIP (USNIP) mode is disabled.

If the mapped IP address is the first in the subnet, the NetScaler appliance adds a route entry, with this IP address as the gateway to reach the subnet. You can create or delete a MIP during run time without rebooting the appliance.

As an alternative to creating MIPs one at a time, you can specify a consecutive range of MIPs.

The following diagram shows the use of the MIP and SNIP addresses in a NetScaler appliance that connects to the backend servers across the subnets.

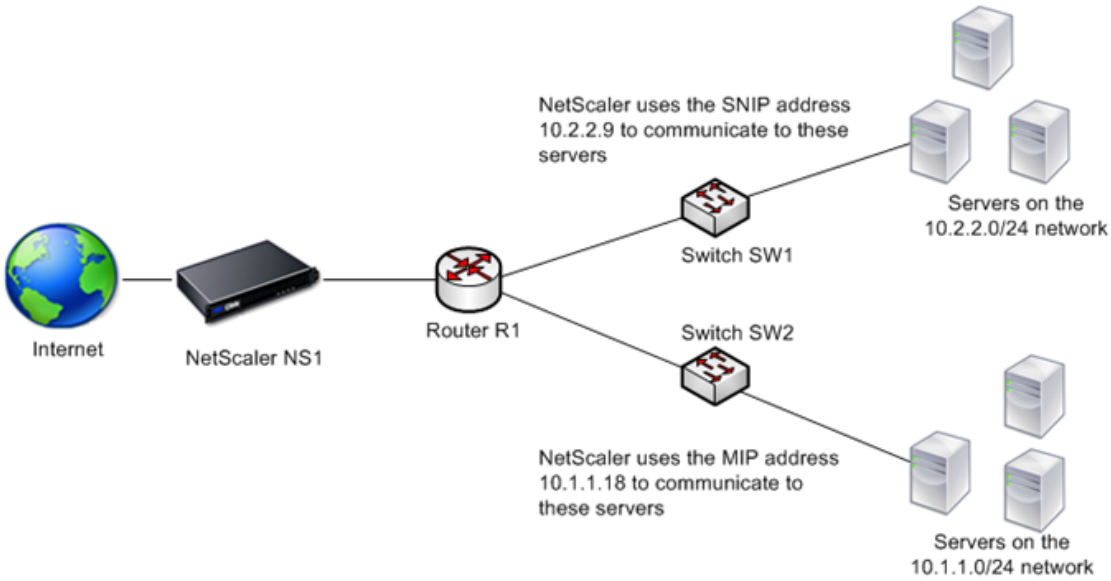


Figure 1. MIP and SNIP addresses

In the setup, if the NetScaler appliance and the backend servers are in the 10.1.1.0/24 subnet, then the appliance uses the MIP address to communicate to the servers. However, if the setup has backend servers on additional subnets, such as 10.2.2.0/24, and there is no router between the NetScaler appliance and the subnet, then you can configure a SNIP address that has a range of 10.2.2.x/24, such as 10.2.2.9 in this case, to communicate to the additional subnet.

You can enable to NetScaler appliance to use MIP to communicate the additional subnet. However, if the setup has a Firewall application between the appliance and the server, then the Firewall might prevent the traffic other than 10.2.2.0/24. In such cases, you need a SNIP address to communicate to the servers.

To create a MIP address by using the command line interface

At the command prompt, type:

- add ns ip <IPAddress> <netmask> -type <type>
- show ns ip <IPAddress>

Example

```
> add ns ip 10.102.29.171 255.255.255.0 -type MIP
 Done
```

To create a range of MIP addresses by using the command line interface

At the command prompt, type:

- add ns ip <IPAddress> <netmask> -type <type>
- show ns ip <IPAddress>

Example

```
> add ns ip 10.102.29.[173-175] 255.255.255.0 -type MIP
ip "10.102.29.173" added
ip "10.102.29.174" added
ip "10.102.29.175" added
Done
```

To configure a MIP address by using the configuration utility

Navigate to Network > IPs > IPV4s, and add a new MIP address or edit an existing address.

To create a range of MIP addresses by using the configuration utility

1. Navigate to Network > IPs > IPV4s.
2. Click Add Range.

Parameter Descriptions (of commands listed in the CLI procedure)

add ns ip

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns ip

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring GSLB Site IP Addresses (GSLBIP)

A GSLB site IP (GSLBIP) address is an IP address associated with a GSLB site. It is not mandatory to specify a GSLBIP address when you initially configure the NetScaler appliance. A GSLBIP address is used only when you create a GSLB site.

For more information about creating a GSLB site IP address, see "Global Server Load Balancing."

Removing a NetScaler-Owned IP Address

You can remove any IP address except the NSIP. The following table provides information about the processes you must follow to remove the various types of IP addresses. Before removing a VIP, remove the associated virtual server.

Table 1. Implications of Removing a NetScaler-Owned IP Address

IP address type	Implications
Subnet IP address (SNIP)	If IP address being removed is the last IP address in the subnet, the associated route is deleted from the route table. If the IP address being removed is the gateway in the corresponding route entry, the gateway for that subnet route is changed to another NetScaler-owned IP address.
Mapped IP address (MIP)	If a SNIP exists, you can remove the MIPs. The NetScaler uses NSIP and SNIPs to communicate with the servers when the MIP is removed. Therefore, you must also enable use SNIP (USNIP) mode. For information about enabling and disabling USNIP mode, see "Configuring Subnet IP Addresses (SNIPs)."
Virtual Server IP address (VIP)	Before removing a VIP, you must first remove the vserver associated with it. For information about removing the vserver, see "Load Balancing."
GSLB-Site-IP address	Before removing a GSLB site IP address, you must remove the site associated with it. For information about removing the site, see "Global Server Load Balancing."

To remove an IP address by using the command line interface

At the command prompt, type:

rm ns ip <IPaddress>

Example

```
rm ns ip 10.102.29.54
```

To remove an IP address by using the configuration utility

Navigate to Network > IPs > IPV4s, delete the IP address.

Configuring Application Access Controls

Application access controls, also known as management access controls, form a unified mechanism for managing user authentication and implementing rules that determine user access to applications and data. You can configure MIPs and SNIPs to provide access for management applications. Management access for the NSIP is enabled by default and cannot be disabled. You can, however, control it by using ACLs.

For information about using ACLs, see "Access Control Lists (ACLs)."

The NetScaler appliance does not support management access to VIPs.

The following table provides a summary of the interaction between management access and specific service settings for Telnet.

Management Access	Telnet (State Configured on the NetScaler)	Telnet (Effective State at the IP Level)
Enable	Enable	Enable
Enable	Disable	Disable
Disable	Enable	Disable
Disable	Disable	Disable

The following table provides an overview of the IP addresses used as source IP addresses in outbound traffic.

Application/ IP	NSIP	MIP	SNIP	VIP
ARP	Yes	Yes	Yes	No
Server side traffic	No	Yes	Yes	No
RNAT	No	Yes	Yes	Yes
ICMP PING	Yes	Yes	Yes	No
Dynamic routing	Yes	No	Yes	Yes

The following table provides an overview of the applications available on these IP addresses.

Application/ IP	NSIP	MIP	SNIP	VIP
SNMP	Yes	Yes	Yes	No
System access	Yes	Yes	Yes	No

You can access and manage the NetScaler by using applications such as Telnet, SSH, GUI, and FTP.

Note: Telnet and FTP are disabled on the NetScaler for security reasons. To enable them, contact the customer support. After the applications are enabled, you can apply the controls at the IP level.

To configure the NetScaler to respond to these applications, you need to enable the specific management applications. If you disable management access for an IP address, existing connections that use the IP address are not terminated, but no new connections can be initiated.

Also, the non-management applications running on the underlying FreeBSD operating system are open to protocol attacks, and these applications do not take advantage of the NetScaler appliance's attack prevention capabilities.

You can block access to these non-management applications on a MIP, SNIP, or NSIP. When access is blocked, a user connecting to a NetScaler by using the MIP, SNIP, or NSIP is not be able to access the non-management applications running on the underlying operating system.

To configure management access for an IP address by using the command line interface

At the command prompt, type:

set ns ip <IPAddress> -mgmtAccess <value> -telnet <value> -ftp <value> -gui <value> -ssh <value> -snmp <value> -restrictAccess (ENABLED | DISABLED)

Example

```
> set ns ip 10.102.29.54 -mgmtAccess enabled -restrictAccess ENABLED
 Done
```

To enable management access for an IP address by using the configuration utility

1. Navigate to Network > IPs > IPV4s.
2. Open an IP address entry, and select the Enable Management Access control to support the below listed applications option.

Parameter Descriptions (of commands listed in the CLI procedure)

set ns ip

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

How the NetScaler Proxies Connections

When a client initiates a connection, the NetScaler appliance terminates the client connection, initiates a connection to an appropriate server, and sends the packet to the server. The appliance does not perform this action for service type UDP or ANY.

For more information about service types, see "Load Balancing."

You can configure the NetScaler to process the packet before initiating the connection with a server. The default behavior is to change the source and destination IP addresses of a packet before sending the packet to the server. You can configure the NetScaler to retain the source IP address of the packets by enabling Use Source IP mode.

How the Destination IP Address Is Selected

Traffic sent to the NetScaler appliance can be sent to a virtual server or to a service. The appliance handles traffic to virtual servers and services differently. The NetScaler terminates traffic received at a virtual server IP (VIP) address and changes the destination IP address to the IP address of the server before forwarding the traffic to the server, as shown in the following diagram.

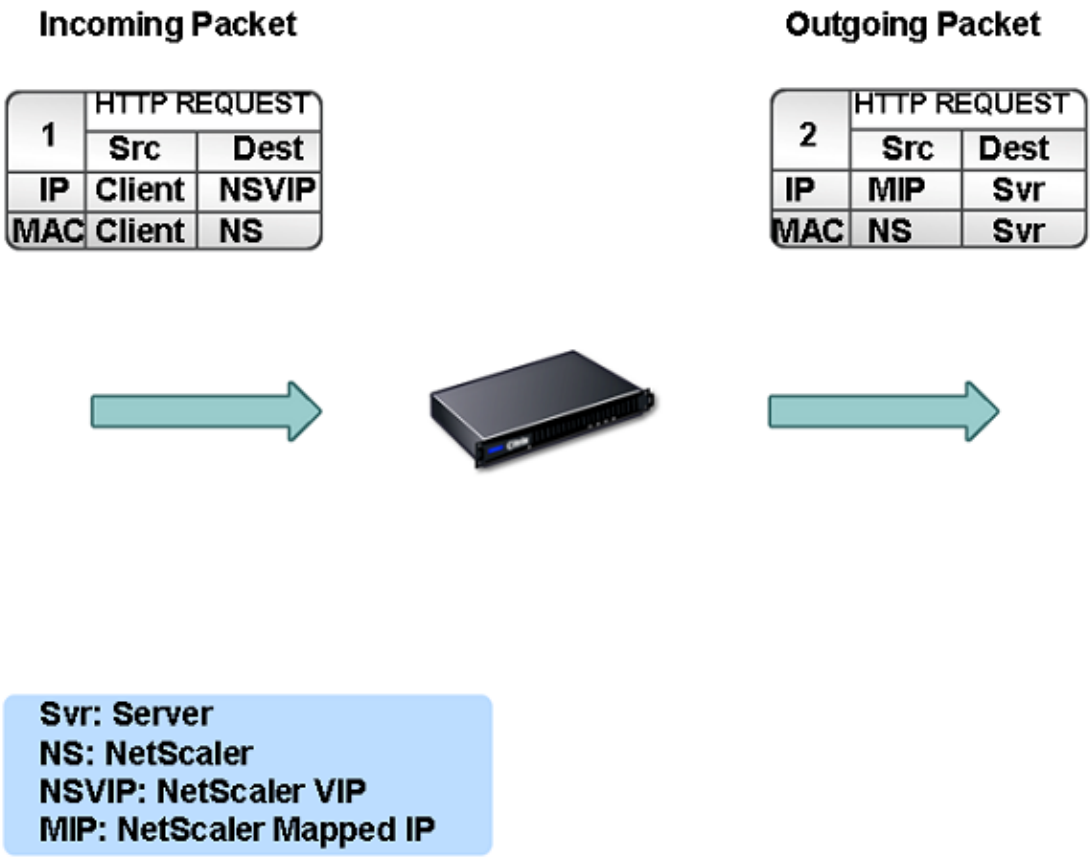


Figure 1. Proxying Connections to VIPs

Packets destined for a service are sent directly to the appropriate server, and the NetScaler does not modify the destination IP addresses. In this case, the NetScaler functions as a proxy.

How the Source IP Address Is Selected

When the NetScaler appliance communicates with the physical servers or peer devices, by default, it does not use the IP address of the client. NetScaler maintains a pool of mapped IP addresses (MIPs) and subnet IP addresses (SNIPs), and selects an IP address from this pool to use as the source IP address of a connection to the physical server. Depending on the subnet in which the physical server is placed, NetScaler decides whether a MIP should be used or SNIP.

Note: If the Use Source IP (USIP) option is enabled, NetScaler uses the IP address of the client.

Enabling Use Source IP Mode

When the NetScaler appliance communicates with the physical servers or peer devices, by default, it uses one of its own IP addresses as the source IP. The appliance maintains a pool of mapped IP addresses (MIPs) and subnet IP addresses (SNIPs), and selects an IP address from this pool to use as the source IP address for a connection to the physical server. The decision of whether to select a MIP or a SNIP depends on the subnet in which the physical server resides.

If necessary, you can configure the NetScaler appliance to use the client's IP address as source IP. Some applications need the actual IP address of the client. The following use cases are a few examples:

- Client's IP address in the web access log is used for billing purposes or usage analysis.
- Client's IP address is used to determine the country of origin of the client or the originating ISP of the client. For example, many search engines such as Goggle provide content relevant to the location to which the user belongs.
- The application must know the client's IP address to verify that the request is from a trustworthy source.
- Sometimes, even though an application server does not need the client's IP address, a firewall placed between the application server and the NetScaler may need the client's IP address for filtering the traffic.

Enable Use Source IP mode (USIP) mode if you want NetScaler to use the client's IP address for communication with the servers. By default, USIP mode is disabled. USIP mode can be enabled globally on the NetScaler or on a specific service. If you enable it globally, USIP is enabled by default for all subsequently created services. If you enable USIP for a specific service, the client's IP address is used only for the traffic directed to that service.

As an alternative to USIP mode, you have the option of inserting the client's IP address (CIP) in the request header of the server-side connection for an application server that needs the client's IP address.

In earlier NetScaler releases, USIP mode had the following source-port options for server-side connections:

- Use the client's port. With this option, connections cannot be reused. For every request from the client, a new connection is made with the physical server.
- Use proxy port. With this option, connection reuse is possible for all requests from the same client. Before NetScaler release 8.1 this option imposed a limit of 64000 concurrent connections for all server-side connections.

In the later NetScaler releases , if USIP is enabled, the default is to use a proxy port for server-side connections and not reuse connections. Not reusing connections may not affect the speed of establishing connections.

By default, the Use Proxy Port option is enabled if the USIP mode is enabled.

For more information about the Use Proxy Port option, see "Using the Client Port When Connecting to the Server."

Note: If you enable the USIP mode, it is recommended to enable the Use Proxy Port option.

The following figure shows how the NetScaler uses IP addresses in USIP mode.

Figure 1. IP Addressing in USIP Mode

Recommended Usage

Enable USIP in the following situations:

- Load balancing of Intrusion Detection System (IDS) servers
- SMTP load balancing
- Stateless connection failover
- Sessionless load balancing
- If you use the Direct Server Return (DSR) mode

Note: When USIP is required in the one-arm mode installation of the NetScaler appliance, make sure that the server's gateway is one of the IP addresses owned by the NetScaler. For more information about NetScaler owned IP addresses, see "Configuring NetScaler owned IP addresses."

- If you enable USIP, set the idle timeout for server connections to a value lower than the default value, so that idle connections are cleared quickly on the server side.

  For more information about setting an idle time-out value, "Load Balancing."

- For transparent cache redirection, if you enable USIP, enable L2CONN also.
- Because HTTP connections are not reused when USIP is enabled, a large number of server-side connections may accumulate. Idle server connections can block connections for other clients. Therefore, set limits on maximum number of connections to a service. Citrix also recommends setting the HTTP server time-out value, for a service on which

USIP is enabled, to a value lower than the default, so that idle connections are cleared quickly on the server side.

To globally enable or disable USIP mode by using the command line interface

At the command prompt, type one of the following commands:

- enable ns mode USIP
- disable ns mode USIP

To enable USIP mode for a service by using the command line interface

At the command prompt, type:

set service <name>@ -usip (**YES** | **NO**)

Example

set service Service-HTTP-1 -usip YES

To globally enable or disable USIP mode by using the configuration utility

1. Navigate to System > Settings, in Modes and Features group, click Change modes.
2. Select or clear the Use Source IP option.

To enable USIP mode for a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to enable the USIP mode, and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Under Settings, select the Use Source IP check box.
5. Click OK.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns mode

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable ns mode

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

set service

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Network Address Translation

Network address translation (NAT) involves modification of the source and/or destination IP addresses and/or the TCP/UDP port numbers of IP packets that pass through the NetScaler appliance. Enabling NAT on the appliance enhances the security of your private network, and protects it from a public network such as the Internet, by modifying your networks source IP addresses when data passes through the NetScaler. Also, with the help of NAT entries, your entire private network can be represented by a few shared public IP addresses. The NetScaler supports the following types of network address translation:

- Inbound NAT (INAT), in which the NetScaler replaces the destination IP address in the packets generated by the client with the private IP address of the server.
- Reverse NAT (RNAT), in which the NetScaler replaces the source IP address in the packets generated by the servers with the public NAT IP addresses.

Configuring INAT

When a client sends a packet to a NetScaler appliance that is configured for Inbound Network Address Translation (INAT), the appliance translates the packet's public destination IP address to a private destination IP address and forwards the packet to the server at that address.

The following configurations are supported:

- **IPv4-IPv4 Mapping**: A public IPv4 address on the NetScaler appliance listens to connection requests on behalf of a private IPv4 server. The NetScaler appliance translates the packet's public destination IP address to the destination IP address of the server and forwards the packet to the server at that address.
- **IPv4-IPv6 Mapping**: A public IPv4 address on the NetScaler appliance listens to connection requests on behalf of a private IPv6 server. The NetScaler appliance creates an IPv6 request packet with the IP address of the IPv6 server as the destination IP address.
- **IPv6-IPv4 Mapping**: A public IPv6 address on the NetScaler appliance listens to connection requests on behalf of a private IPv4 server. The NetScaler appliance creates an IPv4 request packet with the IP address of the IPv4 server as the destination IP address.
- **IPv6-IPv6 Mapping**: A public IPv6 address on the NetScaler appliance listens to connection requests on behalf of a private IPv6 server. The NetScaler appliance translates the packet's public destination IP address to the destination IP address of the server and forwards the packet to the server at that address.

When the appliance forwards a packet to a server, the source IP address assigned to the packet is determined as follows:

- If use subnet IP (USNIP) mode is enabled and use source IP (USIP) mode is disabled, the NetScaler uses a subnet IP address (SNIP) as the source IP address.
- If USNIP mode is disabled and USIP mode is disabled, the NetScaler uses a mapped IP address (MIP) as the source IP address.
- If USIP mode is enabled, and USNIP mode is disabled the NetScaler uses the client IP (CIP) address as the source IP address.
- If both USIP and USNIP modes are enabled, USIP mode takes precedence.
- You can also configure the NetScaler to use a unique IP address as the source IP address, by setting the proxyIP parameter.
- If none of the above modes are enabled and a unique IP address has not been specified, the NetScaler attempts to use a MIP as the source IP address.
- If both USIP and USNIP modes are enabled and a unique IP address has been specified, the order of precedence is as follows: USIP-unique IP-USNIP-MIP-Error.

To protect the NetScaler from DoS attacks, you can enable TCP proxy. However, if other protection mechanisms are used in your network, you may want to disable them.

You can create, modify, or remove an INAT entry.

To create an INAT entry by using the command line interface

At the command prompt, type the following commands to create an INAT entry and verify its configuration:

- add inat <name> <publicIP> <privateIP> [-tcpproxy (ENABLED | DISABLED)] [-ftp (ENABLED | DISABLED)] [-usip (ON | OFF)] [-usnip (ON | OFF)] [-proxyIP <ip_addr|ipv6_addr>]
- show inat [<name>]

Example

```
> add inat ip4-ip4 172.16.1.2 192.168.1.1 -proxyip 10.102.29.171
 Done
```

To modify an INAT entry by using the command line interface

To modify an INAT entry, type the set inat command, the name of the entry, and the parameters to be changed, with their new values.

To remove an INAT configuration by using the command line interface

At the command prompt, type:

rm inat <name>

Example

```
> rm inat ip4-ip4
 Done
```

To configure an INAT entry by using the configuration utility

Navigate to Network > Routes > INAT, and add a new INAT entry or edit an existing INAT entry.

To remove an INAT configuration by using the configuration utility

Navigate to Network > Routes > INAT, delete the INAT configuration.

Parameter Descriptions (of commands listed in the CLI procedure)

add inat

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show inat

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

rm inat

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Coexistence of INAT and Virtual Servers

If both INAT and RNAT are configured, the INAT rule takes precedence over the RNAT rule. If RNAT is configured with a network address translation IP (NAT IP) address, the NAT IP address is selected as the source IP address for that RNAT client.

The default public destination IP in an INAT configuration is the virtual IP (VIP) address of the NetScaler device. Virtual servers also use VIPs. When both INAT and a virtual server use the same IP address, the Vserver configuration overrides the INAT configuration.

Following are a few sample configuration setup scenarios and their effects.

Case	Result
You have configured a virtual server and a service to send all data packets received on a specific NetScaler port to the server directly. You have also configured INAT and enabled TCP. Configuring INAT in this manner sends all data packets received through a TCP engine before sending them to the server.	All packets received on the NetScaler, except those received on the specified port, pass through the TCP engine.
You have configured a virtual server and a service to send all data packets of service type TCP, that are received on a specific port on the NetScaler, to the server after passing through the TCP engine. You have also configured INAT and disabled TCP. Configuring INAT in this manner sends the data packets received directly to the server.	Only packets received on the specified port pass through the TCP engine.
You have configured a virtual server and a service to send all data packets received to either of two servers. You are attempting to configure INAT to send all data packets received to a different server.	The INAT configuration is not allowed.
You have configured INAT to send all received data packets directly to a server. You are attempting to configure a virtual server and a service to send all data packets received to two different servers.	The vserver configuration is not allowed.

Stateless NAT46 Translation

The stateless NAT46 feature enables communication between IPv4 and IPv6 networks through IPv4 to IPv6 packet translation, and vice versa, without maintaining any session information on the NetScaler appliance.

For a stateless NAT46 configuration, the appliance translates an IPv4 packet to IPv6 or an IPv6 packet to IPv4 as defined in RFCs 6145 and 2765.

Note: This feature is supported only on NetScaler 10.e and later.

A stateless NAT46 configuration on the NetScaler appliance has the following components:

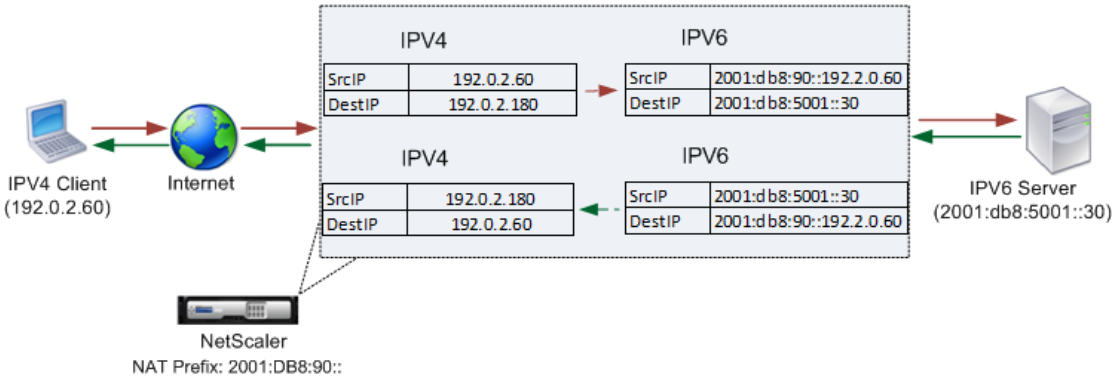
- **IPv4-IPv6 INAT entry**—An INAT entry defining a 1:1 relationship between an IPv4 address and an IPv6 address. In other words, an IPv4 address on the appliance listens to connection requests on behalf of an IPv6 server. An IPv4 request packet for this IPv4 address is translated into an IPv6 packet, and then the IPv6 packet is sent to the IPv6 server.

  The appliance translates an IPv6 response packet into an IPv4 response packet with its source IP address field set as the IPv4 address specified in the INAT entry. The translated packet is then sent to the client.

- **NAT46 IPv6 prefix**—A global IPv6 prefix of length 96 bits (128-32=96) configured on the appliance. During IPv4 packet to IPv6 packet translation, the appliance sets the source IP address of the translated IPv6 packet to a concatenation of the NAT46 IPv6 prefix [96 bits] and the IPv4 source address [32 bits] that was received in the request packet.

  During IPv6 packet to IPv4 packet translation, the appliance sets the destination IP address of the translated IPv4 packet to the last 32 bits of the destination IP address of the IPv6 packet.

Consider an example in which an enterprise hosts site www.example.com on server S1, which has an IPv6 address. To enable communication between IPv4 clients and IPv6 server S1, NetScaler appliance NS1 is deployed with a stateless NAT46 configuration that includes an IPv4-IPv6 INAT entry for server S1, and a NAT46 Prefix. The INAT entry includes an IPv4 address at which the appliance listens to connection requests from IPv4 clients on behalf of the IPv6 server S1.



The following table lists the settings used in this example:

Entities	Name	Value
IP address of the client	Client_IPv4 (for reference purposes only)	192.0.2.60
IPv6 address of the server	Sevr_IPv6 (for reference purposes only)	2001:DB8:5001::30
IPv4 address defined in the INAT entry for IPv6 server S1	Map-Sevr-IPv4 (for reference purposes only)	192.0.2.180
IPv6 prefix for NAT 46 translation	NAT46_Prefix (for reference purposes only)	2001:DB8:90::

Following is the traffic flow in this example:

1. IPv4 Client CL1 sends a request packet to the Map-Sevr-IPv4 (192.0.2.180) address on the NetScaler appliance.

2. The appliance receives the request packet and searches the NAT46 INAT entries for the IPv6 address mapped to the Map-sevr-IPv4 (192.0.2.180) address. It finds the Sevr-IPv6 (2001:DB8:5001::30) address.

3. The appliance creates a translated IPv6 request packet with:

   - Destination IP address field = Sevr-IPv6 = 2001:DB8:5001::30

   - Source IP address field = Concatenation of NAT Prefix (First 96 bits) and Client_IPv4 (last 32 bits) = 2001:DB8:90::192.0.2.60
4. The appliance sends the translated IPv6 request to Sevr-IPv6.

5. The IPv6 server S1 responds by sending an IPv6 packet to the NetScaler appliance with:

   - Destination IP address field = Concatenation of NAT Prefix (First 96 bits) and Client_IPv4 (last 32 bits)= 2001:DB8:90::192.0.2.60

   - Source IP address field = Sevr-IPv6 = 2001:DB8:5001::30
6. The appliance receives the IPv6 response packet and verifies that its destination IP address matches the NAT46 prefix configured on the appliance. Because the destination address matches the NAT46 prefix, the appliance searches the NAT46 INAT entries for the IPv4 address associated with the Sevr-IPv6 address (2001:DB8:5001::30). It finds the Map-Sevr-IPv4 address (192.0.2.180).

7. The appliance creates an IPv4 response packet with:

   - Destination IP address field = The NAT46 prefix stripped from the destination address of the IPv6 response = Client_IPv4 (192.0.2.60)

   - Source IP address field = Map-Sevr-IPv4 address (192.0.2.180)
8. The appliance sends the translated IPv4 response to client CL1.

Configuring Stateless NAT46

Creating the required entities for stateless NAT46 configuration on the NetScaler appliance involves the following procedures:

1. Create an IPv4-IPv6 mapping INAT entry with stateless mode enabled.
2. Add a NAT46 IPv6 prefix.

To configure an INAT mapping entry by using the command line interface

At the command prompt, type:

- add inat <name> <publicIPv4> <privateIPv6> -mode STATELESS
- show inat <name>

To add an NAT46 prefix by using the command line interface

At the command prompt, type:

- set inatparam -nat46v6Prefix <ipv6_addr|*>
- show inatparam

Example

```
 > add inat exmpl-com-stls-nat46 192.0.2.180
2001:DB8:5001::30 -mode stateless
Done

> set inatparam -nat46v6Prefix 2001:DB8:90::/96
Done
```

To configure an INAT mapping entry by using the configuration utility

1. Navigate to Network > Routes > INAT.
2. Add a new INAT entry, or edit an existing INAT entry.
3. Set the following parameters:
   - Name*
   - Public IP Address*
   - Private IP Address* (Select the IPv6 check box and enter the address in IPv6 format.)
   - Mode (Select Stateless from the drop down list.)

   * A required parameter

To add a NAT46 prefix by using the configuration utility

Navigate to Network, in the Settings group, click Change IPv6 settings, and set the IPv6 NAT Prefix parameter.

Parameter Descriptions (of commands listed in the CLI procedure)

add inat

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show inat

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Setting Global Parameters for Stateless NAT46

The appliance provides some optional global parameters for stateless NAT46 configurations.

To set global parameters for stateless NAT46 by using the command line interface

At the command prompt, type:

- set inatparam [-nat46IgnoreTOS (YES | NO)] [-nat46ZeroCheckSum (ENABLED | DISABLED)] [-nat46v6Mtu <positive_integer>] [-nat46FragHeader (ENABLED | DISABLED)]
- show inatparam

Example

```
> set inatparam -nat46IgnoreTOS YES -nat46ZeroCheckSum DISABLED -nat46v6Mtu 1400 -nat46FragHeader
 Done
```

To set global parameters for stateless NAT46 by using the configuration utility

Navigate to Network, in the Settings group, click Change IPv6 settings.

Limitations of Stateless NAT46

The following limitations apply to stateless NAT46:

- Translation of IPv4 options is not supported.
- Translation of IPv6 routing headers is not supported.
- Translation of hop-by-hop extension headers of IPv6 packets is not supported.
- Translation of ESP and EH headers of IPv4 packets is not supported.
- Translation of multicast packets is not supported.
- Translation of destination option headers and source routing headers is not supported.
- Translation of fragmented IPv4 UDP packets that do not contain UDP checksum is not supported.

Stateful NAT64 Translation

The stateful NAT64 feature enables communication between IPv4 clients and IPv6 servers through IPv6 to IPv4 packet translation, and vice versa, while maintaining session information on the NetScaler appliance.

A stateful NAT64 configuration on the NetScaler appliance has the following components:

- **NAT64 rule**— An entry consisting of an ACL6 rule and a netprofile, which consists of a pool of NetScaler owned SNIP Addresses.
- **NAT64 IPv6 Prefix**— A global IPv6 prefix of length 96 bits (128-32=96) configured on the appliance.

  Note: Currently the NetScaler appliance supports only one prefix to be used commonly with all NAT 64 rules.

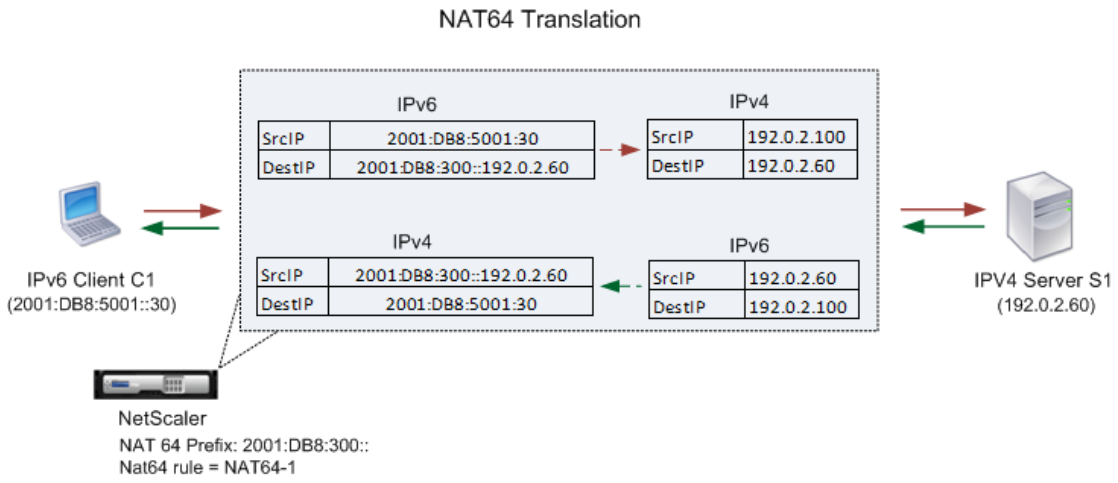
The NetScaler appliance considers an incoming IPv6 packet for NAT64 translation when all of the following conditions are met:

- The incoming IPv6 packet matches the ACL6 rule bound to a NAT64 rule.
- The destination IP address of the IPv6 packet matches the NAT64 IPv6 prefix.

When an IPv6 request packet received by the NetScaler appliance matches an ACL6 defined in a NAT64 rule and the destination IP of the packet matches the NAT64 IPv6 prefix, the NetScaler appliance considers the IPv6 packet for translation.

The appliance translates this IPv6 packet to an IPv4 packet with a source IP address matching one of the IP address bound to the netprofile defined in the NAT64 rule, and a destination IP address consisting of the last 32 bits of the destination IPv6 address of the IPv6 request packet. The NetScaler appliance creates a NAT64 session for this particular flow and forwards the packet to the IPv4 server. Subsequent responses from the IPv4 server and requests from the IPv6 client are translated accordingly by the appliance, on the basis of information in the particular NAT64 session.

Consider an example in which an enterprise hosts site www.example.com on server S1, which has an IPv4 address. To enable communication between IPv6 clients and IPv4 server S1, NetScaler appliance NS1 is deployed with a stateful NAT64 configuration that includes a NAT64 rule and a NAT64 prefix. A mapped IPv6 address of server S1 is formed by concatenating the NAT64 IPv6 prefix [96 bits] and the IPv4 source address [32 bits]. This mapped IPv6 address is then manually configured in the DNS servers. The IPv6 clients get the mapped IPv6 address from the DNS servers to communicate withIPv4 server S1.



The following table lists the settings used in this example:

Entities	Name	Value
IPv6 address of client CL1	Client_IPv6 (for reference purposes only)	2001:DB8:5001::30
IPv4 address of server S1	Sevr_IPv4 (for reference purposes only)	192.0.2.60
IPv6 prefix for NAT64 translation	NAT64_Prefix (for reference purposes only)	2001:DB8:300::
Mapped IPv6 address (NAT64_Prefix + Sevr_IPv4) of server S1 for IPv6 clients to reach server S1	Map-Sevr-IPv6 (for reference purposes only)	2001:DB8:300::192.0.2.60
ACL6 rule	ACL6-1	· Action = ALLOW · Source IP address =2001:DB8:5001::30
IPset	IPset-1	IP addresses bound (of type SNIPs) = 192.0.2.100 and 192.0.2.102
Netprofile	Netprofile-1	Source IP address = IPset-1
NAT64 rule	NAT64-1	ACL6 rule = ACL6-1 Netprofile = Netprofile-1

Following is the traffic flow in this example:

1. IPv6 client CL1 sends a request packet to Map-Sevr-IPv6 (2001:DB8:300::192.0.2.60) address.

2. The NetScaler appliance receives the request packet. If the request packet matches the ACL6 defined in the NAT64 rule, and the destination IP address of the packet matches the NAT64 IPv6 prefix, the NetScaler considers the IPv6 packet for translation.

3. The appliance creates a translated IPv4 request packet with:

- Destination IP address field containing the NAT64 prefix stripped from the destination address of the IPv6 request (Sevr_IPv4 = 192.0.2.60)

- Source IP address field containing one of the IPv4 address bound to Netprofile-1(in this case, 192.0.2.100)

4. The NetScaler appliance creates a NAT64 session for this flow and sends the translated IPv4 request to server S1.

5. IPv64 server S1 responds by sending an IPv4 packet to the NetScaler appliance with:

   - Destination IP address field containing 192.0.2.100

   - Source IP address field containing the address ofSevr_IPv4(192.0.2.60)
6. The appliance receives the IPv4 response packet, searches all the session entries, and finds that the IPv6 response packet matches the NAT64 session entry created in step 4. The appliance considers the IPv4 packet for translation.

7. The appliance creates a translated IPv6 response packet with:

   - Destination IP address field=Client_IPv6=2001:DB8:5001::30

   - Source IP address field = Concatenation of NAT64 Prefix (First 96 bits) and Sevr_IPv4 (last 32 bits) =2001:DB8:300::192.0.2.60
8. The appliance sends the translated IPv6 response to client CL1.

Limitations of Statelful NAT64

The following limitations apply to stateful NAT64 translation:

- Translation of IPv4 options is not supported.
- Translation of IPv6 routing headers is not supported.
- Translation of hop-by-hop extension headers of IPv6 packets is not supported.
- Translation of ESP and EH headers of IPv6 packets is not supported.
- Translation of multicast packets is not supported.
- Packets of Stream Control Transmission Protocol (SCTP), Datagram Congestion Control Protocol (DCCP), and IPSec, are not translated.

Configuring Stateful NAT64

Creating the required entities for stateful NAT64 configuration on the NetScaler appliance involves the following procedures:

1. Add an ACL6 rule with action ALLOW.
2. Add an ipset, which binds multiple IP addresses.
3. Add a netprofile and bind the ipset to it. If you want to bind only one IP address, you need not create an ipset entity. In that case, bind the IP address directly to the netprofile.
4. Add a NAT64 rule, which includes binding the ACl6 rule and the netprofile to the NAT 64 rule.
5. Add a NAT64 IPv6 prefix.

To add an ACL6 rule by using the command line interface

At the command prompt, type:

- add ns acl6 <acl6name> <acl6action> ...

To add an IPset and bind multiple IPs to it by using the command line interface

At the command prompt, type:

- add ipset <name>
- bind ipset <name> <IPaddress …>

To add a netprofile by using the command line interface

At the command prompt, type:

- add netprofile <name> -srcIP <IPaddress or IPset>

To add a NAT64 rule by using the command line interface

At the command prompt, type:

- add nat64 <name> <acl6name> -netProfile <string>

To add a NAT64 prefix by using the command line interface

At the command prompt, type:

- set ipv6 -natprefix <ipv6_addr|*>

Example

```
> add acl6 ACL6-1 ALLOW -srcIPv6 2001:DB8:5001::30
Done
```

```
> apply acls6
 Done

> add ip 192.0.2.100 255.255.255.0 -type SNIP
 Done

> add ip 192.0.2.102 255.255.255.0  -type SNIP
 Done

> add ipset IPset-1
 Done

> bind ipset IPset-1 192.0.2.100 192.0.2.102
IPAddress "192.0.2.100" bound
IPAddress "192.0.2.102" bound
 Done

> add netprofile Netprofile-1 -srcIP IPset-1
 Done

> add nat64 NAT64-1 ACL6-1 -netprofile Netprofile-1
 Done

> set ipv6 -natprefix 2001:DB8:300::/96
 Done
```

To add a NAT64 rule by using the configuration utility

Navigate to Network > Routes > NAT64, and a new NAT64 rule, or edit an existing rule.

To add a NAT64 prefix by using the configuration utility

Navigate to Network, in the Settings group, click Change IPv6 settings, and set the IPv6 NAT Prefix parameter.

Parameter Descriptions (of commands listed in the CLI procedure)

add ns acl6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add ipset

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind ipset

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add netprofile

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

set ipv6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring RNAT

In Reverse Network Address Translation (RNAT), the NetScaler appliance replaces the source IP addresses in the packets generated by the servers with public NAT IP addresses. By default, the appliance uses a Mapped IP address (MIP) as the NAT IP address. You can also configure the appliance to use a unique NAT IP address for each subnet. You can also configure RNAT by using Access Control Lists (ACLs). Use Source IP (USIP), Use Subnet IP (USNIP), and Link Load Balancing (LLB) modes affect the operation of RNAT. You can display statistics to monitor RNAT.

Note: The ephemeral port range for RNAT on the NetScaler appliance is 1024-65535.

You can use either a network address or an extended ACL as the condition for an RNAT entry:

- **Using a Network address.** When you use a network address, RNAT processing is performed on all of the packets coming from the specified network.
- **Using Extended ACLs.** When you use ACLs, RNAT processing is performed on all packets that match the ACLs. To configure the NetScaler appliance to use a unique IP address for traffic that matches an ACL, you must perform the following three tasks:

  1. Configure the ACL.
  2. Configure RNAT to change the source IP address and Destination Port.
  3. Apply the ACL.

  The following diagram illustrates RNAT configured with an ACL.

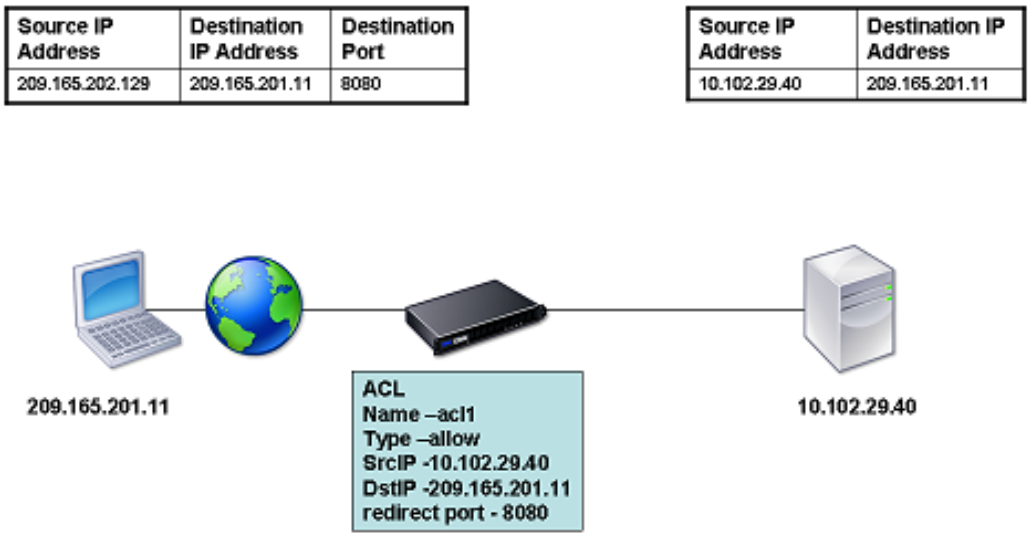


Figure 1. RNAT with an ACL

You have the following basic choices for the type of NAT IP address:

- **Using a MIP or SNIP as the NAT IP Address.** When using a MIP as the NAT IP address, the NetScaler appliance replaces the source IP addresses of server-generated packets with the a MIP. Therefore, the MIP address must be a public IP address. If Use Subnet IP (USNIP) mode is enabled, the NetScaler can use a subnet IP address (SNIP) as the NAT IP address.

- **Using a Unique IP Address as the NAT IP Address.** When using a unique IP address as the NAT IP address, the NetScaler appliance replaces the source IP addresses of server-generated packets with the unique IP address specified. The unique IP address must be a public NetScaler-owned IP address. If multiple NAT IP addresses are configured for a subnet, NAT IP selection uses the round robin algorithm.

  This configuration is illustrated in the following diagram.

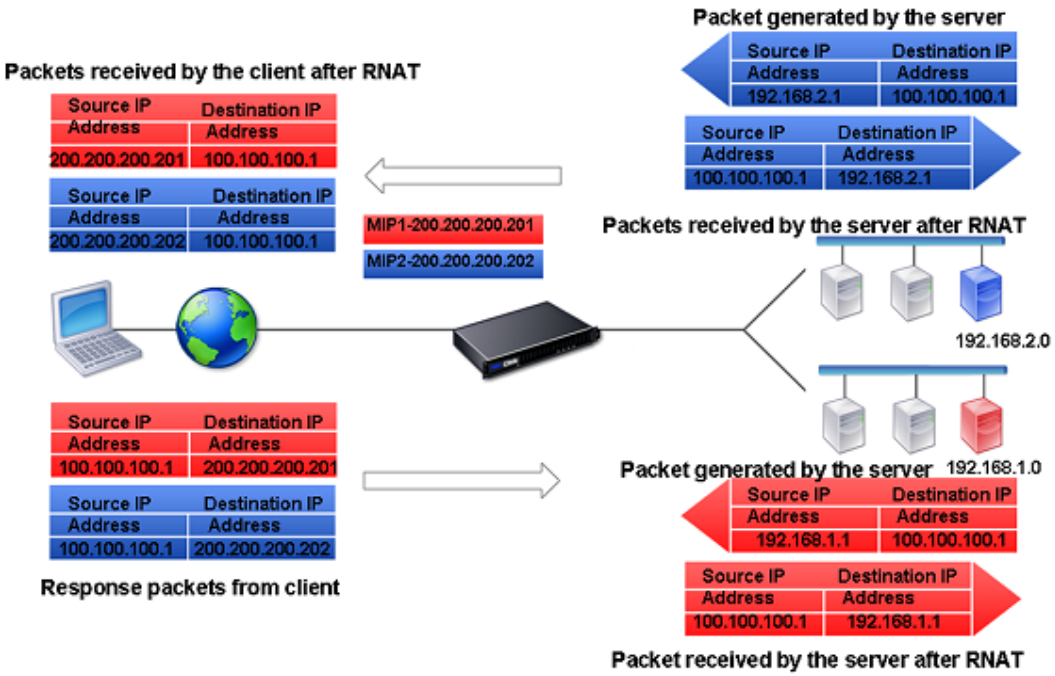


Figure 2. Using a Unique IP Address as the NAT IP Address

Creating an RNAT Entry

The following instructions provide separate command-line procedures for creating RNAT entries that use different conditions and different types of NAT IP addresses. In the configuration utility, all of the variations can be configured in the same dialog box, so there is only one procedure for configuration utility users.

To create an RNAT entry by using the command line interface

At the command prompt, type one the following commands to create, respectively, an RNAT entry that uses a network address as the condition and a MIP or SNIP as the NAT IP address, an RNAT entry that uses a network address as the condition and a unique IP address as the NAT IP address, an RNAT entry that uses an ACL as the condition and a MIP or SNIP as the NAT IP address, or an RNAT entry that uses an ACL as a condition and a unique IP address as the NAT IP address:

- set rnat <IPAddress> <netmask>
- set rnat IPAddress <netMask> -natip <NATIPAddress>
- set rnat <aclname> [-redirectPort <port>]
- set rnat <aclname> [-redirectPort <port>] -natIP <NATIPAddress>

  Use the following command to verify the configuration:

- show rnat

Examples

A network address as the condition and a MIP or SNIP as the NAT IP address:

```
> set rnat 192.168.1.0 255.255.255.0
 Done
```

A network address as the condition and a unique IP address as the NAT IP address:

```
> set rnat 192.168.1.0 255.255.255.0 -natip 10.102.29.50
 Done
```

If instead of a single NAT IP address you specify a range, RNAT entries are created with all the NetScaler-ow

```
> set rnat 192.168.1.0 255.255.255.0  -natIP 10.102.29.[50-110]
 Done
```

An ACL as the condition and a MIP or SNIP as the NAT IP address:

```
> set rnat acl1
 Done
```

An ACL as a condition and a unique IP address as the NAT IP address:

```
> set rnat acl1  -natIP 209.165.202.129
Done
```

If instead of a single NAT IP address you specify a range, RNAT entries are created with all the NetScaler-ow

```
> set rnat acl1  -natIP 10.102.29.[50-70]
 Done
```

To create an RNAT entry by using the configuration utility

1. Navigate to Network > Routes > RNAT.
2. Click Configure RNAT.

Parameter Descriptions (of commands listed in the CLI procedure)

set rnat

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show rnat

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Monitoring RNAT

You can display RNAT statistics to troubleshoot issues related to IP address translation.

To view RNAT statistics by using the command line interface

At the command prompt, type:

stat rnat

Example

```
> stat rnat

RNAT summary
                        Rate (/s)          Total
Bytes Received                0                0
Bytes Sent                    0                0
Packets Received              0                0
Packets Sent                  0                0
Syn Sent                      0                0
Current RNAT sessions         --               0
 Done
>
```

The following tables describes the statistics associated with RNAT and RNAT IP.

Table 1. RNAT Statistics

Statistic	Description
Bytes received	Bytes received during RNAT sessions
Bytes sent	Bytes sent during RNAT sessions
Packets received	Packets received during RNAT sessions
Packets sent	Packets sent during RNAT sessions
Syn sent	Requests for connections sent during RNAT sessions
Current sessions	Currently active RNAT sessions

To monitor RNAT by using the configuration utility

Navigate to Network > Routes > RNAT, and click Statistics.

Parameter Descriptions (of commands listed in the CLI procedure)

stat rnat

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

RNAT in USIP, USNIP, and LLB Modes

Before configuring a RNAT rule, consider the following points:

- When RNAT and Use Source IP (USIP) are both configured on the NetScaler appliance, RNAT takes precedence. In other words, the source IP address of the packets, which matches a RNAT rule, is replaced according to the setting in the RNAT rule.
- When RNAT and Use SNIP (USNIP) are configured on the NetScaler appliance, selection of the source IP address is based on the state of USNIP, as follows:
    - If USNIP is off, the NetScaler appliance uses the mapped IP addresses.
    - If USNIP is on, the NetScaler uses a SNIP address as the NAT IP address.

This behavior does not apply when a unique NAT IP address is used.

In a topology where the NetScaler appliance performs both Link Load Balancing (LLB) and RNAT for traffic originating from the server, the appliance selects the source IP address based on the router. The LLB configuration determines selection of the router. For more information about LLB, see "Link Load Balancing."

Configuring RNAT for IPv6 Traffic

Reverse Network Address Translation (RNAT) rules for IPv6 packets are called *RNAT6s*. When an IPv6 packet generated by a server matches the conditions specified in the RNAT6 rule, the appliance replaces the source IPv6 address of the IPv6 packet with a configured NAT IPv6 address before forwarding it to the destination. The NAT IPv6 address is one of the NetScaler owned SNIP6 or VIP6 addresses.

When configuring an RNAT6 rule, you can specify either an IPv6 prefix or an ACL6 as the condition:

- **Using a IPv6 network address**. When you use an IPv6 prefix, the appliance performs RNAT processing on those IPv6 packets whose IPv6 address matches the prefix.
- **Using ACL6s**. When you use an ACL6, the appliance performs RNAT processing on those IPv6 packets that match the conditions specified in the ACL6.

You have one of the following options to set the NAT IP address:

- Specify a set of NetScaler owned SNIP6 and VIP6 addresses for an RNAT6 rule. The NetScaler appliance uses any one of the IPv6 addresses from this set as a NAT IP address for each session. The selection is based on the round robin algorithm and is done for each session.
- Do not specify any NetScaler owned SNIP6 or VIP6 address for an RNAT6 rule. The NetScaler appliance uses any one of the NetScaler owned SNIP6 or VIP6 addresses as a NAT IP address. The selection is based on the next hop network to which an IPv6 packet that matches the RNAT rule is destined.

To create an RNAT6 rule by using the command line interface

At the command prompt, to create the rule and verify the configuration, type:

- add rnat6 <name> (<network> | (<acl6name> [-redirectPort <port>]))
- bind rnat6 <name> <natIP6>@ ...
- show rnat6

To modify or remove an RNAT6 rule by using the command line interface

- To modify an RNAT6 rule whose condition is an ACL6, type the set rnat6 <name> command, followed by a new value for the redirectPort parameter.
- To remove an RNAT6 rule, type the clear rnat6 <name> command.
- show rnat6

To configure an RNAT6 rule by using the configuration utility

Navigate to Network > Routes > RNAT6, and add a new RNAT6 rule, or edit an existing rule.

Parameter Descriptions (of commands listed in the CLI procedure)

add rnat6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind rnat6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show rnat6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Prefix-Based IPv6-IPv4 Translation

Prefix-based translation is a process of translating packets sent from private IPv6 servers into IPv4 packets, using an IPv6 prefix configured in the NetScaler appliance. This prefix has a length of 96 bits (128-32=96). The IPv6 servers embed the destination IP address of the IPv4 servers or hosts in the last 32 bits of the destination IP address field of the IPv6 packets. The first 96 bits of the destination IP address field are set as the IPv6 NAT prefix.

The NetScaler appliance compares the first 96 bits of the destination IP address of all the incoming IPv6 packets to the configured prefix. If there is a match, the NetScaler appliance generates an IPv4 packet and sets the destination IP address as the last 32 bits of the destination IP address of the matched IPv6 packet. IPv6 packets addressed to this prefix have to be routed to the NetScaler so that the IPv6-IPv4 translation is done by the NetScaler.

In the following diagram, 3ffe::/96 is configured as the IPv6 NAT prefix on NetScaler NS1. The IPv6 host sends an IPv6 packet with destination IP address 3ffe::74.125.91.105. NS1 compares the first 96 bits of the destination IP address of all the incoming IPv6 packets to the configured prefix, and they match. NS1 then generates an IPv4 packet and sets the destination IP address as 74.125.91.105.

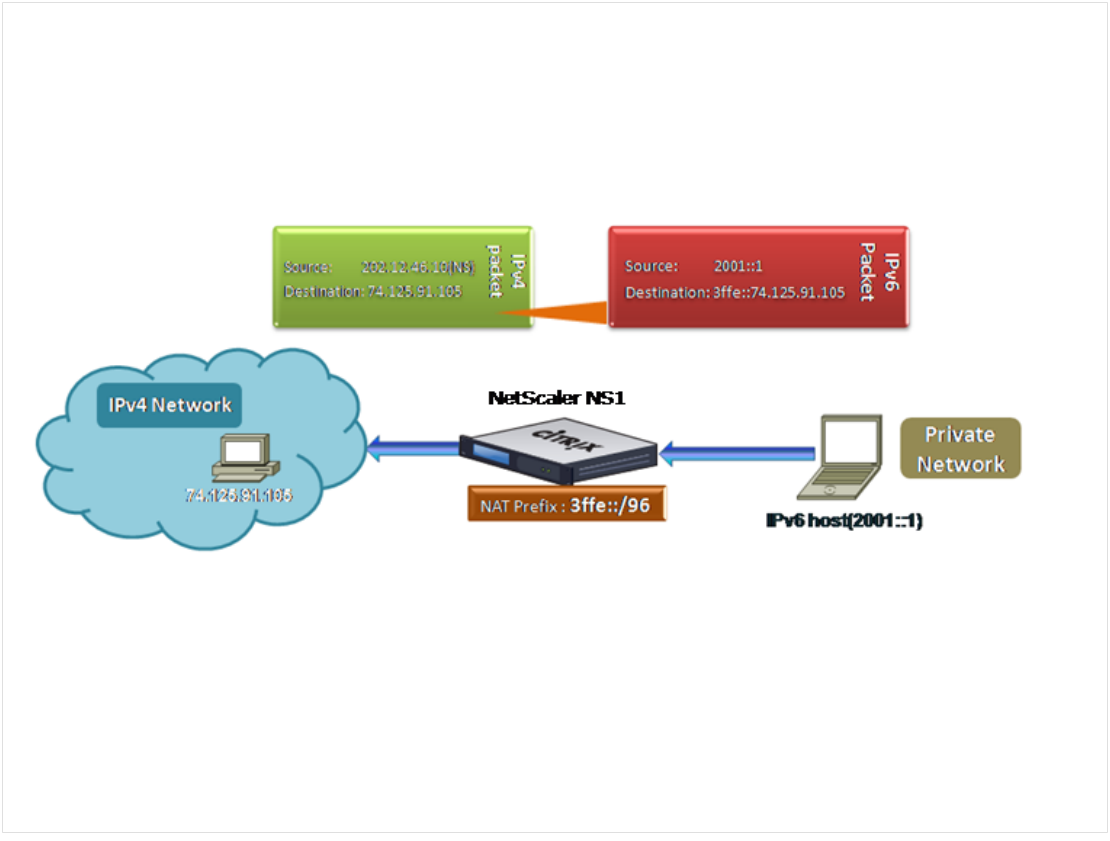


Figure 1. IPv6-IPv4 Prefix-Based Translation

To configure prefix-based IPv6-IPv4 translation by using the command line interface

At the command prompt, type the following commands to set a NAT prefix and verify its configuration:

- set ipv6 [-natprefix <ipv6_addr|*>]
- show ipv6

Example

```
> set ipv6 -natprefix 3ffe::/96
 Done
```

To configure prefix-based IPv6-IPv4 translation by using the configuration utility

Navigate to Network, in the Settings group, click Change IPv6 settings, and set the IPv6 NAT Prefix parameter.

Parameter Descriptions (of commands listed in the CLI procedure)

set ipv6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ipv6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Static ARP

You can add static ARP entries to and remove static ARP entries from the ARP table. After adding an entry, you should verify the configuration. If the IP address, port, or MAC address changes after you create a static ARP entry, you must remove or manually adjust the static entry. Therefore, creating static ARP entries is not recommended unless necessary.

To add a static ARP entry by using the command line interface

At the command prompt, type:

- add arp -IPAddress <ip_addr> -mac<mac_addr> -ifnum <interface_name>
- show arp <IPAddress>

Example

```
> add arp -ip 10.102.29.6 -mac 00:24:e8:73:ca:ec -ifnum 1/1
 Done
```

To remove a static ARP entry by using the command line interface

At the command prompt, type the rm arp command and the IP address.

To add a static ARP entry by using the configuration utility

Navigate to Network > ARP Table, and a new ARP entry.

Parameter Descriptions (of commands listed in the CLI procedure)

add arp

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show arp

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Setting the Timeout for Dynamic ARP Entries

You can globally set an aging time (time-out value) for dynamically learned ARP entries. The new value applies only to ARP entries that are dynamically learned after the new value is set. Previously existing ARP entries expire after the previously configured aging time.

You can specify an ARP time-out value of from 1 through 1200 seconds.

To set the time-out for dynamic ARP entries by using the command line interface

At the command prompt, type the following commands to set the time-out for dynamic ARP entries and verify its configuration:

- set arpparam -timeout <positive_integer>]
- show arpparam

Example

```
> set arpparam -timeout 500
 Done
```

To set the time-out for dynamic ARP entries to its default value by using the command line interface

At the command prompt, type the following commands to set the time-out for dynamic ARP entries to its default value and verify its configuration:

- unset arpparam
- show arpparam

Example

```
> unset arpparam
 Done
```

To set the time-out for dynamic ARP entries by using the configuration utility

Navigate to Network, in the Settings group, click Configure ARP Global Parameters, and set the ARP Table Entry Timeout parameter.

Parameter Descriptions (of commands listed in the CLI procedure)

set arpparam

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show arpparam

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

unset arpparam

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Neighbor Discovery

Neighbor discovery (ND) is one of the most important protocols of IPv6. It is a message-based protocol that combines the functionality of the Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Router Discovery. ND allows nodes to advertise their link layer addresses and obtain the MAC addresses or link layer addresses of the neighboring nodes. This process is performed by the Neighbor Discovery protocol (ND6).

Neighbor discovery can perform the following functions:

Router Discovery

Enables a host to discover the local routers on an attached link and automatically configure a default router.

Prefix Discovery

Enables the host to discover the network prefixes for local destinations.

Note: Currently, the NetScaler does not support Prefix Discovery.

Parameter Discovery

Enables a host to discover additional operating parameters, such as MTU and the default hop limit for outbound traffic.

Address Autoconfiguration

Enables hosts to automatically configure IP addresses for interfaces both with and without stateful address configuration services such as DHCPv6. The NetScaler does not support Address Autoconfiguration for Global IPv6 addresses.

Address Resolution

Equivalent to ARP in IPv4, enables a node to resolve a neighboring node's IPv6 address to its link-layer address.

Neighbor Unreachability Detection

Enables a node to determine the reachability state of a neighbor.

Duplicate Address Detection

Enables a node to determine whether an NSIP address is already in use by a neighboring node.

Redirect

Equivalent to the IPv4 ICMP Redirect message, enables a router to redirect the host to a better first-hop IPv6 address to reach a destination.

Note: The NetScaler does not support IPv6 Redirect.

To enable neighbor discovery, you create entries for the neighbors.

Adding IPv6 Neighbors

Adding IPv6 neighbors enables neighbor discovery.

To add an IPv6 neighbor by using the command line interface

At the command prompt, type:

- add nd6 <neighbor> <mac> <ifnum> [-vlan <integer>]
- show nd6

Example

```
> add nd6 2001::1 00:04:23:be:3c:06 1/1 –vlan 1
 Done
> show nd6
  Neighbor              MAC-Address(Vlan, Interface)      State       TIME
  --------              ----------------------------      -----     --------
1) ::1                  00:d0:68:0b:58:da(   1,  LO/1)   REACHABLE     PERMANENT
2) fe80::2d0:68ff:fe0b:58da 00:d0:68:0b:58:da(   1,  LO/1)   REACHABLE     PERMANENT
3) 2001::1                00:04:23:be:3c:06(   1,   1/1)   REACHABLE       STATIC
 Done
```

Neighbor Discovery Parameters

neighbor

IPv6 neighbor entry. Mandatory.

mac

Unique address assigned to identify the network appliance. Mandatory.

ifnum

The interface on which the MAC resides. Mandatory.

vlan

Virtual LAN (VLAN) that the neighbor is part of.

To add an IPv6 neighbor by using the configuration utility

Navigate to Network > IPv6 Neighbors, and add a new IPv6 neighbor.

Parameter Descriptions (of commands listed in the CLI procedure)

add nd6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show nd6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Removing IPv6 Neighbors

To remove a neighbor discovery entry by using the command line interface

At the command prompt, type:

rm nd6 <Neighbor> -vlan <VLANID>

Example

rm nd6 3ffe:100:100::1 -vlan 1

To remove all neighbor discovery entries by using the command line interface

At the command prompt, type:

clear nd6

To remove a neighbor discovery entry by using the configuration utility

Navigate to Network > IPv6 Neighbors, delete the IPv6 neighbor.

To remove all neighbor discovery entries by using the configuration utility

Navigate to Network > IPv6 Neighbors, and click Clear.

Parameter Descriptions (of commands listed in the CLI procedure)

rm nd6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

clear nd6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring IP Tunnels

An IP Tunnel is a communication channel, that can be created by using encapsulation technologies, between two networks that do not have a routing path. Every IP packet that is shared between the two networks is encapsulated within another packet and then sent via the tunnel.

The NetScaler appliance implements IP Tunneling in the following ways:

- NetScaler as an Encapsulator (Load Balancing with DSR mode)
- NetScaler as a Decapsulator

NetScaler as an Encapsulator (Load Balancing with DSR Mode)

Consider an organization that has multiple data centers across different countries, where the NetScaler maybe at one location and the back-end servers are located in a different country. In essence, the NetScaler and the back-end servers are on different networks and are connected via a router.

When you configure Direct Server Return (DSR) on this NetScaler, the packet sent from the source subnet is encapsulated by the NetScaler and sent via a router and tunnel to the appropriate back-end server. The back-end server decapsulates the packet and responds directly to the client, without allowing the packet to pass via the NetScaler.

NetScaler as a Decapsulator

Consider an organization having multiple data centers each having NetScalers and back-end servers. When a packet is sent from data center A to data center B it is usually sent via an intermediary, say a router or another NetScaler. The NetScaler processes the packet and then forwards the packet to the back-end server. However, if an encapsulated packet is sent, the NetScaler must be able to decapsulate the packet before sending it to the back-end servers. To enable the NetScaler to function as a decapsulator, a tunnel is added between the router and the NetScaler. When the encapsulated packet, with additional header information, reaches the NetScaler, the data packet is decapsulated i.e. the additional header information is removed, and the packet is then forwarded to the appropriate back-end servers.

The NetScaler can also be used as a decapsulator for the Load Balancing feature, specifically in scenarios when the number of connections on a vserver exceeds a threshold value and all the new connections are then diverted to a back-up vserver.

Creating IP Tunnels

To create an IP tunnel by using the command line interface

At the command prompt type:

- add iptunnel <name> <remote> <remoteSubnetMask> <local> -type -protocol (ipoverip | GRE) -ipsecprofile <name>
- show iptunnel

To remove an IP tunnel by using the command line interface

To remove an IP tunnel, type the rm iptunnel command and the name of the tunnel.

Parameters for creating an IP tunnel

name

Name of the IP Tunnel. This alphanumeric string is required and cannot be changed after the service group is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

remoteIp

A public IPv4 address of the remote NetScaler appliance used to set up the tunnel.

remoteSubnetMask

Subnet mask of the remote IP address of the tunnel.

localIp

A public IPv4 address of the local NetScaler appliance used to set up the tunnel. Possible values: Auto, MIP, SNIP, and VIP. Default: Auto.

protocol

The protocol to be used in setting up the IP tunnel. Select GRE for using the Generic Routing Encapsulation (GRE) protocol to set up a GRE tunnel.

ipsecProfileName

Name of the IPSec profile that is used for securing communication in the GRE tunnel.

To create an IP Tunnel by using the configuration utility

Navigate to Network > IP Tunnels, add a new IP tunnel.

To create an IPv6 tunnel by using the command line interface

At the command prompt type:

- add ip6tunnel <name> <remoteIp> <local>
- show ip6tunnel

To remove an IPv6 tunnel by using the command line interface

To remove an IPv6 tunnel, type the rm ip6tunnel command and the name of the tunnel.

Parameters for creating an IPv6 tunnel

name (Name)

A name for the IPv6 Tunnel. This alphanumeric string is required and cannot be changed after the service group is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

remoteIp (Remote IP)

An IPv6 address of the remote NetScaler appliance used to set up the tunnel.

localIp (Local IP Type)

An IPv6 address of the local NetScaler appliance used to set up the tunnel. Possible values: SNIP6 and VIP6. Default: Auto.

To create an IPv6 Tunnel by using the configuration utility

Navigate to Network > IP Tunnels > IPv6 Tunnels, and add a new IPv6 tunnel.

Customizing IP Tunnels Globally

By globally specifying the source IP address, you can assign a common source IP address across all tunnels. Also, because fragmentation is CPU-intensive, you can globally specify that the NetScaler appliance drop any packet that requires fragmentation. Alternatively, if you would like to fragment all packets as long as a CPU threshold value is not reached, you can globally specify the CPU threshold value.

To globally customize IP tunnels by using the command line interface

At the command prompt, type the following commands to globally customize IP tunnels and verify the configuration:

- set ipTunnelParam -srcIP <sourceIPAddress> -srcIPRoundRobin (YES | NO)-dropFrag [YES | NO] -dropFragCpuThreshold <Positive integer>
- show ipTunnelParam

Example

```
> set iptunnelparam –srcIP 12.12.12.22 -dropFrag Yes –dropFragCpuThreshold 50
 Done
> set iptunnelparam -srcIPRoundRobin YES -dropFrag Yes –dropFragCpuThreshold 50
 Done
```

Note: To create a new MIP or SNIP address to use as the global source IP address, use the add ns ip command before you type the set iptunnelparam command.

To globally customize IP tunnels by using the configuration utility

Navigate to Network, in the Settings group, click IPv4 Tunnel Global Settings.

1. Navigate to Network.
2. In the details pane, in the Settings group, click IPv4 Tunnel Global Settings.
3. In the Configure IP Tunnel Global Parameters dialog box, set the parameters. For a description of a parameter, hover the mouse cursor over the corresponding field.
4. Click OK and then click Close.

To globally customize IPv6 tunnels by using the command line interface

At the command prompt, type the following commands to globally customize IPv6 tunnels and verify the configuration:

- set ip6tunnelparam -srcIP <IPv6Address> -srcIPRoundRobin (YES | NO)-dropFrag [YES | NO] -dropFragCpuThreshold <Positive integer>
- show ip6tunnelparam

Note: To create a new VIP6 or SNIP6 address to use as the global source IP address, use the add ns ip6 command before you type the set ip6tunnelparam command.

To globally customize IPv6 tunnels by using the configuration utility

Navigate to Network, in the Settings group, click IPv6 Tunnel Global Settings.

Parameter Descriptions (of commands listed in the CLI procedure)

set ipTunnelParam

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ipTunnelParam

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

set ip6tunnelparam

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Interfaces

Before you begin configuring interfaces, decide whether your configuration can use MAC-based forwarding mode, and either enable or disable this system setting accordingly. The number of interfaces in your configuration is different for the different models of the Citrix NetScaler appliance. In addition to configuring individual interfaces, you can logically group interfaces, using VLANs to restrict data flow within a set of interfaces, and you can aggregate links into channels. In a high availability setup, you can configure a virtual MAC (VMAC) address if necessary. If you use L2 mode, you might want to modify the aging of the bridge table.

When your configuration is complete, decide whether you should enable the system setting for path MTU discovery. NetScaler appliances can be deployed in active-active mode using VRRP. An active-active deployment, in addition to preventing downtime, makes efficient use of all the NetScaler appliances in the deployment. You can use the Network Visualizer tool to view the network configuration of a NetScaler deployment and configure interfaces, channels, VLANs, and bridge groups.

Configuring MAC-Based Forwarding

With MAC-based forwarding (MBF) enabled, when a request reaches the NetScaler appliance, the appliance remembers the source MAC address of the frame and uses it as the destination MAC address for the resulting replies. MAC-based forwarding can be used to avoid multiple-route/ARP lookups and to avoid asymmetrical packet flows. MAC-based forwarding may be required when the NetScaler is connected to multiple stateful devices, such as VPNs or firewalls, because it ensures that the return traffic is sent to the same device that the initial traffic came from.

MAC-based forwarding is useful when you use VPN devices, because it guarantees that all traffic flowing through a VPN passes back through the same VPN device.

The following topology diagram illustrates the process of MAC-based forwarding.

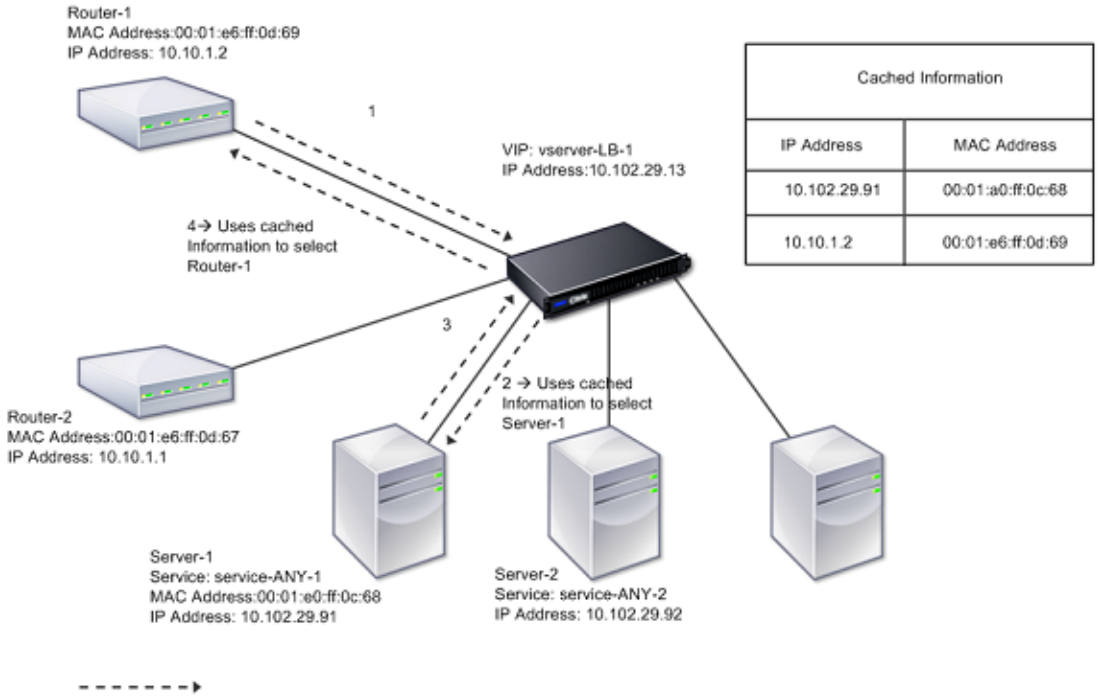


Figure 1. MAC-Based Forwarding Mode

When MAC-based forwarding (MBF) is enabled, the NetScaler caches the MAC address of:

- The source (a transmitting device such as router, firewall, or VPN device) of the inbound connection.
- The server that responds to the requests.

When a server replies through the NetScaler appliance, the appliance sets the destination MAC address of the response packet to the cached address, ensuring that the traffic flows in a symmetric manner, and then forwards the response to the client. The process bypasses the route table lookup and ARP lookup functions. However, when the NetScaler initiates a

connection, it uses the route and ARP tables for the lookup function. In a direct server return configuration, you must enable MAC-based forwarding.

For more information about direct server return configurations, see "Load Balancing."

Some deployment topologies may require the incoming and outgoing paths to flow through different routers. MAC-based forwarding would break this topology design.

MBF should be disabled in the following situations:

- **When you configure link load balancing.** In this case, asymmetric traffic flows are desirable because of link costs.
- **When a server uses network interface card (NIC) teaming without using LACP (802.1ad Link Aggregation).** To enable MAC-based forwarding in this situation, you must use a layer 3 device between the NetScaler and server.

  Note: MBF can be enabled when the server uses NIC teaming with LACP, because the virtual interface uses one MAC address.
- When firewall clustering is used. Firewall clustering assumes that ARP is used to resolve the MAC address for inbound traffic. Sometimes the inbound MAC address can be a non-clustered MAC address and should not be used for inbound packet processing.

When MBF is disabled, the NetScaler uses L2 or L3 connectivity to forward the responses from servers to the clients. Depending on the route table, the routers used for outgoing connection and incoming connection can be different. In the case of reverse traffic (response from the server):

- If the source and destination are on different IP subnets, the NetScaler uses the route lookup to locate the destination.
- If the source is on the same subnet as the destination, the NetScaler looks up the ARP table to locate the network interface and forwards the traffic to it. If the ARP table does not exist, the NetScaler requests the ARP entries.

To enable or disable MAC-based forwarding by using the command line interface

At the command prompt, type:

- enable ns mode MBF
- disable ns mode MBF

To enable or disable MAC-based forwarding by using the configuration utility

1. Navigate to System > Settings, in the Modes and Features group, click Configure modes.
2. Select or clear the MAC-based forwarding option.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns mode

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable ns mode

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Network Interfaces

Network interfaces in the NetScaler appliance are numbered in <slot>/<port> notation. After configuring your interfaces, you should display the interfaces and their settings to verify the configuration. You can also display this information to troubleshoot a problem in the configuration.

To manage the network interfaces, you might have to enable some interfaces and disable others. You can reset an interface to renegotiate its settings. You can clear the accumulated statistics for an interface. To verify the configuration, you can display the interface settings. You can display the statistics for an interface to evaluate its health.

Setting the Network Interface Parameters

The network interface configuration is neither synchronized nor propagated. For an HA pair, you must perform the configuration on each unit independently.

Network interface parameters include Link Aggregate Control Protocol (LACP) settings. For more information about Link Aggregate Control Protocol (LACP), see "Configuring Link Aggregation Using the Link Aggregate Channel Protocol."

To set the network interface parameters by using the command line interface

At the command prompt, type:

- set interface <id> [-speed <speed>] [-duplex <duplex>] [-flowControl <flowControl>] [-autoneg (DISABLED | ENABLED)] [-haMonitor (ON | OFF)] [(ON | OFF)] [-tagall (ON | OFF)] [-lacpMode <lacpMode>] [-lacpKey<positive_integer>] [-lacpPriority <positive_integer>] [-lacpTimeout (LONG | SHORT)] [-ifAlias <string>] [-throughput <positive_integer>][-bandwidthHigh <positive_integer> [-bandwidthNormal <positive_integer>]]

- show interface [<id>]

Example

```
> set interface 1/8 -duplex full
 Done
```

To set the network interface parameters by using the configuration utility

Navigate to Network > Interfaces, select the network interface that you want to modify (for example, 1/8), click Open, and then set the parameters.

1. Navigate to Network > Interfaces, and open the network interface.
2. Set the following parameters:
   - Speed*—speed
   - Duplex*—duplex
   - Flow Control*—flowControl

- Maximum Transmission Unit—mtu
- Auto Negotiation—autoneg
- HA Monitoring—haMonitor
- Tag all VLANs—tagall
- Trunk—trunk
- Alias Name—ifAlias
- Throughput—throughput
- Bandwidth High—bandwidthHigh
- Bandwidth Normal—bandwidthNormal
- LLDP mode*—lldpmode

* A required parameter

Parameter Descriptions (of commands listed in the CLI procedure)

set interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Enabling and Disabling Network Interfaces

By default, the network interfaces are enabled. You must disable any network interface that is not connected to the network, so that it cannot send or receive packets. Disabling a network interface that is connected to the network in a high availability setup can cause failover.

For more information about high availability, see "High Availability."

To enable or disable a network interface by using the command line interface

At the command prompt, type one of the following pairs of commands to enable or disable an interface and verify the setting:

- enable interface <interface_num>
- show interface <interface_num>
- disable interface <interface_num>
- show interface <interface_num>

Example

```
> enable interface 1/8
 Done
> show interface 1/8
      Interface 1/8 (Gig Ethernet 10/100/1000 MBits) #2
      flags=0x4004000 <ENABLED, DOWN, BOUND to LA/1, down, autoneg, 802.1q>
      MTU=1514, MAC=00:d0:68:15:fd:3d, downtime 906h58m40s
      Requested: media UTP, speed AUTO, duplex FULL, fctl OFF, throughput 0
      RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
      TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
      NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
      Bandwidth thresholds are not set.
Done
```

To enable or disable a network interface by using the configuration utility

1. Navigate to Network > Interfaces.
2. Select the network interface, and click Enable or Disable.

Parameter Descriptions (of commands listed in the CLI procedure)

enable interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Resetting Network Interfaces

Network interface settings control properties such as duplex and speed. To renegotiate the settings of a network interface, you must reset it.

To reset a network interface by using the command line interface

At the command prompt, type the following commands to reset an interface and verify the setting:

- reset interface <interface_num>
- show interface <interface_num>

Example

```
> reset interface 1/8
 Done
```

To reset a network interface by using the configuration utility

1. Navigate to Network > Interfaces.
2. Select the network interface, and click Reset Interface.

Parameter Descriptions (of commands listed in the CLI procedure)

reset interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Monitoring a Network Interface

You can display network interface statistics to monitor parameters such as packets sent and packets received, throughput, Link Aggregate Control Protocol (LACP) data units, and errors, and use the information to check the health of the network interface. You can clear the statistics of a network interface to monitor its statistics from the time the statistics are cleared.

To display the statistics of the network interfaces by using the command line interface

At the command prompt, type:

stat interface <interface_num>

To display the statistics of an Interface by using the configuration utility

Navigate to Network > Interfaces, select the network interface, and click StatisticsInterface Statistics.

To clear a network interface's statistics by using the command line interface

At the command prompt, type:

clear interface <interface_num>

Example

```
> clear interface 1/8
 Done
```

To clear a network interface's statistics by using the configuration utility

1. Navigate to Network > Interfaces.
2. Select the network interface, and click Clear Statistics.

Parameter Descriptions (of commands listed in the CLI procedure)

stat interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

clear interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Forwarding Session Rules

By default, the NetScaler appliance does not create session entries for traffic that it only forwards (L3 mode). For a case in which a client request that the appliance forwards to a server results in a response that has to return by the same path, you can create a forwarding-session rule. A forwarding-session rule creates forwarding-session entries for traffic that originates from or is destined for a particular network and is forwarded by the NetScaler. You can create forwarding session rules for IPv4 traffic as well as IPv6 traffic.

When configuring an IPv4 forwarding-session rule, you can specify either an IPv4 network address or an extended ACL as the condition for identifying IPv4 traffic for which to create a forwarding-session entry:

- **Network address**. When you specify an IPv4 network address, the appliance creates forwarding sessions for IPv4 traffic whose source or destination matches the network address.
- **Extended ACL rule**. When you specify an extended ACL rule, the appliance creates forwarding sessions for IPv4 traffic that matches the conditions specified in the extended ACL rule.

When configuring an IPv6 forwarding-session rule, you can specify either an IPv6 prefix or an ACL6 as the condition for identifying IPv6 traffic for which to create a forwarding-session entry:

- **IPv6 prefix**. When you specify an IPv6 prefix, the appliance creates forwarding sessions for IPv6 traffic whose source or destination matches the IPv6 prefix.
- **ACL6 rule**. When you specify an ACL6 rule, the appliance creates forwarding sessions for IPv6 traffic that matches the conditions specified in the ACL6 rule.

To create an IPv4 forwarding session rule by using the command line interface

At the command prompt, type the following commands to create a forwarding-session rule and verify the configuration:

- add forwardingSession <name> [<network> <netmask>] | [-aclname <string>] -connfailover (ENABLED | DISABLED)
- show forwardingSession

Example

A network address as the condition:

```
> add forwardingSession fs-nw-1 10.102.105.51 255.255.255.255
 Done
```

An ACL as the condition:

```
> add forwardingSession fs-acl-1 acl1
 Done
```

To configure an IPv4 forwarding session rule by using the configuration utility

Navigate to Network > Forwarding Sessions, add a new IPv4 forwarding session, or edit an existing forwarding session.

To create an IPv6 forwarding session rule by using the command line interface

At the command prompt, type the following commands to create a forwarding-session rule and verify the configuration:

- add forwardingSession <name> [<IPv6 prefix>] | [-acl6name <string>]
- show forwardingSession

Example

An IPv6 prefix as the condition:

```
> add forwardingSession fsv6-pfx-1 3ffe::/64
 Done
```

An ACL6 rule as the condition:

```
> add forwardingSession fsv6-acl6-1 –acl6name ACL6-FS
 Done
```

To configure an IPv6 forwarding session rule by using the configuration utility

Navigate to Network > Forwarding Sessions, add a new IPv6 forwarding session, or edit an existing forwarding session.

Parameter Descriptions (of commands listed in the CLI procedure)

add forwardingSession

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show forwardingSession

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Understanding VLANs

A NetScaler appliance supports Layer 2 port and IEEE 802.1q tagged VLANs. VLAN configurations are useful when you need to restrict traffic to certain groups of stations. You can configure a network interface as a part of multiple VLANs by using IEEE 802.1q tagging.

You can configure VLANs and bind them to IP subnets. The NetScaler then performs IP forwarding between these VLANs (if it is configured as the default router for the hosts on these subnets).

The NetScaler supports the following types of VLANs:

Port-Based VLANs. The membership of a port-based VLAN is defined by a set of network interfaces that share a common, exclusive Layer 2 broadcast domain. You can configure multiple port-based VLANs. By default, all network interfaces on the NetScaler are members of VLAN 1.

If you apply 802.1q tagging to the port, the network interface belongs to a port-based VLAN. Layer 2 traffic is bridged within a port-based VLAN, and Layer 2 broadcasts are sent to all members of the VLAN if Layer 2 mode is enabled. When you add an untagged network interface as a member of a new VLAN, it is removed from its current VLAN.

Default VLAN. By default, the network interfaces on the NetScaler are included in a single, port-based VLAN as untagged network interfaces. This VLAN is the default VLAN. It has a VLAN ID (VID) of 1. This VLAN exists permanently. It cannot be deleted, and its VID cannot be changed.

When you add a network interface to a to a different VLAN as an untagged member, the network interface is automatically removed from the default VLAN. If you unbind a network interface from its current port-based VLAN, it is added to the default VLAN again.

Tagged VLANs. 802.1q tagging (defined in the IEEE 802.1q standard) allows a networking device (such as the NetScaler) to add information to a frame at Layer 2 to identify the VLAN membership of the frame. Tagging allows network environments to have VLANs that span multiple devices. A device that receives the packet reads the tag and recognizes the VLAN to which the frame belongs. Some network devices do not support receiving both tagged and untagged packets on the same network interface—in particular, Force10 switches. In such cases, you need to contact customer support for assistance.

The network interface can be a tagged or untagged member of a VLAN. Each network interface is an untagged member of one VLAN only (its native VLAN). This network interface transmits the frames for the native VLAN as untagged frames. A network interface can be a part of more than one VLAN if the other VLANs are tagged.

When you configure tagging, be sure to match the configuration of the VLAN on both ends of the link. The port to which the NetScaler connects must be on the same VLAN as the NetScaler network interface.

Note: This VLAN configuration is neither synchronized nor propagated, therefore you must perform the configuration on each unit in an HA pair independently.

Applying Rules to Classify Frames

VLANs have two types of rules for classifying frames:

Ingress rules. Ingress rules classify each frame as belonging only to a single VLAN. When a frame is received on a network interface, the following rules are applied to classify the frame:

- If the frame is untagged, or has a tag value equal to 0, the VID of the frame is set to the port VID (PVID) of the receiving interface, which is classified as belonging to the native VLAN. (PVIDs are defined in the IEEE 802.1q standard.)
- If frame has a tag value equal to FFF, the frame is dropped.
- If the VID of the frame specifies a VLAN of which the receiving network interface is not a member, the frame is dropped. For example, if a packet is sent from a subnet associated with VLAN ID 12 to a subnet associated with VLAN ID 10, the packet is dropped. If an untagged packet with VID 9 is sent from the subnet associated with VLAN ID 10 to a network interface PVID 9, the packet is dropped.

Egress Rules. The following egress rules are applied:

- If the VID of the frame specifies a VLAN of which the transmission network interface is not a member, the frame is discarded.
- During the learning process (defined by the IEEE 802.1q standard), the Src MAC and VID are used to update the bridge lookup table of the NetScaler.
- A frame is discarded if its VID specifies a VLAN that does not have any members. (You define members by binding network interfaces to a VLAN.)

VLANs and Packet Forwarding on the NetScaler

The forwarding process on the NetScaler appliance is similar to that on any standard switch. However, the NetScaler performs forwarding only when Layer 2 mode is on. The key features of the forwarding process are:

- Topology restrictions are enforced. Enforcement involves selecting each network interface in the VLAN as a transmission port (depending on the state of the network interface), bridging restrictions (do not forward on the receiving network interface), and MTU restrictions.
- Frames are filtered on the basis of information in the bridge table lookup in the forwarding database (FDB) table of the NetScaler. The bridge table lookup is based on the destination MAC and the VID. Packets addressed to the MAC address of the NetScaler are processed at the upper layers.
- All broadcast and multicast frames are forwarded to each network interface that is a member of the VLAN, but forwarding occurs only if L2 mode is enabled. If L2 mode is disabled, the broadcast and multicast packets are dropped. This is also true for MAC addresses that are not currently in the bridging table.
- A VLAN entry has a list of member network interfaces that are part of its untagged member set. When forwarding frames to these network interfaces, a tag is not inserted

in the frame.

- If the network interface is a tagged member of this VLAN, the tag is inserted in the frame when the frame is forwarded.

When a user sends any broadcast or multicast packets without the VLAN being identified, that is, during duplicate address detection (DAD) for NSIP or ND6 for the next hop of the route, the packet is sent out on all the network interfaces, with appropriate tagging based on either the Ingress and Egress rules. ND6 usually identifies a VLAN, and a data packet is sent on this VLAN only. Port-based VLANs are common to IPv4 and IPv6. For IPv6, the NetScaler supports prefix-based VLANs.

Configuring a VLAN

You can implement VLANs in the following environments:

- Single subnet
- Multiple subnets
- Single LAN
- VLANs (no tagging)
- VLANs (802.1q tagging)

If you configure VLANs that have only untagged network interfaces as their members, the total number of possible VLANs is limited to the number of network interfaces available in the NetScaler. If more IP subnets are required with a VLAN configuration, 802.1q tagging must be used.

When you bind a network interface to a VLAN, the network interface is removed from the default VLAN. If the network interfaces need to be a part of more than one VLAN, you can bind the network interfaces to the VLANs as tagged members.

You can configure the NetScaler to forward traffic between VLANs at Layer 3. In this case, a VLAN is associated with a single IP subnet. The hosts in a VLAN that belong to a single subnet use the same subnet mask and one or more default gateways connected to that subnet. Configuring Layer 3 for a VLAN is optional. Layer 3 is used for IP forwarding (inter-VLAN routing). Each VLAN has a unique IP address and subnet mask that define an IP subnet for the VLAN. In an HA configuration, this IP address is shared with the other NetScaler appliances. The NetScaler forwards packets between configured IP subnets (VLANs).

When you configure the NetScaler, you must not create overlapping IP subnets. Doing so impedes Layer 3 functionality.

Each VLAN is a unique Layer 2 broadcast domain. Two VLANs, each bound to separate IP subnets, cannot be combined into a single broadcast domain. Forwarding traffic between two VLANs requires a Layer 3 forwarding (routing) device, such as the NetScaler appliance.

Creating or Modifying a VLAN

To configure a VLAN, you create a VLAN entity, and then bind network interfaces and IP addresses to the VLAN. If you remove a VLAN, its member interfaces are added to the default VLAN.

To create a VLAN by using the command line interface

At the command prompt, type:

add vlan <id> [-aliasName <string>] [-ipv6DynamicRouting (ENABLED|DISABLED)]

Example

> add vlan 2 –aliasName “Network A”
Done

To bind an interface to a VLAN by using the command line interface

At the command prompt, type:

bind vlan <id> -ifnum <slot/port>

Example

> bind vlan 2 -ifnum 1/8
Done

To bind an IP address to a VLAN by using the command line interface

At the command prompt, type:

bind vlan <id> -IPAddress <IPAddress> <netMask>

Example

```
> bind vlan 2 -IPAddress 10.102.29.54 255.255.255.0
 Done
```

To remove a VLAN by using the command line interface

At the command prompt, type:

rm vlan <id>

To configure a VLAN by using the configuration utility

1. Navigate to Network > VLANs, add a new VLAN, or edit an existing VLAN.
2. To bind an IP address to a VLAN, under IP Bindings, select the Active option corresponding to the IP address that you want to bind to the VLAN (for example, 10.102.29.54). The Type column displays the IP address type (such as mapped IP, virtual IP, or subnet IP) for each IP address in the IP Address column.
3. To bind a network interface to a VLAN, under Interface Bindings, select the Active option corresponding to the interface that you want to bind to the VLAN.

Parameter Descriptions (of commands listed in the CLI procedure)

add vlan

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind vlan

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

rm vlan

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Monitoring VLANS

You can display VLAN statistics such as packets received, bytes received, packets sent, and bytes sent, and use the information to identify anomalies and or debug a VLAN.

To view the statistics of a VLAN by using the command line interface

At the command prompt, type:

stat vlan <vlanID>

Example

stat vlan 2

To view the statistics of a VLAN by using the configuration utility

1. Navigate to Network > VLANs.
2. Select the VLAN, and click Statistics.

Parameter Descriptions (of commands listed in the CLI procedure)

stat vlan

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring VLANs in an HA Setup

VLAN configuration for a high-availability setup requires that the NetScaler appliances have the same hardware configuration, and the VLANs configured on them must be mirror images.

The correct VLAN configuration is implemented automatically when the configuration is synchronized between the NetScaler appliances. The result is identical actions on all the appliances. For example, adding network interface 0/1 to VLAN2 adds this network interface to VLAN 2 on all the appliances participating in the high-availability setup.

Note: If you use network-interface-specific commands in an HA setup, the configurations you create are not propagated to the other NetScaler appliance. You must perform these commands on each appliance in an HA pair to ensure that the configuration of the two appliances in the HA pair remains synchronized.

Configuring VLANs on a Single Subnet

Before configuring a VLAN on a single subnet, make sure that Layer 2 Mode is enabled.

The following figure shows a single subnet environment

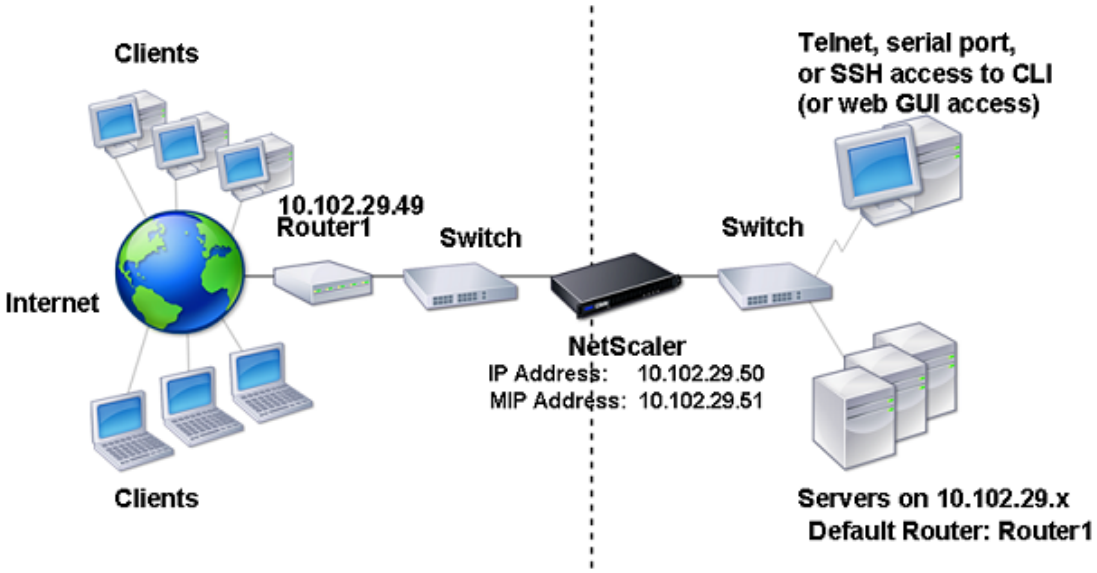


Figure 1. VLAN on a Single Subnet

In the above figure:

1. The default router for the NetScaler and the servers is Router 1.
2. Layer 2 mode must be enabled on the NetScaler for the NetScaler to have direct access to the servers.
3. For this subnet, a virtual server can be configured for load balancing on the NetScaler.

To configure a VLAN on a single subnet, follow the procedures described in "Creating or Modifying a VLAN." VLAN configuration parameters are not required, because the network interfaces are members of this VLAN.

Configuring VLANs on Multiple Subnets

To configure a single VLAN across multiple subnets, you must add a VIP for the VLAN and configure the routing appropriately. The following figure shows a single VLAN configured across multiple subnets.

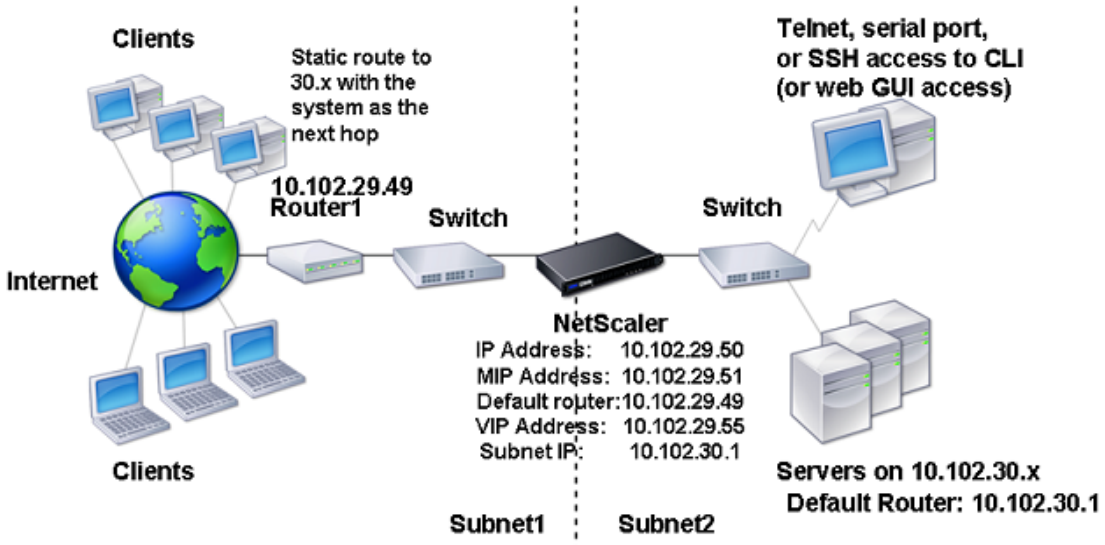


Figure 1. Multiple Subnets in a Single VLAN

To configure a single VLAN across multiple subnets, perform the following tasks:

1. Disable Layer 2 mode. For the procedure to disable Layer 2 mode, see "Enabling and Disabling Layer 2 Mode."

2. Add a VIP.

   For the procedure to add a VIP, see "Configuring and Managing Virtual IP Addresses (VIPs)."

3. Configure RNAT ID.

   For the procedure to configure the RNAT ID, see "Configuring RNAT."

Configuring Multiple Untagged VLANs across Multiple Subnets

In environments with multiple untagged VLANs across multiple subnets, a VLAN is configured for each IP subnet. A network interface is bound to one VLAN only. The following figure shows this configuration.

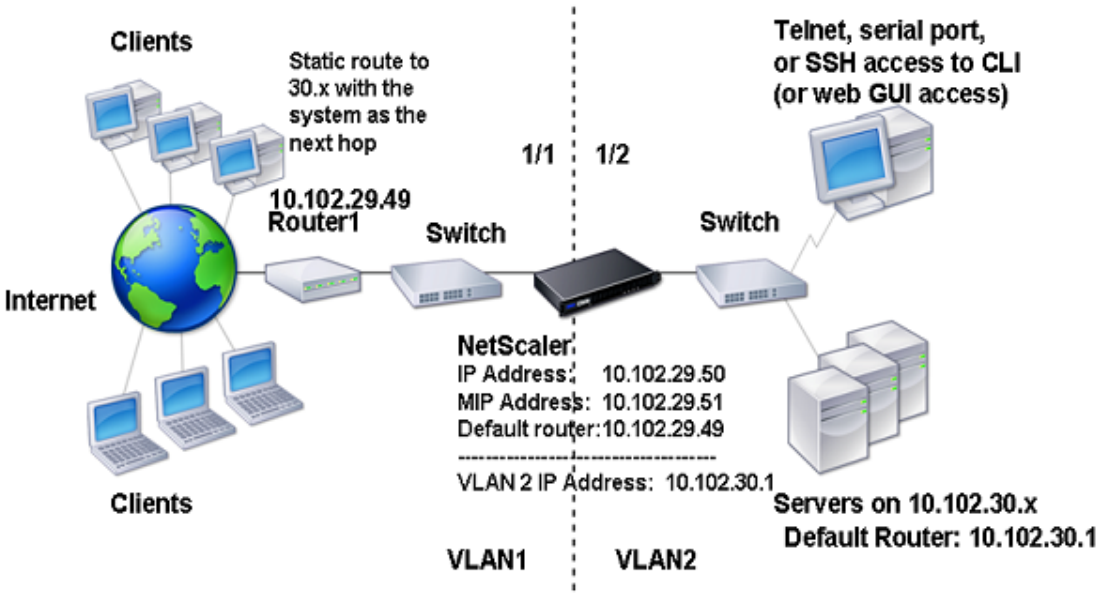


Figure 1. Multiple Subnets with VLANs - No Tagging

To implement the configuration shown in the above figure, perform the following tasks:

1. Add VLAN 2.

   For the procedure to create a VLAN, see "Creating or Modifying a VLAN."

2. Bind the 1/2 network interface of the NetScaler to VLAN 2 as an untagged network interface.

   For the procedure to bind a network interface to a VLAN, see "Creating or Modifying a VLAN."

3. Bind the IP address and subnet mask to VLAN 2.

   For the procedure to bind a network interface to a VLAN, see "Creating or Modifying a VLAN."

Configuring Multiple VLANs with 802.1q Tagging

For multiple VLANs with 802.1q tagging, each VLAN is configured with a different IP subnet. Each network interface is in one VLAN. One of the VLANs is set up as tagged. The following figure shows this configuration.

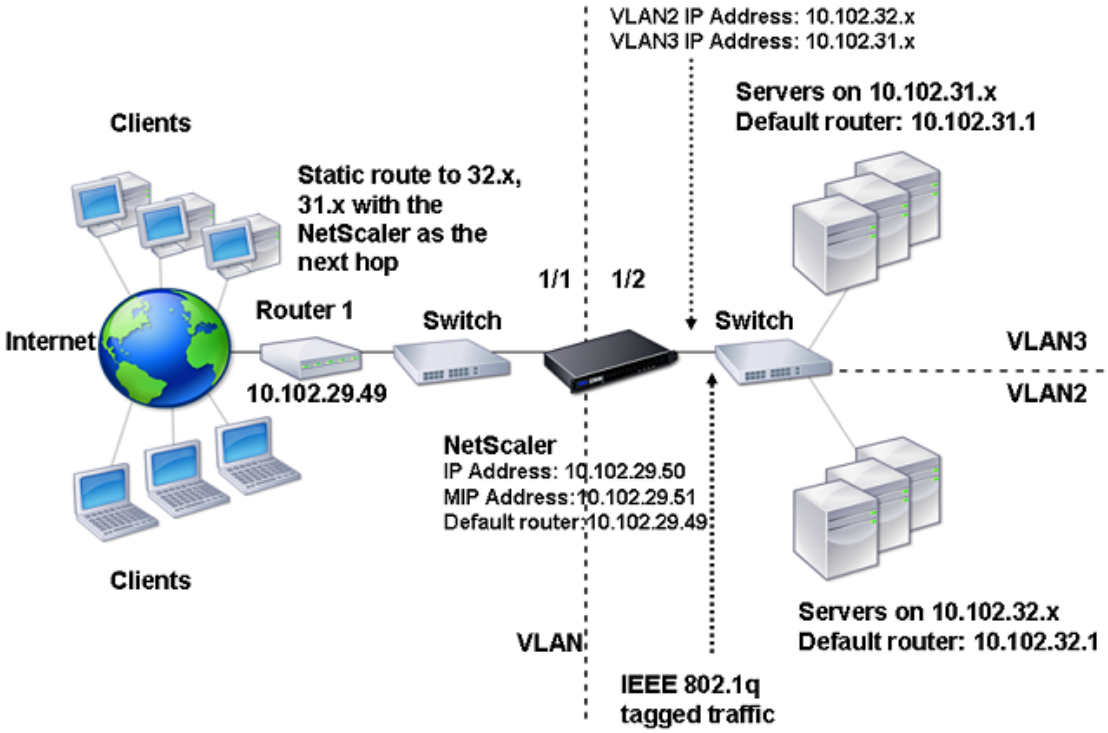


Figure 1. Multiple VLANs with IEEE 802.1q Tagging

To implement the configuration shown in the above figure, perform the following tasks:

1. Add VLAN 2.

   For the procedure to create a VLAN, see "Creating or Modifying a VLAN."

2. Bind the 1/2 network interface of the NetScaler to VLAN 2 as an untagged network interface.

   For the procedure to bind a network interface to a VLAN, see "Creating or Modifying a VLAN."

3. Bind the IP address and netmask to VLAN 2.

   For the procedure to bind an IP address to a VLAN, see "Creating or Modifying a VLAN."

4. Add VLAN 3.

   For the procedure to create a VLAN, see "Creating or Modifying a VLAN."

5. Bind the 1/2 network interface of the NetScaler to VLAN 3 as a tagged network interface.

   For the procedure to bind a network interface to a VLAN, see "Creating or Modifying a VLAN."

   For the procedure to bind a tagged network interface, see "Creating or Modifying a VLAN."

6. Bind the IP address and netmask to VLAN 3.

   For the procedure to bind an IP address to a VLAN, see "Creating or Modifying a VLAN."

Configuring NSVLAN

NSVLAN is a VLAN to which the NetScaler management IP (NSIP) address's subnet is bound. The NSIP subnet is available only on interfaces that are associated with NSVLAN. By default, NSVLAN is VLAN1, but you can designate a different VLAN as NSVLAN. If you do so, you must reboot the NetScaler appliance for the change to take effect. After the reboot, NSIP subnet traffic is restricted to the new NSVLAN.

The traffic from the NetScaler IP subnet can be tagged (802.1q) with the VLAN ID specified for NSVLAN. You must configure the attached switch interface to tag and allow this same VLAN ID on the connected interface.

If you remove your NSVLAN configuration, the NSIP subnet is automatically bound to VLAN1, restoring the default NSVLAN.

To configure NSVLAN by using the command line interface

At the command prompt, type:

- set ns config -nsvlan <positive_integer> -ifnum <interface_name> ... [-tagged (YES|NO)]
- show ns config

Note: The configuration takes effect after the NetScaler appliance is rebooted.

Example

```
> set ns config -nsvlan 300 -ifnum 1/1 1/2 1/3 -tagged NO
 Done

> save config
 Done
```

To restore the default NSVLAN configuration by using the command line interface

At the command prompt, type:

- unset ns config -nsvlan
- show ns config

Example

```
> unset ns config -nsvlan
 Done
```

To configure NSVLAN by using the configuration utility

Navigate to System > Settings, in the Settings group, click Change NSVLAN Settings.

Parameter Descriptions (of commands listed in the CLI procedure)

set ns config

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns config

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

unset ns config

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Bridge Groups

Typically, when you want to merge two or more VLANs into a single domain, you change the VLAN configuration on all the devices in the separate domains. This can be a tedious task. To more easily merge multiple VLANs into a single broadcast domain, you can use bridge groups.

The bridge groups feature works the same way as a VLAN. Multiple VLANS can be bound to a single bridge group, and all VLANs bound to same bridge group form a single broadcast domain. You can bind only Layer 2 VLANs to a bridge group. For Layer 3 functionality, you must assign an IP address to a bridge group.

In Layer 2 mode, a broadcast packet received on an interface belonging to a particular VLAN is bridged to other VLANs that belong to the same bridge group. In the case of a unicast packet, the NetScaler appliance searches its bridge table for the learned MAC addresses of all the VLANs belonging to same bridge group.

In Layer 3 forwarding mode, an IP subnet is bound to a bridge group. The NetScaler accepts incoming packets belonging to the bound subnet and forwards the packets only on VLANs that are bound to the bridge group.

IPv6 routing can be enabled on a configured bridge group.

To add a bridge group and bind VLANs by using the command line interface

To add a bridge group and bind VLANs and verify the configuration, type the following commands:

- add bridgegroup <id> [-ipv6DynamicRouting (ENABLED | DISABLED)]
- show bridgegroup <id>
- bind bridgegroup <id> -vlan <positive_integer>
- show bridgegroup <id>

Example

```
> add bridgegroup 12
 Done
```

To remove a bridge group by using the command line interface

At the command prompt, type:

rm bridgegroup <id>

Example

rm bridgegroup 12

To configure a bridge group by using the configuration utility

Navigate to Network > Bridge Groups, add a new bridge group, or edit an existing bridge group.

Parameter Descriptions (of commands listed in the CLI procedure)

add bridgegroup

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show bridgegroup

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind bridgegroup

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

rm bridgegroup

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring VMACs

The primary and secondary nodes in a high availability (HA) setup share the Virtual MAC address (VMAC) floating entity. The primary node owns the floating IP addresses (such as MIP, SNIP, and VIP) and responds to ARP requests for these IP addresses with its own MAC address. Therefore, the ARP table of an external device, such as an upstream router, is updated with the floating IP address and the MAC address of the primary node.

When a failover occurs, the secondary node takes over as the new primary node. The former secondary node uses Gratuitous ARP (GARP) to advertise the floating IP addresses that it had learned from the old primary node. The MAC address that the new primary node advertises is the MAC address of its own network interface. Some devices (a few routers) do not accept these GARP messages. Therefore, these external devices retain the IP address-to-MAC address mapping that the old primary node had advertised. This can result in a GSLB site going down.

Therefore, you must configure a VMAC on both nodes of an HA pair. This means that both nodes have identical MAC addresses. When a failover occurs, the MAC address of the secondary node remains unchanged, and the ARP tables on the external devices do not need to be updated.

For the procedures to configure a VMAC, see "High Availability."

Configuring Link Aggregation

Link aggregation combines data coming from multiple ports into a single high-speed link. Configuring link aggregation increases the capacity and availability of the communication channel between the NetScaler appliance and other connected devices. An aggregated link is also referred to as a "channel." You can configure the channels manually, or you can use Link Aggregation Control Protocol (LACP). You cannot apply LACP to a manually configured channel, nor can you manually configure a channel created by LACP.

When a network interface is bound to a channel, the channel parameters have precedence over the network interface parameters. (That is, the network interface parameters are ignored.) A network interface can be bound only to one channel.

When a network interface is bound to a channel, it drops its VLAN configuration. When network interfaces are bound to a channel, either manually or by LACP, they are removed from the VLANs that they originally belonged to and added to the default VLAN. However, you can bind the channel back to the old VLAN, or to a new one. For example, if you bind the network interfaces 1/2 and 1/3 to a VLAN with ID 2, and then bind them to a channel LA/1, the network interfaces are moved to the default VLAN, but you can bind them back to VLAN 2.

Configuring Link Aggregation Manually

When you create a link aggregation channel, its state is DOWN until you bind an active interface to it. You can modify a channel at any time. You can remove channels, or you can enable/disable them.

To create a link aggregation channel by using the command line interface

At the command prompt, type:

- add channel <id> [-ifnum <interfaceName> ...] [-state (ENABLED | DISABLED)] [-speed <speed>] [-flowControl <flowControl>] [-haMonitor (ON | OFF)][-tagall (ON | OFF)] [-ifAlias <string>] [-throughput <positive_integer>] [-bandwidthHigh <positive_integer> [-bandwidthNormal <positive_integer>]]
- show channel

Example

add channel LA/1 -ifnum 1/8
show channels

To bind an interface to or unbind an interface from an existing link aggregation channel by using the command line interface

At the command prompt, type one of the following commands:

- bind channel <id> <interfaceName>
- unbind channel <id> <interfaceName>

Example

bind channel LA/1 1/8

To modify a link aggregation channel by using the command line interface

At the command prompt, type the set channel command, the channel ID, and the parameters to be changed, with their new values.

To configure a link aggregation channel by using the configuration utility

Navigate to Network > Channels, add a new channel, or edit an existing channel.

To remove a link aggregation channel by using the command line interface

Important: When a channel is removed, the network interfaces bound to it induce network loops that decrease network performance. You must disable the network interfaces before you remove the channel.

At the command prompt, type:

rm channel <id>

Example

```
> rm channel LA/1
 Done
```

To remove a link aggregation channel by using the configuration utility

Important: When a channel is removed, the network interfaces bound to it induce network loops that decrease network performance. You must disable the network interfaces before you remove the channel.

Navigate to Network > Channels, select the channel that you want to remove and click Remove.

Parameter Descriptions (of commands listed in the CLI procedure)

add channel

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show channel

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind channel

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

unbind channel

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

rm channel

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Link Aggregation by Using the Link Aggregation Control Protocol

The Link Aggregation Control Protocol (LACP) enables network devices to exchange link aggregation information by exchanging LACP Data Units (LACPDUs). Therefore, you cannot enable LACP on network interfaces that are members of a channel that you created manually.

When using LACP to configure link aggregation, you use different commands and parameters for modifying link aggregation channels than you do for creating link aggregation channels. To remove a channel, you must disable LACP on all interfaces that are part of the channel.

Note: In an High Availability configuration, LACP configurations are neither propagated nor synchronized.

Creating Link Aggregation Channels

For creating a link aggregation channel by using LACP, you need to enable LACP and specify the same LACP key on each interface that you want to be the part of the channel. For example, if you enable LACP and set the LACP Key to 3 on interfaces 1/1 and 1/2, a link aggregation channel LA/3 is created and interfaces 1/1 and 1/2 are automatically bound to it.

Note: When enabling LACP on a network interface, you must specify the LACP Key.

By default, LACP is disabled on all network interfaces.

To create an LACP channel by using the command line interface

At the command prompt, type:

- set interface <id> [-lacpMode <lacpMode>] [-lacpKey<positive_integer>] [-lacpPriority <positive_integer>] [-lacpTimeout (LONG | SHORT)]
- show interface [<id>]

To create an LACP channel by using the configuration utility

Navigate to Network > Interfaces, open the network interface, and set the parameters.

Parameter Descriptions (of commands listed in the CLI procedure)

set interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Modifying Link aggregation Channels

After you have created an LACP channel by specifying interfaces, you can modify properties of the channel.

To modify an LACP channel using the command line interface

At the command prompt, type:

- set channel <id> [-ifnum <interfaceName> ...] [-state (ENABLED | DISABLED)] [-speed <speed>] [-flowControl <flowControl>] [-haMonitor (ON | OFF)] [-ifAlias <string>] [-throughput <positive_integer>] [-tagall (ON | OFF)] [-bandwidthHigh <positive_integer> [-bandwidthNormal <positive_integer>]]
- show channel

Example

```
> set channel LA/3 -state ENABLED -speed 10000
 Done
```

To modify an LACP channel by using the configuration utility

Navigate to Network > Channels, and modify an existing LACP channel.

Parameter Descriptions (of commands listed in the CLI procedure)

set channel

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show channel

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Removing a Link Aggregation Channel

To remove a link aggregation channel that was created by using LACP, you need to disable LACP on all the interfaces that are part of the channel.

To remove an LACP channel by using the command line interface

At the command prompt, type:

- set interface <id> -lacpMode Disable
- show interface [<id>]

To remove an LACP channel by using the configuration utility

Navigate to Network > Interfaces, open the network interface, and clear the Enable LACP option.

Parameter Descriptions (of commands listed in the CLI procedure)

set interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

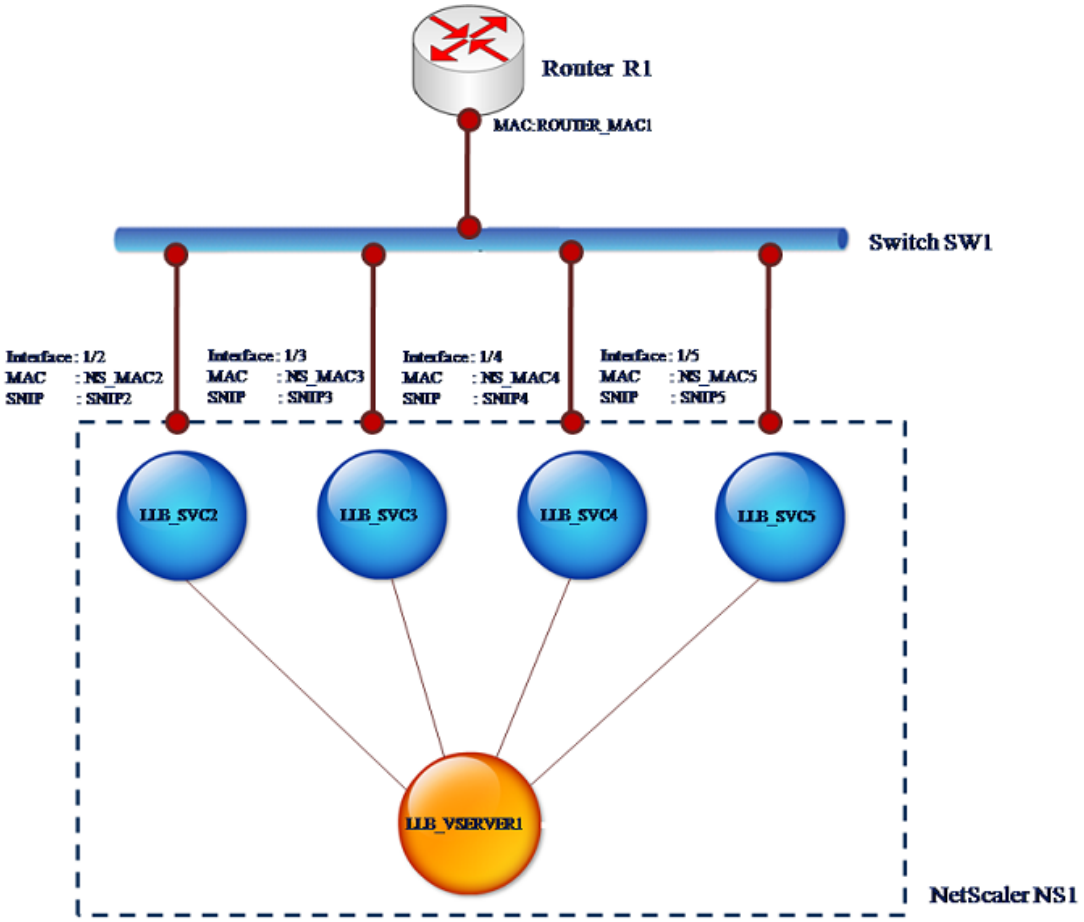
show interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Binding an SNIP address to an Interface

You can now bind a NetScaler owned SNIP address to an interface without using Layer 3 VLANs. Any packets related to the SNIP address will go only through the bound interface.

This feature can be useful in a scenario where the upstream switch does not support Link Aggregation channels and you want the NetScaler appliance to load balance traffic, originated from a server, across the four links to the upstream switch as shown in the following illustration.



The following tables describe the example settings for the scenario:

Entity	Name	Value

SNIP addresses on NS1	SNIP2 (for reference purpose only)	10.10.10.2
	SNIP3 (for reference purpose only)	10.10.10.3
	SNIP4 (for reference purpose only)	10.10.10.4
	SNIP5 (for reference purpose only)	10.10.10.5
LLB virtual server on NS1	LLB_VSERVER1	-
Transparent monitor on NS1	TRANS_MON	-
LLB services on NS1	LLB_SVC2	10.10.10.240
	LLB_SVC3	10.10.10.120
	LLB_SVC4	10.10.10.60
	LLB_SVC5	10.10.10.30
MAC address of interface 1/2 on NS1	NS_MAC_2 (for reference purpose only)	00:e0:ed:0f:bc:e0
MAC address of interface 1/3 on NS1	NS_MAC_3 (for reference purpose only)	00:e0:ed:0f:bc:df
MAC address of interface 1/4 on NS1	NS_MAC_4 (for reference purpose only)	00:e0:ed:0f:bc:de
MAC address of interface 1/5 on NS1	NS_MAC_5 (for reference purpose only)	00:e0:ed:1c:89:53
IP address of Router R1	Router_IP (for reference purpose only)	10.10.10.1
MAC address of interface of R1	ROUTER_MAC1 (for reference purpose only)	00:21:a1:2d:db:cc

To configure the example settings

1. Add four different SNIPs in different subnet ranges. This is for ARP to be resolved on four different links. For more information on creating a SNIP address, see "Configuring Subnet IP Addresses (SNIPs)."

   Command Line Interface example

   ```
   > add ns ip 10.10.10.2 255.255.255.0 -type SNIP
    Done
   > add ns ip 10.10.10.3 255.255.255.128 –type SNIP
   Done
   > add ns ip 10.10.10.4 255.255.255.192 –type SNIP
   Done
   > add ns ip 10.10.10.5 255.255.255.224 –type SNIP
   Done
   ```

2. Add four different dummy services in the added SNIP subnets. This is to ensure that the traffic is sent out with source IP as one of the four configured SNIPs. For more information on creating a service, see "Configuring Services."

   Command Line Interface example

   ```
   > add service LLB_SVC2 10.10.10.240 any *
    Done
   > add service LLB_SVC3 10.10.10.120 any *
    Done
   > add service LLB_SVC4 10.10.10.60 any *
    Done
   > add service LLB_SVC5 10.10.10.30 any *
    Done
   ```

3. Add a transparent ping monitor for monitoring the gateway. Bind the monitor to each of the configured dummy services. This is to make the state of the services as UP. For more information on creating a transparent monitor, see "Creating and Binding a Transparent Monitor."

   Command Line Interface example

   ```
   > add monitor TRANS_MON ping -destIP 10.10.10.1 -transparent YES
    Done
   > bind monitor TRANS_MON LLB_SVC2
    Done
   > bind monitor TRANS_MON LLB_SVC3
    Done
   > bind monitor TRANS_MON LLB_SVC4
    Done
   > bind monitor TRANS_MON LLB_SVC5
    Done
   ```

4. Add a link load balancing (LLB) virtual server and bind the dummy services to it. For more information on creating an LLB virtual server, see "Configuring an LLB Virtual Server and Binding a Service."

   Command Line Interface example

   ```
   > add lb vserver LLB_VSERVER1 any
    Done
   > set lb vserver LLB_VSERVER1 -lbmethod ROUNDROBIN
    Done
   > bind lb vserver LLB_VSERVER1 LLB_SVC2
    Done
   > bind lb vserver LLB_VSERVER1 LLB_SVC2
    Done
   > bind lb vserver LLB_VSERVER1 LLB_SVC2
    Done
   > bind lb vserver LLB_VSERVER1 LLB_SVC2
    Done
   ```

5. Add the LLB virtual server as the default LLB route. For more information on creating an LLB route see "Configuring an LLB Route."

   Command Line Interface example

   ```
   > add lb route 0.0.0.0 0.0.0.0  LLB_VSERVER1
    Done
   ```

6. Add an ARP entry for each of the dummy services with the MAC address of the gateway. This way the gateway is reachable through these dummy services. For more information on adding an ARP entry, see "Configuring Static ARP."

   Command Line Interface example

   ```
   > add arp -ipaddress 10.10.10.240 -mac 00:21:a1:2d:db:cc -ifnum 1/2
    Done
   > add arp -ipaddress 10.10.10.120 -mac 00:21:a1:2d:db:cc -ifnum 1/3
    Done
   > add arp -ipaddress 10.10.10.60 -mac 00:21:a1:2d:db:cc -ifnum 1/4
    Done
   > add arp -ipaddress 10.10.10.30 -mac 00:21:a1:2d:db:cc -ifnum 1/5
    Done
   ```

7. Bind a specific interface to an SNIP by adding an ARP entry for each of these SNIPs. This is to ensure that the response traffic will reach the same interface through which the request went out. For more information on adding an ARP entry, see "Configuring Static ARP."

   Command Line Interface example

```
> add arp -ipAddress 10.10.10.2 -mac 00:e0:ed:0f:bc:e0 -ifnum 1/2
 Done
> add arp -ipAddress 10.10.10.3 -mac 00:e0:ed:0f:bc:df -ifnum 1/3
 Done
> add arp -ipAddress 10.10.10.4 -mac 00:e0:ed:0f:bc:de -ifnum 1/4
 Done
> add arp -ipAddress 10.10.10.5 -mac 00:e0:ed:1c:89:53 -ifnum 1/5
 Done
```

Monitoring the Bridge Table and Changing the Aging time

NetScaler appliance bridges frames on the basis of bridge table lookup of the destination MAC address and the VLAN ID. However, the appliance performs forwarding only when Layer 2 mode is enabled.

The bridge table is dynamically generated, but you can display it, modify the aging time for the bridge table, and view bridging statistics.

All the MAC entries in the bridge table are updated with the aging time.

To change the aging time by using the command line interface

At the command prompt, type:

- set bridgetable -bridgeAge <positive_integer>
- show bridgetable

Example

```
> set bridgetable -bridgeage 70
 Done
```

To change the aging time by using the configuration utility

1. Navigate to Network > Bridge Table.
2. Click Change Ageing Time, and set the Ageing Time (seconds) parameter.

To view the statistics of a bridge table by using the command line interface

At the command prompt, type:

stat bridge

To view the statistics of a bridge table by using the configuration utility

Navigate to Network > Bridge Table, select the MAC address, and click Statistics.

Parameter Descriptions (of commands listed in the CLI procedure)

set bridgetable

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show bridgetable

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

stat bridge

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Understanding NetScaler Appliances in Active-Active Mode Using VRRP

An active-active deployment, in addition to preventing downtime, makes efficient use of all the NetScaler appliances in the deployment. In active-active deployment mode, the same VIPs are configured on all NetScaler appliances in the configuration, but with different priorities, so that a given VIP can be active on only one appliance at a time.

Note: This feature is supported only on NetScaler nCore builds.

The active VIP is called the master VIP, and the corresponding VIPs on the other NetScaler appliances are called the backup VIPs. If a master VIP fails, the backup VIP with the highest priority takes over and becomes the master VIP. All the NetScaler appliances in an active-active deployment use the Virtual Router Redundancy Protocol (VRRP) protocol to advertise their VIPs and the corresponding priorities at regular intervals.

NetScaler appliances in active-active mode can be configured so that no NetScaler is idle. In this configuration, different sets of VIPs are active on each NetScaler. For example, in the following diagram, VIP1, VIP2, VIP3, and VIP4 are configured on appliances NS1, NS2, and NS3. Because of their priorities, VIP1 and VIP 2 are active on NS1, VIP3 is active on NS2 and VIP 4 is active on NS3. If, for example, NS1 fails, VIP1 on NS3 and VIP2 on NS2 become active.

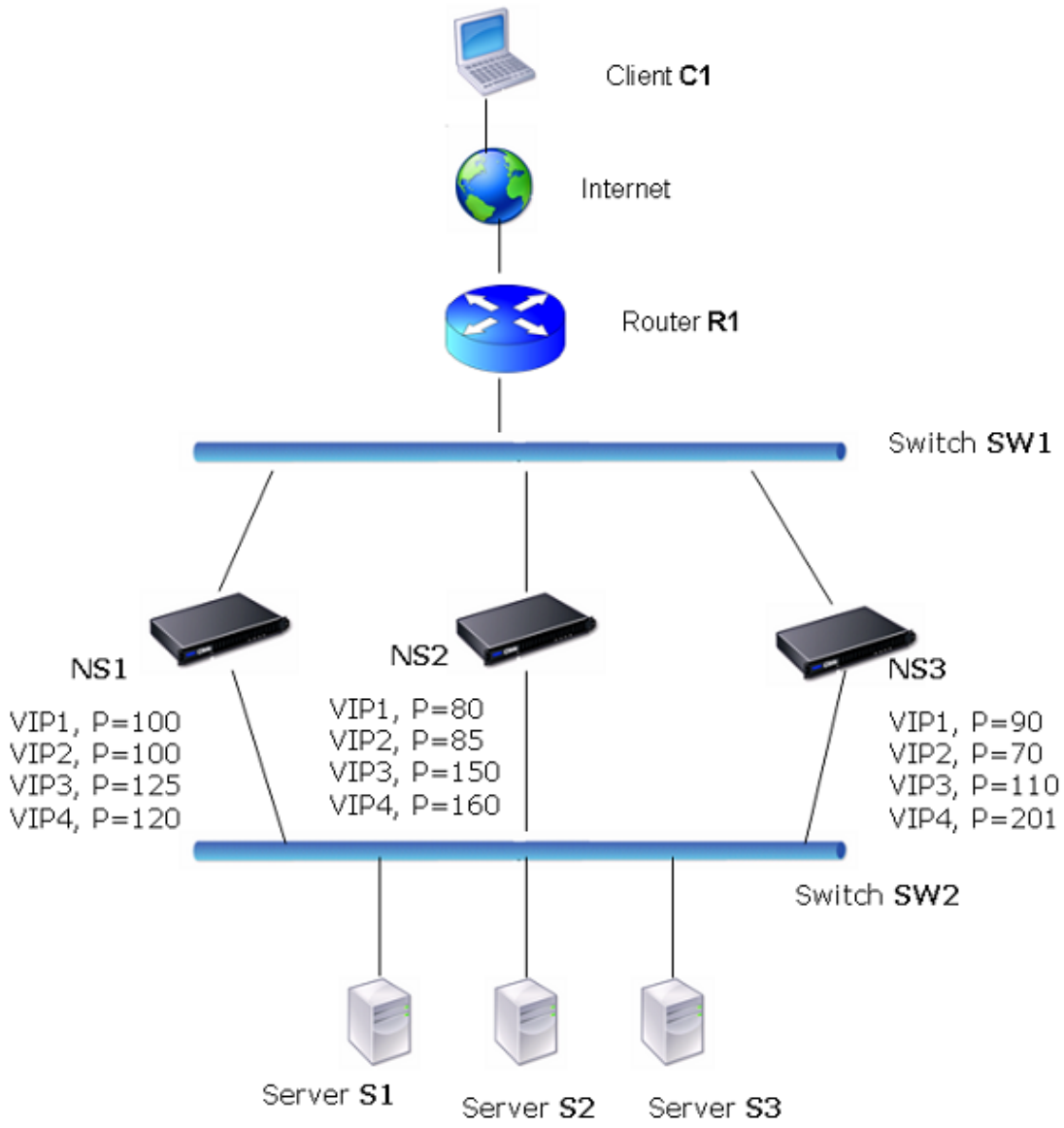


Figure 1. An Active-Active Configuration

The NetScaler appliances in the above diagram process traffic as follows:

1. Client C1 sends a request to VIP1. The request reaches R1.
2. R1 does not have an APR entry for VIP1, so it broadcasts an ARP request for VIP1.
3. VIP1 is active in NS1, so NS1 replies with a source MAC address as the VMAC (for example VMAC1) associated with VIP1, and VIP1 as the source IP address.
4. SW1 learns the port for VIP1 from the ARP reply and updates its bridge table.
5. R1 updates the ARP entry with VMAC1 and VIP1.
6. R1 forwards the packet to the VIP1 on NS1.

7. NS1's load balancing algorithm selects server S2, and NS1 opens a connection between one of its SNIP or MIP addresses and S2.

8. S2 replies to the SNIP or MIP on the NetScaler.

9. NS1 sends S2's reply to the client. In the reply, NS1 inserts MAC address of the physical interface as the source MAC address and VIP1 as the source IP address.

10. Should NS1 fail, the NetScaler appliances use the VRRP protocol to select the VIP1 with the highest priority. In this case, VIP1 on NS3 becomes active, and the following two steps update the active-active configuration.

11. NS3 broadcasts a GARP message for VIP1. In the message, VMAC1 is the source MAC address and VIP1 is the source IP address.

12. SW1 learns the new port for VMAC1 from the GARP broadcast and updates its bridge table to send subsequent client requests for VIP1 to NS3. R1 updates its ARP table.

The priority of a VIP can be modified by health tracking. If you enable health tracking, you should make sure that preemption is also enabled, so that a VIP whose priority is lowered can be preempted by another VIP.

In some situations, traffic might reach a backup VIP. To avoid dropping such traffic, you can enable sharing, on a per-node basis, as you create an active-active configuration. Or you can enable the global send to master option. On a node on which sharing is enabled, it takes precedence over send to master.

Health Tracking

Base priority (BP-range 1-255) ordinarily determines which VIP is the master VIP, but effective priority (EP) can also affect the determination.

For example, if a VIP on NS1 has a priority of 101 and same VIP on NS2 has a priority of 99, the VIP on NS1 is active. However, if two vservers are using the VIP on NS1 and one of them goes DOWN, health tracking can reduce the EP of VIP on NS1. VRRP then makes the VIP on NS2 the active VIP.

Following are the health tracking options for modifying EP:

- **NONE.** No tracking. EP = BP

- **ALL.** If all virtual servers are UP, then EP = BP. Otherwise, EP = 0.

- **ONE.** If at least one virtual server is UP, then EP = BP. Otherwise, EP = 0.

- **PROGRESSIVE.** If ALL virtual servers are UP, then EP = BP. If ALL virtual servers are DOWN then EP = 0. Otherwise EP = BP (1 - K/N), where N is the total number of virtual servers associated with the VIP and k is the number of virtual servers that are down.

Note: If you specify a value other than NONE, preemption should be enabled, so that the backup VIP with the highest priority becomes active if the priority of the master VIP is downgraded.

Preemption

Preemption of an active VIP by another VIP that attains a higher priority is enabled by default, and normally should be enabled. In some cases, however, you may want to disable it. Preemption is a per-node setting for each VIP.

Preemption can occur in the following situations:

- An active VIP goes down and a VIP with a lower priority takes its place. If the VIP with the higher priority comes back online, it preempts the currently active VIP.
- Health tracking causes the priority of a backup VIP to become higher than that of the active VIP. The backup VIP then preempts the active VIP.

Sharing

In the event that traffic reaches a backup VIP, the traffic is dropped unless the sharing option is enabled on the backup VIP. This behavior is a per node setting for each VIP and is disabled by default.

In the figure "An Active-Active Configuration," VIP1 on NS1 is active and VIP1 VIPs on NS2 and NS3 are backups. Under certain circumstances, traffic may reach VIP1 on NS2. If Sharing is enabled on NS2, this traffic is processed instead of dropped.

Configuring Active-Active Mode

On each NetScaler appliance that you want to deploy in active-active mode, you must add a VMAC and bind the VMAC to a VIP. The VMAC for a given VIP must be same on each appliance. For example, if VIP 10.102.29.5, is created on the appliances, a virtual router ID must be created on each NetScaler and bound to VIP 10.102.29.5 on each NetScaler. When you bind a VMAC to a VIP, the NetScaler sends VRRP advertisements to each VLAN that is bound to that VIP. The VMAC can be shared by different VIPs configured on the same NetScaler.

Adding a VMAC

To add a VMAC for an active-active configuration, you create a virtual router ID. To bind a VMAC to a VIP, you associate the VMAC's virtual router ID with the VIP.

To add a VMAC by using the command line interface

At the command prompt, type:

add vrID <value> -priority <value> -preemption (ENABLED|DISABLED) -sharing (ENABLED | DISABLED) -tracking (NONE|ONE|ALL|PROGRESSIVE)

Example

add vrID 125 -priority 100 -sharing ENABLED -tracking ONE

To add a VMAC by using the configuration utility

1. Navigate to Network > VMAC, on the VMAC tab, add a new VMAC, or edit an existing VMAC.
2. Set the following parameters:
   - Virtual Router ID
   - Priority
   - Tracking
   - Preemption
   - Sharing

To bind a VMAC by using the command line interface

At the command prompt, type:

set ns ip <VIP address> -vrid <value>

Example

```
set ns ip 10.102.29.5 -vrid 125
```

To bind a VMAC to a VIP by using the NetScaler configuration utility

1. Navigate to Network > IPs, on the IPV4s tab, open the VIP address that you want to bind to a VMAC.
2. In the Virtual Router Id drop down box, select a virtual router ID.

Parameter Descriptions (of commands listed in the CLI procedure)

add vrID

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

set ns ip

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Send to Master

Usually, the traffic destined to a VIP reaches the NetScaler appliance on which the VIP is active, because an ARP request with the VIP and a VMAC on that appliance has reached the upstream router. But in some cases, such as static routes configured on the upstream router for the VIP subnet, or a topology that blocks this route, the traffic can reach a NetScaler appliance on which the VIP is in backup state. If you want this appliance to forward the data packets to the appliance on which the VIP is active, you need to enable the send to master option. This behavior is a per node setting and is disabled by default.

For example, in the following diagram, VIP1 is configured on NS1, NS2, and NS3 and is active on NS1. Under certain circumstances, traffic for VIP1 (active on NS1) may reach VIP1 on NS3. When the send to master option is enabled on NS3, NS3 forwards the traffic to NS1 through NS2 by using route entries for NS1.

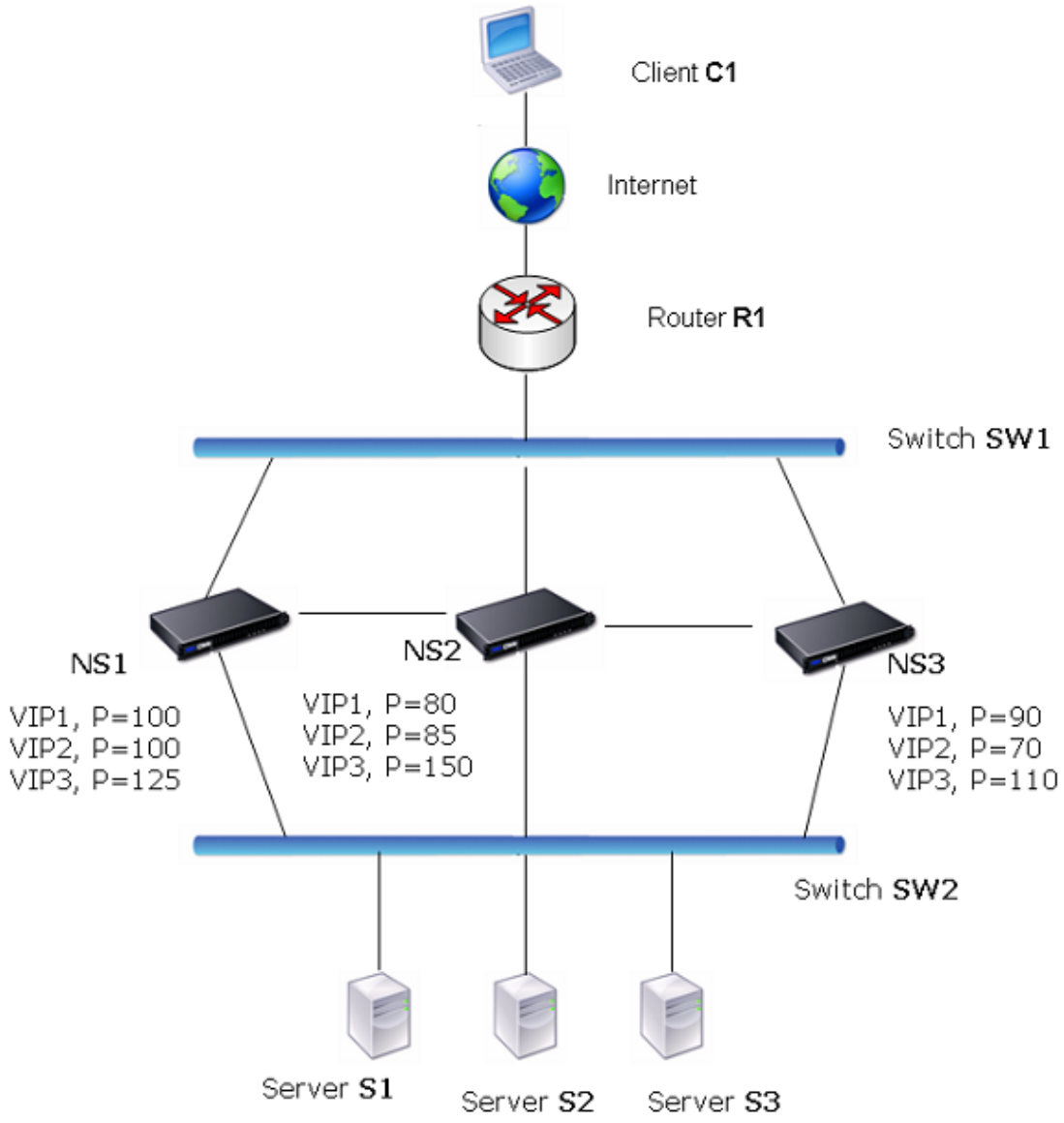


Figure 1. An Active-Active Configuration with Send to Master Option Enabled

To enable send to master by using the command line interface

At the command prompt, type:

set vrIDParam -sendToMaster (ENABLED|DISABLED)

Example

```
> set vrIDParam -sendToMaster ENABLED
 Done
```

To enable send to master by using the configuration utility

1. Select the Send to Master option.

Parameter Descriptions (of commands listed in the CLI procedure)

set vrIDParam

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

An Active-Active Deployment Scenario

Following is an example of a possible active-active deployment scenario.

In the following diagram, VIP1, VIP 2 and VIP3 are configured on all three appliances, NS1, NS2, and NS3. Base Priorities for each VIPs are as shown in the diagram. Health tracking is disabled for each VIP. The priorities of VIPs are set so that VIP1, VIP2, and VIP3 are active on NS3. If NS3 fails, VIP1, VIP2, and VIP3 become active on NS1.

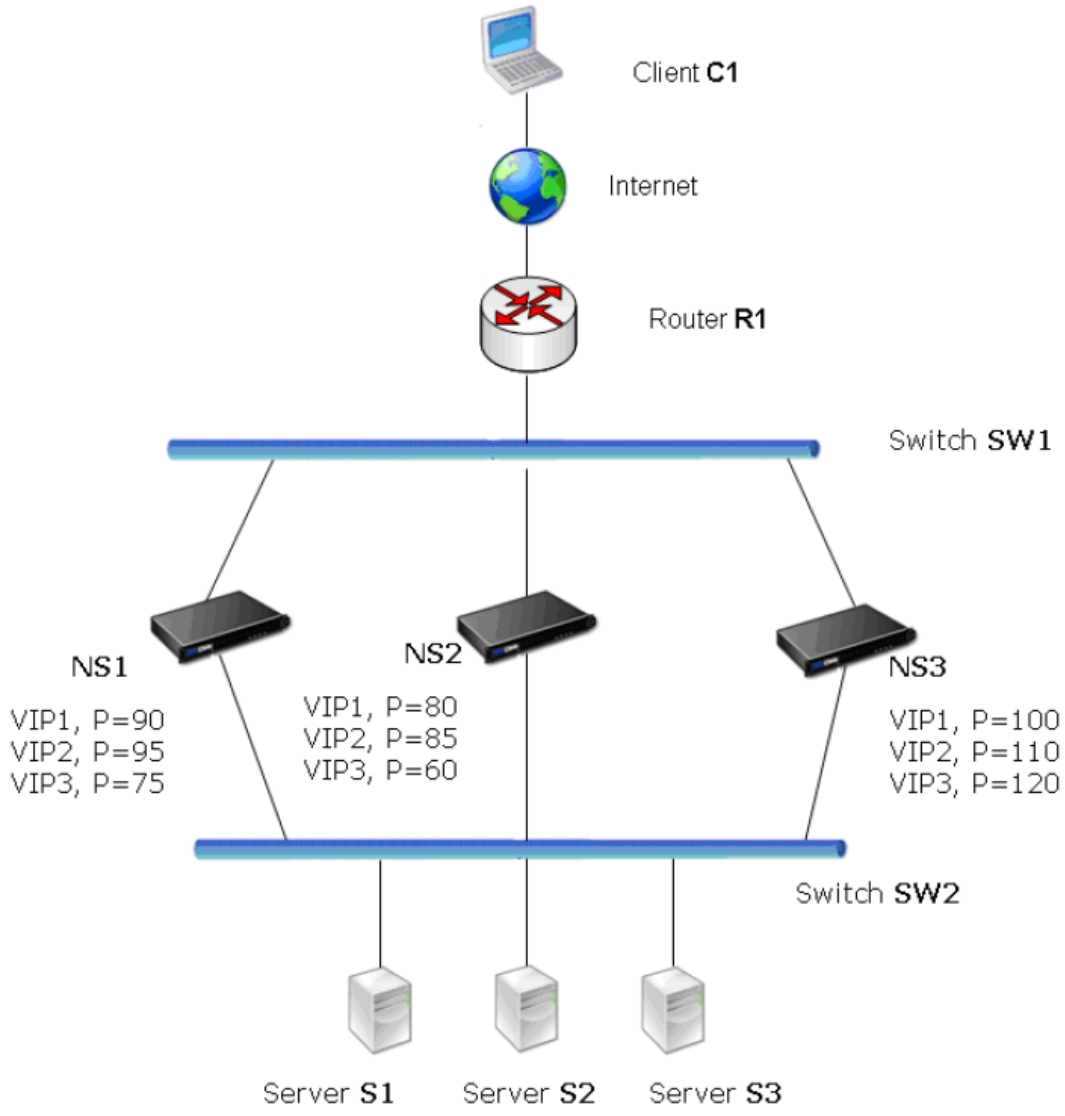


Figure 1. An Active-Active Deployment Scenario

Using the Network Visualizer

The Network Visualizer is a tool that you can use to view the network configuration of a NetScaler node, including the network configuration of the nodes in a high availability (HA) deployment. You can also modify the configuration of VLANs, interfaces, channels, and bridge groups, and perform HA configuration tasks.

In an HA deployment, you can both view and configure network entities on the node to which you are logged on, but you can view the details of only the network entities that are configured on the peer node. However, you can perform certain tasks, such as viewing details and statistics of the peer node and forcing a failover.

When you are logged on to a standalone appliance, you can use the Network Visualizer to do the following:

- View a consolidated graphical summary of key network components, such as VLANs, interfaces, channels, and bridge groups. You can also view the individual details of various network components.
- Modify appliance settings.
- Add, modify, and enable and disable interfaces and channels that are configured on the NetScaler appliance.
- Add and modify VLANs and bridge groups.
- Configure an HA deployment (add a node).
- View node details, node statistics, and statistics for VLANs and interfaces.
- Copy the properties of a network entity to a document or spreadsheet.

When you are logged on to an appliance in an HA deployment, you can perform the above tasks only on the appliance to which you are logged on. Following are additional tasks that you can perform in the Network Visualizer when you are logged on to one of the appliances in an HA pair:

- View the configuration details and high availability details of both nodes in an HA pair.
- Perform HA configuration tasks, such as synchronization and force failover.
- Remove the peer node from the HA configuration.
- View statistics for the peer node.
- Copy the properties of the peer node to a document or spreadsheet.

To open the Network Visualizer

1. In the navigation pane, expand Network.
2. In Monitor Connections, click Network Visualizer.

To locate a VLAN or bridge group in the Visualizer

1. Open the Network Visualizer, and then do the following:
   - To locate a VLAN or bridge group, in the Search text field, begin typing the ID of the VLAN or the bridge group that you want to locate.

     Alternatively, begin typing the IP address of a bound subnet or the ID of a bound interface. The VLANs or bridge groups whose names match the typed characters are highlighted.

     To highlight multiple entities simultaneously, separate the IDs and IP addresses with white spaces. Entities whose IDs or IP addresses match any of the typed IDs and IP addresses are highlighted.
   - To clear the Search field, click the x adjacent to the field.

To modify the network settings of the appliance by using the Visualizer

1. Open the Network Visualizer and click the icon representing the appliance to which you are logged on.
2. In Related Tasks, click Open.

To add a channel by using the Visualizer

1. Open the Network Visualizer and click a network interface.
2. In Related Tasks, click Add Channel.

To add a VLAN by using the Visualizer

1. Open the Network Visualizer, click the appliance to which you are logged on, and then do one of the following:
   - Click an existing VLAN, and then, in Related Tasks, click Add.
   - Click an existing bridge group, and then, in Related Tasks, click Add VLAN.

To add a bridge group by using the Visualizer

1. Open the Network Visualizer, click the appliance to which you are logged on, and then do one of the following:

   - Click an existing bridge group, and then, in Related Tasks, click Add.
   - Click an existing VLAN, and then, in Related Tasks, click Add Bridge Group.

To modify the settings of an interface or channel by using the Visualizer

1. Open the Network Visualizer and click the interface whose settings you want to modify.
2. In Related Tasks, click Open.

To enable or disable an interface or channel by using the Visualizer

1. Open the Network Visualizer and click the interface or channel that you want to enable or disable.
2. In Related Tasks, do one of the following.

   - To enable the interface or channel, click Enable.
   - To disable the interface or channel, click Disable.

To remove a configured channel, VLAN, or bridge group by using the Visualizer

1. Open the Network Visualizer and click the channel, VLAN, or bridge group that you want to remove from the configuration.
2. In Related Tasks, click Remove.

To view statistics for a node, channel, interface, or VLAN by using the Visualizer

1. Open the Network Visualizer and click the node, interface, or VLAN whose statistics you want to view.
2. In Related Tasks, click Statistics.

To set up an HA deployment by using the Visualizer

1. Open the Network Visualizer and click the appliance.
2. In Related Tasks, click HA Setup.

To force the secondary node to take over as the primary by using the Visualizer

1. Open the Network Visualizer and click one of the nodes.
2. In Related Tasks, click Force Failover.

To synchronize the secondary node's configuration with the primary node by using the Visualizer

1. Open the Network Visualizer and click one of the nodes.
2. In Related Tasks, click Force Synchronization.

To remove the peer node from the HA configuration

1. Open the Network Visualizer and click the peer node.
2. In Related Tasks, click Remove.

To copy the properties of a node or network entity by using the Visualizer

1. Open the Network Visualizer and click the appliance or network entity whose properties you want to copy to a document or spreadsheet.
2. In Related Tasks, click Copy Properties.

Access Control Lists

Access Control Lists (ACLs) filter IP traffic and secure your network from unauthorized access. An ACL consists of a set of conditions that the NetScaler® appliance uses to allow or deny access. Consider a small organization that consists of 3 departments, Finance, HR, and Documentation, where no department wants another to access its data. The administrator of the organization can configure ACLs on the NetScaler to allow or deny access. When the NetScaler receives a data packet, it compares the information in the data packet with the conditions specified in the ACL and allows or denies access. The NetScaler supports simple ACLs, extended ACLs, and ACL6s. If both simple and extended ACLs are configured, incoming packets are compared to the simple ACLs first.

Simple ACLs filter packets on the basis of their source IP address and, optionally, their destination port and/or their protocol. Any packet that has the characteristics specified in the ACL is dropped. You can create up to 200,000 simple ACLs.

Extended ACLs filter data packets on the basis of various parameters, such as source IP address, source port, action, and protocol. An extended ACL defines the conditions that a packet must satisfy for the NetScaler to process the packet, bridge the packet, or drop the packet. These actions are known as "processing modes." You can create up to 10,000 extended ACLs.

The processing modes are:

- ALLOW - The NetScaler processes the packet.
- BRIDGE - The NetScaler bridges the packet to the destination without processing it.
- DENY - The NetScaler drops the packet.

The NetScaler processes an IP packet directly when both of the following conditions exist:

- ACLs are configured on the NetScaler.
- The IP packet does not match any of the ACLs.

Simple ACL6s filter IPv6 packets on the basis of their source IPv6 address and, optionally, their destination port and/or their protocol. Any packet that has the characteristics specified in the simple ACL6 is dropped. You can create up to 200,000 simple ACL6s.

ACL6s are ACLs created specifically for IPv6 addresses. ACL6s filter packets on the basis of packet parameters, such as source IP address, source port, action, and so on. An ACL6 defines the condition that a packet must satisfy for the NetScaler to process the packet, bridge the packet, or drop the packet. These actions are known as "processing modes." You can create up to 8,000 ACL6s.

The processing modes are:

- ALLOW - The NetScaler processes the packet.
- BRIDGE - The NetScaler bridges the packet to the destination without processing it.

- DENY - The NetScaler drops the packet.

The NetScaler processes an IP packet directly when both of the following conditions exist:

- ACL6s are configured on the NetScaler.
- The IP packet does not match any of the ACL6s.

ACL Precedence

An IPv4 packet that matches the conditions specified in a simple ACL is dropped. If the packet does not match any simple ACL, the NetScaler compares the packet's characteristics to those specified in any configured extended ACLs. If the packet matches an extended ACL, the NetScaler applies the action specified in the Extended ACL, as shown in the following diagram.

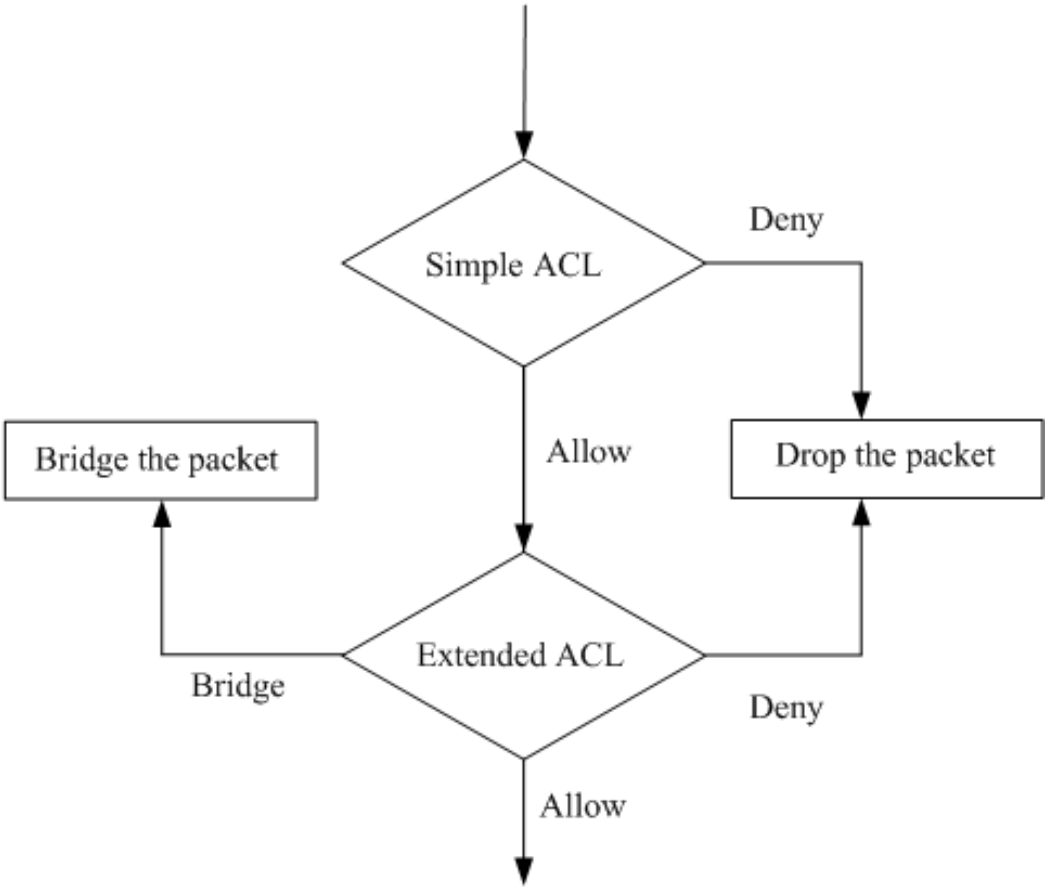


Figure 1. Simple and Extended ACLs Flow Sequence

IPv6 packets are compared only to ACL6s.

Configuring Simple ACLs

A simple ACL, which uses few parameters, cannot be modified once created. When creating a simple ACL, you can specify a time to live (TTL), in seconds, after which the ACL expires. ACLs with TTLs are not saved when you save the configuration. You can also remove a simple ACL manually. You can display simple ACLs to verify their configuration, and you can display statistics to monitor their performance.

Creating Simple ACLs

Use either of the following procedures to create a simple ACL.

To create a simple ACL by using the command line interface

At the command prompt, type the following commands to add an ACL and verify the configuration:

- add ns simpleacl <aclname> DENY -srcIP <ip_addr> [-destPort<port> -protocol (TCP | UDP)] [-TTL <positive_integer>]
- show ns simpleacl [<aclname>]

Example

```
> add simpleacl rule1 DENY -srcIP 10.102.29.5 -TTL 600
 Done
```

To create a simple ACL by using the configuration utility

Navigate to Network > ACLs and, on the Simple ACLs tab, add a new simple ACL.

Parameter Descriptions (of commands listed in the CLI procedure)

add ns simpleacl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns simpleacl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Monitoring Simple ACLs

You can display the simple ACL statistics, which include the number of hits, the number of misses, and the number of simple ACLs configured.

To view simple ACL statistics by using the command line interface

At the command prompt, type:

stat ns simpleacl

Example

```
>stat ns simpleacl

                        Rate (/s)          Total
Deny SimpleACL hits           0                0
SimpleACL hits                0                0
SimpleACL misses              0               11
SimpleACLs count             --                1
 Done
```

The following table describes statistics you can display for simple ACLs.

Table 1. Simple ACL Statistics

Statistic	Indicates
Deny SimpleACL hits	Packets dropped because they match deny simple ACL
SimpleACL hits	Packets matching a simple ACL
SimpleACL misses	Packets not matching any simple ACL
SimpleACL count	Number of simple ACLs configured

To display simple ACL statistics by using the configuration utility

Navigate to Network > ACLs, on the Simple ACLs tab, select the ACL, and click Statistics.

Parameter Descriptions (of commands listed in the CLI procedure)

stat ns simpleacl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Removing Simple ACLs

If you need to modify a simple ACL, you must remove it and create a new one.

To remove a single simple ACL by using the command line interface

At the command prompt, type:

- rm ns simpleacl <aclname>
- show ns simpleacl

To remove all simple ACLs by using the command line interface

At the command prompt, type:

- clear ns simpleacl
- show ns simpleacl

To remove a single simple ACL by using the configuration utility

Navigate to Network > ACLs and, on the Simple ACLs tab, delete the simple ACL.

To remove all simple ACLs by using the configuration utility

Navigate to Network > ACLs and, on the Simple ACLs tab, click Clear.

Parameter Descriptions (of commands listed in the CLI procedure)

rm ns simpleacl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns simpleacl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

clear ns simpleacl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Extended ACLs

To configure extended ACLs, many users first create extended ACLs and then modify them.

For any of the following actions to take effect, they must be applied, by clicking the Commit button:

- Activate
- Remove
- Disable
- Change the Priority

Other actions include:

- Configure logging
- Verify the configuration
- Monitor ACL statistics

Note: If you configure both simple and extended ACLs, simple ACLs take precedence over extended ACLs.

Parameters of Extended ACLs can be configured during creation. Additionally, the following actions can be performed on Extended ACLs: Modify, Remove, Apply, Disable, Enable and Renumber the priority of Extended ACLs.

You can collect statistics of packets using Extended ACLs by enabling logging.

Creating and Modifying an Extended ACL

To create an extended ACL by using the command line interface

At the command prompt, type:

- add ns acl <aclname> <aclaction> [-srcIP [<operator>] <srcIPVal>] [-srcPort [<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-destPort [<operator>] <destPortVal>] [-TTL <positive_integer>] [-srcMac <mac_addr>] [(-protocol <protocol> [-established]) | -protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-icmpType <positive_integer> [-icmpCode <positive_integer>]] [-priority <positive_integer>] [-state (ENABLED | DISABLED)] [-logstate (ENABLED | DISABLED) [-ratelimit <positive_integer>]]

- show ns acl [<aclname>]

Example

```
> add ns acl restrict DENY -srcport 45-1024 -destIP 192.168.1.1 -protocol TCP
 Done
```

To configure an extended ACL by using the configuration utility

Navigate to Network > ACLs and, on the Extended ACLs tab, add a new extended ACL, or edit an existing extended ACL.

Parameter Descriptions (of commands listed in the CLI procedure)

add ns acl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns acl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Applying an Extended ACL

After you create or modify an extended ACL, you must activate it by using one of the following procedures. These procedures reapply all the ACLs.

For example, if you have created the ACLs rule1 through rule10, and then you create an ACL called rule11, and apply it, all of the ACLs (rule1 through rule11) are applied afresh.

If a session has a DENY ACL related to it, that session is terminated.

To apply an ACL by using the command line interface

At the command prompt, type:

- apply ns acls
- show ns acl

To apply an ACL by using the configuration utility

1. Navigate to Network > ACLs.
2. On the Extended ACLs tab, click Apply.

Parameter Descriptions (of commands listed in the CLI procedure)

apply ns acls

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns acl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Disabling and Enabling Extended ACLs

By default, ACLs are enabled. This means when ACLs are applied, the NetScaler appliance compares incoming packets against the ACLs.

Disable an ACL if it will not be used for a certain period. After the ACLs are applied, the NetScaler does not compare incoming packets against disabled ACLs.

To disable or enable an extended ACL by using the command line interface

At the command prompt, type one of the following pairs of commands to disable or enable an ACL and verify the result:

- disable ns acl <aclname>
- show ns acl [<aclname>]
- enable ns acl <aclname>
- show ns acl [<aclname>]

Example

```
> disable ns acl restrict
 Done

> show ns acl restrict
        Name: restrict                  Action: DENY     Hits: 0
        srcIP
        destIP = 192.168.1.1
        srcMac:                      Protocol: TCP
        srcPort =  45-1024               destPort
        Vlan:                        Interface:
        Active Status: DISABLED             Applied Status: NOTAPPLIED
        Priority: 10                 NAT: NO
        TTL:
        Log Status: DISABLED
 Done

> enable ns acl restrict
 Done

> show ns acl restrict
        Name: restrict                  Action: DENY     Hits: 0
        srcIP
        destIP = 192.168.1.1
```

```
        srcMac:                     Protocol: TCP
        srcPort =  45-1024             destPort
        Vlan:                      Interface:
        Active Status: ENABLED             Applied Status: APPLIED
        Priority: 10                NAT: NO
        TTL:
        Log Status: DISABLED
Done
```

To disable or enable an extended ACL by using the configuration utility

1. Navigate to Network > ACLs.
2. On the Extended ACLs tab, select the extended ACL, and click Enable or Disable.

Parameter Descriptions (of commands listed in the CLI procedure)

disable ns acl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns acl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

enable ns acl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Renumbering the priority of Extended ACLs

The renumber procedure resets the priorities of the ACLs to multiples of 10. The priority (an integer value) defines the order in which the NetScaler appliance evaluates ACLs. All priorities are multiples of 10, unless you configure a specific priority to an integer value. When you create an ACL without specifying a priority, the NetScaler automatically assigns a priority that is a multiple of 10.

If a packet matches the condition defined by the ACL, the NetScaler performs an action. If the packet does not match the condition defined by the ACL, the NetScaler compares the packet against the ACL with the next-highest priority.

Consider the following example. Two ACLs, rule1 and rule2, are automatically assigned priorities 20 and 30 when they are created. You need to add a third ACL, rule3, to be evaluated immediately after rule1. Rule3 must have a priority between 20 and 30. In this case, you can specify the priority as 25. Later, you can easily renumber the ACLs with priorities that are multiples of 10, without affecting the order in which the ACLs are applied.

To renumber the ACLs by using the command line interface

At the command prompt, type:

renumber ns acls

To renumber the ACLs by using the configuration utility

Navigate to Network > ACLs and, on the Extended ACLs tab, click Renumber Priority (s).

Parameter Descriptions (of commands listed in the CLI procedure)

renumber ns acls

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Extended ACL Logging

You can configure the NetScaler appliance to log details for packets that match an extended ACL. In addition to the ACL name, the logged details include packet-specific information such as the source and destination IP addresses. The information is stored either in the syslog file or in the nslog file, depending on the type of global logging (syslog or nslog) enabled.

Logging can be enabled at both the global level and the ACL level. The global setting takes precedence.

For more information about enabling logging globally, see "Audit Logging."

To optimize logging, when multiple packets from the same flow match an ACL, only the first packet's details are logged, and the counter is incremented for every packet that belongs to the same flow. A flow is defined as a set of packets that have the same values for the following parameters:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Protocol

If the packet is not from the same flow, or if the time duration is beyond the meantime, a new flow is created. Mean time is the time during which packets of the same flow do not generate additional messages (although the counter is incremented).

Note: The total number of different flows that can be logged at any given time is limited to 10,000.

To configure ACL Logging by using the command line interface

At the command prompt, type the following commands to configure logging and verify the configuration:

- set ns acl <aclName> [-logState (ENABLED | DISABLED)] [-rateLimit <positive_integer>]
- show ns acl [<aclName>]

Example

```
> set ns acl restrict -logstate ENABLED -ratelimit 120
Warning: ACL modified, apply ACLs to activate change

> apply ns acls
Done
```

To configure ACL Logging by using the configuration utility

1. Navigate to Network > ACLs and, on the Extended ACLs tab, open the extended ACL.
2. Set the following parameters:
   - Log State
   - Log Rate Limit

Parameter Descriptions (of commands listed in the CLI procedure)

set ns acl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns acl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Monitoring the Extended ACL

You can display statistics for monitoring the performance of an extended ACL.

To display the statistics of an extended ACL by using the command line interface

At the command prompt, type:

stat ns acl

Example

```
>stat ns acl rule1

ACL: rule1
                          Rate (/s)          Total
Hits for this ACL                 0              0
 Done
```

The following table lists the statistics associated with extended ACLs and their descriptions.

Table 1. Extended ACL Statistics

Statistic	Specifies
Allow ACL hits	Packets matching ACLs with processing mode set to ALLOW. NetScaler processes these packets.
NAT ACL hits	Packets matching a NAT ACL, resulting in a NAT session.
Deny ACL hits	Packets dropped because they match ACLs with processing mode set to DENY.
Bridge ACL hits	Packets matching a bridge ACL, which in transparent mode bypasses service processing.
ACL hits	Packets matching an ACL.
ACL misses	Packets not matching any ACL.

To display the statistics of an extended ACL by using the configuration utility

Navigate to Network > ACLs, on the Extended ACLs tab, select the extended ACL, and click Statistics.

Parameter Descriptions (of commands listed in the CLI procedure)

stat ns acl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Removing Extended ACLs

You can remove a single extended ACL or all extended ACLs.

To remove a single extended ACL by using the command line interface

At the command prompt, type:

- rm ns acl <aclName>
- show ns acl

To remove all extended ACLs by using the command line interface

At the command prompt, type:

- clear ns acls
- show ns acl

To remove a single extended ACL by using the configuration utility

Navigate to Network > ACLs and, on the Extended ACLs tab, delete the extended ACL.

To remove all extended ACLs by using the configuration utility

Navigate to Network > ACLs and, on the Extended ACLs tab, click Clear.

Parameter Descriptions (of commands listed in the CLI procedure)

rm ns acl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns acl

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

clear ns acls

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Simple ACL6s

A simple ACL6, which uses few parameters, cannot be modified once created. Instead, you must remove the simple ACL6 and create a new one. When creating a simple ACL6, you must specify its name, and a source IP address value against which to match packets. Optionally, you can specify a destination port and a time to live (TTL) value. A TTL is the number of seconds after which the simple ACL6 expires. ACL6s with TTLs are not saved when you save the configuration. Simple ACL6s can traverse the extension headers (if present) of all the incoming IPv6 packets to identify the layer 4 protocol and take a specified action.

Creating Simple ACL6s

To create a simple ACL6, you must specify its name and source IP address. You can also specify a destination port and time to live (TTL).

To create a simple ACL6 by using the command line interface

At the command prompt, type the following commands to create a simple ACL6 and verify the configuration:

- add ns simpleacl6 <aclname> DENY -srcIPv6 <ipv6_addr|null> [-destPort<port> -protocol (TCP | UDP)] [-TTL <positive_integer>]
- show ns simpleacl6 [<aclname>]

Example

> add ns simpleacl6 rule1 DENY –srcIPv6 3ffe:192:168:215::82 -destPort 80 -Protocol TCP -TTL 9000
Done

To create a simple ACL6 by using the configuration utility

Navigate to Network > ACLs and, on the Simple ACL6s tab, add a new simple ACL6.

To remove a single simple ACL6 by using the command line interface

At the command prompt, type:

- rm ns simpleacl6 <aclname>

- show ns simpleacl6

To remove all simple ACL6s by using the command line interface

At the command prompt, type:

- clear ns simpleacl6
- show ns simpleacl6

To remove one or all simple ACL6s by using the configuration utility

1. Navigate to Network > ACLs.
2. Do one of the following:
   - On the Simple ACL6s tab, select the simple ACL6, and delete it.
   - To remove all simple ACL6s, click Clear.

Monitoring Simple ACL6s

You can display the following simple ACL6 statistics:

Table 1. Simple ACL6 Statistics

Statistic	Indicates
Deny simpleACL6 hits	Packets dropped because they match a simple deny ACL6
Simple ACL6 hits	Packets matching a simple ACL6
Simple ACL6 misses	Packets not matching any simple ACL6
Simple ACL6 count	Number of simple ACL6s configured

To display simple ACL6 statistics by using the command line interface

At the command prompt, type:

stat ns simpleacl6

To display simple ACL6 statistics by using the configuration utility

Navigate to Network > ACLs, on the Simple ACL6s tab, select the simple ACL6, and click Statistics.

Parameter Descriptions (of commands listed in the CLI procedure)

add ns simpleacl6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

rm ns simpleacl6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

clear ns simpleacl6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns simpleacl6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

stat ns simpleacl6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring ACL6s

ACL6s can be configured during creation. Additionally, the following actions can be performed on ACL6s: Modify, Apply, Disable, Enable, Renumber and Remove the priority of ACL6s. Log files of ACL6s can be configured to collect statistics of packets. If a packet matches the condition defined by the ACL6, the NetScaler performs an action. If the packet does not match the condition defined by the ACL6, the NetScaler compares the packet against the ACL6 with the next-highest priority. ACL6s can traverse the extension headers (if present) of all the incoming IPv6 packets to identify the layer 4 protocol and take a specified action.

Creating and Modifying ACL6s

To create an ACL6 by using the command line interface

At the command prompt, type:

- add ns acl6 <acl6name> <acl6action> [-srcIPv6 [<operator>] <srcIPv6Val>] [-srcPort [<operator>] <srcPortVal>] [-destIPv6 [<operator>] <destIPv6Val>] [-destPort [<operator>] <destPortVal>] [-TTL <positive_integer>] [-srcMac <mac_addr>] [(-protocol <protocol> [-established]) | -protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-icmpType <positive_integer> [-icmpCode <positive_integer>]] [-priority <positive_integer>] [-state (ENABLED | DISABLED)]

- show ns acl6 [<acl6name>]

Example

Example
> add ns acl6 rule6 DENY -srcport 45-1024 -destIPv6 2001::45 -protocol TCP
 Done

To modify or remove an ACL6 by using the command line interface

- To modify an ACL6, type the set ns ACL6 command, the name of the ACL6, and the parameters to be changed, with their new values.

- To remove an ACL6, type the rm ns ACL6 command and the name of the <entity>.

To configure an ACL6 by using the configuration utility

Navigate to Network > ACLs and, on the ACL6s tab, add a new ACL6, or edit an existing ACL6.

Parameter Descriptions (of commands listed in the CLI procedure)

add ns acl6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns acl6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Applying ACL6s

After you create an ACL6, you must activate it. The following procedures reapply all the ACL6s.

For example, if you have created the ACL6s rule1 through rule10, and then you create an ACL6 called rule11 and apply it, all of the ACL6s (rule1 through rule11) are applied afresh.

If a session has a DENY ACL related to it, the session is destroyed.

You must apply one of the following procedures after every action you perform on an ACL6 (for example, after disabling an ACL6). However, you can add or modify more than one ACL6 and apply all of them at the same time.

Note: ACL6s created on the NetScaler do not work until they are applied.

To apply ACL6s by using the command line interface

At the command prompt, type:

apply ns acls6

To apply ACL6s by using the configuration utility

1. Navigate to Network > ACLs.
2. On the ACL6s tab, click Apply.

Parameter Descriptions (of commands listed in the CLI procedure)

apply ns acls6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Enabling and Disabling ACL6s

By default, ACL6s are enabled. Therefore, after the ACL6s are applied, the NetScaler appliance compares incoming packets against the configured ACL6s.

If an ACL6 is not required to be part of the lookup table but needs to be retained in the configuration, it must be disabled before the ACL6s are applied. After the ACL6s are applied, the NetScaler does not compare incoming packets against disabled ACL6s.

To disable or enable an ACL6 by using the command line interface

At the command prompt, type:

- enable ns acl6 <acl6name>
- show ns acl6 [<acl6name>]
- disable ns acl6 <acl6name>
- show ns acl6 [<acl6name>]

Note: ACL6s created on the NetScaler do not work until they are applied.

Example

```
> enable ns acl6 rule6
 Done

> show ns acl6 rule6
      Name: rule6                    Action: DENY
      srcIPv6
      destIPv6 = 2001::45
      srcMac:                      Protocol: TCP
      srcPort =  45-1024               destPort
      Vlan:                       Interface:
      Active Status: ENABLED             Applied Status: NOTAPPLIED
      Priority: 10                 Hits: 0
      TTL:
 Done

> disable ns acl6 rule6
 Done

> show ns acl6 rule6
      Name: rule6                    Action: DENY
      srcIPv6
```

```
        destIPv6 = 2001::45
        srcMac:                      Protocol: TCP
        srcPort =  45-1024               destPort
        Vlan:                       Interface:
        Active Status: DISABLED            Applied Status: NOTAPPLIED
        Priority: 10                Hits: 0
        TTL:
Done
```

To disable or enable an ACL6 by using the configuration utility

1. Navigate to Network > ACLs.
2. On the ACL6s tab, select the ACL6, and click Enable or Disable.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns acl6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns acl6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable ns acl6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Renumbering the Priority of ACL6s

The renumber procedure resets the priorities of the ACL6s to multiples of 10. The priority (an integer value) defines the order in which the NetScaler appliance evaluates ACL6s. All priorities are multiples of 10, unless you configure a specific priority to an integer value. When you create an ACL6 without specifying a priority, the NetScaler automatically assigns a priority that is a multiple of 10.

If a packet matches the condition defined by the ACL6, the NetScaler performs an action. If the packet does not match the condition defined by the ACL6, the NetScaler compares the packet against the ACL6 with the next-highest priority.

Consider the following example. Two ACL6s, rule1 and rule2, are automatically assigned priorities 20 and 30 when they are created. You need to add a third ACL, rule3, to be evaluated immediately after rule1. Rule3 must have a priority between 20 and 30. In this case, you can specify the priority as 25. Later, you can easily renumber the ACL6s with priorities that are multiples of 10, without affecting the order in which the ACL6s are applied.

To renumber the priorities of the ACL6s by using the command line interface

At the command prompt, type:

renumber ns acls6

Example

```
> renumber ns acls6
Done
```

To renumber the priority of ACL6s by using the configuration utility

Navigate to Network > ACLs and, on the ACL6s tab, click Renumber Priority (s).

Parameter Descriptions (of commands listed in the CLI procedure)

renumber ns acls6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Monitoring ACL6s

You can display statistics for monitoring the performance of an ACL6.

To display the statistics for an ACL6s by using the command line interface

At the command prompt, type:

stat ns acl6 <acl6name>

The following table lists the statistics associated with ACL6s and their descriptions.

Table 1. ACL6 Statistics

Statistic	Specifies
Allow ACL6 hits	Packets matching IPv6 ACLs with processing mode set to ALLOW. The NetScaler processes these packets.
NAT ACL6 hits	Packets matching a NAT ACL6, resulting in a NAT session.
Deny ACL6 hits	Packets dropped because they match IPv6 ACLs with processing mode set to DENY.
Bridge ACL6 hits	Packets matching a bridge IPv6 ACL, which in transparent mode bypasses service processing.
ACL6 hits	Packets matching an IPv6 ACL.
ACL6 misses	Packets not matching any IPv6 ACL.

To display the statistics for an ACL6 by using the configuration utility

Navigate to Network > ACLs, on the ACL6s tab, select the ACL6, and click Statistics.

Parameter Descriptions (of commands listed in the CLI procedure)

stat ns acl6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Removing ACL6s

You can remove a single ACL6 or all ACL6s.

To remove an ACL6 by using the command line interface

At the command prompt, type:

- rm ns acl6 <acl6name>
- show ns acl6

To remove all ACL6s by using the command line interface

At the command prompt, type:

clear ns acls6

To remove an ACL6 by using the configuration utility

Navigate to Network > ACLs and, on the ACL6s tab, delete the ACL6.

To remove all ACLs by using the configuration utility

Navigate to Network > ACLs and, on the ACL6s tab, click Clear.

Parameter Descriptions (of commands listed in the CLI procedure)

rm ns acl6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns acl6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

clear ns acls6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Terminating Established Connections

For a simple ACL, the NetScaler appliance blocks any new connections that match the conditions specified in the ACL. The appliance does not block any packets related to existing connections that were established before the ACL was created.

However, you can immediately terminate the established connections by running a flush operation from the command line interface or the configuration utility.

Flush can be useful in the following cases:

- You receive a list of blacklisted IP addresses and want to completely block those IP addresses from accessing the NetScaler appliance. In this case, you create simple ACLs to block any new connections from these IP addresses, and then run flush to terminate any existing connections.
- You want to terminate a large number of connections from a particular network without taking the time to terminate them one by one.

When you run flush, the appliance searches through all of its established connections and terminates those that match conditions specified in any of the simple ACLs configured on the appliance.

Note: If you plan to create more than one simple ACL and flush existing connections that match any of them, you can minimize the effect on performance by first creating all of the simple ACLs and then running flush only once.

To terminate all established IPv4 connections that match any of your configured simple ACLs by using the command line interface

At the command prompt, type:

```
flush simpleacl -estSessions
```

To terminate all established IPv4 connections that match any of your configured simple ACLs by using the configuration utility

Navigate to Network > ACLs and, on the Simple ACLs tab, click Flush.

To terminate all established IPv6 connections that match any of your configured simple ACL6s by using the command line interface

At the command prompt, type:

```
flush simpleacl6 -estSessions
```

To terminate all established IPv6 connections that match any of your configured simple ACL6s by using the configuration utility

Navigate to Network > ACLs and, on the Simple ACL6s tab, click Flush.

IP Routing

NetScaler appliances support both dynamic and static routing. Because simple routing is not the primary role of a NetScaler, the main objective of running dynamic routing protocols is to enable route health injection (RHI), so that an upstream router can choose the best among multiple routes to a topographically distributed virtual server.

Most NetScaler implementations use some static routes to reduce routing overhead. You can create backup static routes and monitor routes to enable automatic switchover in the event that a static route goes down. You can also assign weights to facilitate load balancing among static routes, create null routes to prevent routing loops, and configure IPv6 static routes. You can configure policy based routes (PBRs), for which routing decisions are based on criteria that you specify.

Configuring Dynamic Routes

When a dynamic routing protocol is enabled, the corresponding routing process monitors route updates and advertises routes. Routing protocols enable an upstream router to use the equal cost multipath (ECMP) technique to load balance traffic to identical virtual servers hosted on two standalone NetScaler appliances. Dynamic routing on a NetScaler appliance uses three routing tables. In a high-availability setup, the routing tables on the secondary appliance mirror those on the primary.

The NetScaler supports the following protocols:

- Routing Information Protocol (RIP) version 2
- Open Shortest Path First (OSPF) version 2
- Border Gateway Protocol (BGP)
- Routing Information Protocol next generation (RIPng) for IPv6
- Open Shortest Path First (OSPF) version 3 for IPv6
- ISIS Protocol

You can enable more than one protocol simultaneously.

Routing Tables in the NetScaler

In a NetScaler appliance, the NetScaler kernel routing table, the FreeBSD kernel routing table, and the NSM FIB routing table each hold a different set of routes and serve a different purpose. They communicate with each other by using UNIX routing sockets. Route updates are not automatically propagated from one routing table to another. You must configure propagation of route updates for each routing table.

NS Kernel Routing Table

The NS kernel routing table holds subnet routes corresponding to the NSIP and to each SNIP and MIP. Usually, no routes corresponding to VIPs are present in the NS kernel routing table. The exception is a VIP added by using the `add ns ip` command and configured with a subnet mask other than 255.255.255.255. If there are multiple IP addresses belonging to the same subnet, they are abstracted as a single subnet route. In addition, this table holds a route to the loopback network (127.0.0.0) and any static routes added through the command line interface (CLI). The entries in this table are used by the NetScaler in packet forwarding. From the NetScaler CLI, they can be inspected with the `show route` command.

FreeBSD Routing Table

The sole purpose of the FreeBSD routing table is to facilitate initiation and termination of management traffic (telnet, ssh, etc.). In a NetScaler appliance, these applications are tightly coupled to FreeBSD, and it is imperative for FreeBSD to have the necessary information to handle traffic to and from these applications. This routing table contains a route to the NSIP subnet and a default route. In addition, FreeBSD adds routes of type `WasCloned(W)` when the NetScaler establishes connections to hosts on local networks. Because of the highly specialized utility of the entries in this routing table, all other route updates from the NS kernel and NSM FIB routing tables bypass the FreeBSD routing table. Do not modify it with the `route` command. The FreeBSD routing table can be inspected by using the `netstat` command from any UNIX shell.

Network Services Module (NSM) FIB

The NSM FIB routing table contains the advertisable routes that are distributed by the dynamic routing protocols to their peers in the network. It may contain:

Connected routes

IP subnets that are directly reachable from the NetScaler. Typically, routes corresponding to the NSIP subnet and subnets over which routing protocols are enabled are present in NSM FIB as connected routes.

Kernel routes

All the VIP addresses on which the -hostRoute option is enabled are present in NSM FIB as kernel routes if they satisfy the required RHI Levels. In addition, NSM FIB contains any static routes configured on the NetScaler CLI that have the - advertise option enabled. Alternatively, if the NetScaler is operating in Static Route Advertisement (SRADV) mode, all static routes configured on the NetScaler CLI are present in NSM FIB. These static routes are marked as kernel routes in NSM FIB, because they actually belong to the NS kernel routing table.

Static routes

Normally, any static route configured in VTYSH is present in NSM FIB. If administrative distances of protocols are modified, this may not always be the case. An important point to note is that these routes can never get into the NS kernel routing table.

Learned routes

If the NetScaler is configured to learn routes dynamically, the NSM FIB contains routes learned by the various dynamic routing protocols. Routes learned by OSPF, however, need special processing. They are downloaded to FIB only if the fib-install option is enabled for the OSPF process. This can be done from the router-config view in VTYSH.

High Availability Setup

In a high availability setup, the primary node runs the routing process and propagates routing table updates to the secondary node. The routing table of the secondary node mirrors the routing table on the primary node.

Non-Stop Forwarding

After failover, the secondary node takes some time to start the protocol, learn the routes, and update its routing table. But this does not affect routing, because the routing table on the secondary node is identical to the routing table on the primary node. This mode of operation is known as non-stop forwarding.

Black Hole Avoidance Mechanism

After failover, the new primary node injects all its VIP routes into the upstream router. However, that router retains the old primary node's routes for 180 seconds. Because the router is not aware of the failover, it attempts to load balance traffic between the two nodes. During the 180 seconds before the old routes expire, the router sends half the traffic to the old, inactive primary node, which is, in effect, a black hole.

To prevent this, the new primary node, when injecting a route, assigns it a metric that is slightly lower than the one specified by the old primary node.

Interfaces for Configuring Dynamic Routing

To configure dynamic routing, you can use either the configuration utility or a command-line interface. The NetScaler supports two independent command-line interfaces: the NetScaler CLI and the Virtual Teletype Shell (VTYSH). The NetScaler CLI is the appliance's native shell. VTYSH is exposed by ZebOS. The NetScaler routing suite is based on ZebOS, the commercial version of GNU Zebra.

Note: Citrix recommends that you use VTYSH for all commands except those that can be configured only on the NetScaler CLI. Use of the NetScaler CLI should generally be limited to commands for enabling the routing protocols, configuring host route advertisement, and adding static routes for packet forwarding.

Parameter Descriptions (of commands listed in the CLI procedure)

add ns ip

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show route

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring RIP

Routing Information Protocol (RIP) is a Distance Vector protocol. The NetScaler supports RIP as defined in RFC 1058 and RFC 2453. RIP can run on any subnet.

After enabling RIP, you need to configure advertisement of RIP routes. For troubleshooting, you can limit RIP propagation. You can display RIP settings to verify the configuration.

Enabling and Disabling RIP

Use either of the following procedures to enable or disable RIP. After you enable RIP, the NetScaler appliance starts the RIP process. After you disable RIP, the appliance stops the RIP process.

To enable or disable RIP routing by using the command line interface

At the command prompt, enter one of the following commands to enable or disable RIP:

- enable ns feature RIP
- disable ns feature RIP

To enable or disable RIP routing by using the configuration utility

1. Navigate to System > Settings, in Modes and Features group, click Change advanced features.
2. Select or clear the RIP Routing option.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Advertising Routes

RIP enables an upstream router to load balance traffic between two identical virtual servers hosted on two standalone NetScaler appliances. Route advertisement enables an upstream router to track network entities located behind the NetScaler.

To configure RIP to advertise routes by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Command	Specifies
VTYSH	Display VTYSH command prompt.
`configure terminal`	Enter global configuration mode.
`router rip`	Start the RIP routing process and enter configuration mode for the routing process.
`redistribute static`	Redistribute static routes.
`redistribute kernel`	Redistribute kernel routes.

Example:

```
>VTYSH
NS# configure terminal
NS(config)# router rip
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
```

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Limiting RIP Propagations

If you need to troubleshoot your configuration, you can configure listen-only mode on any given interface.

To limit RIP propagation by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Command	Specifies
VTYSH	Display VTYSH command prompt.
`configure terminal`	Enter global configuration mode.
`router rip`	Start the RIP routing process and enter configuration mode for the routing process.
`passive-interface` < vlan_name>	Suppress routing updates on interfaces bound to the specified VLAN.

Example

>VTYSH
NS# configure terminal
NS(config)# router rip
NS(config-router)# passive-interface VLAN0

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Verifying the RIP Configuration

You can display the routing table and other RIP settings.

To view the RIP settings by using the VTYSH command line

At the command prompt, type the following commands in the following order:

Command	Specifies
VTYSH	Display VTYSH command prompt.
`sh rip`	Display updated RIP routing table.
`sh rip interface <vlan_name>`	Displays RIP information for the specified VLAN.

Example

```
NS# VTYSH
NS# sh rip
NS# sh rip interface VLAN0
```

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring OSPF

The NetScaler supports Open Shortest Path First (OSPF) Version 2 (RFC 2328). The features of OSPF on the NetScaler are:

- If a vserver is active, the host routes to the vserver can be injected into the routing protocols.
- OSPF can run on any subnet.
- Route learning advertised by neighboring OSPF routers can be disabled on the NetScaler.
- The NetScaler can advertise Type-1 or Type-2 external metrics for all routes.
- The NetScaler can advertise user-specified metric settings for VIP routes. For example, you can configure a metric per VIP without special route maps.
- You can specify the OSPF area ID for the NetScaler.
- The NetScaler supports not-so-stubby-areas (NSSAs). An NSSA is similar to an OSPF stub area but allows injection of external routes in a limited fashion into the stub area. To support NSSAs, a new option bit (the N bit) and a new type (Type 7) of Link State Advertisement (LSA) area have been defined. Type 7 LSAs support external route information within an NSSA. An NSSA area border router (ABR) translates a type 7 LSA into a type 5 LSA that is propagated into the OSPF domain. The OSPF specification defines only the following general classes of area configuration:
    - Type 5 LSA: Originated by routers internal to the area are flooded into the domain by AS boarder routers (ASBRs).
    - Stub: Allows no type 5 LSAs to be propagated into/throughout the area and instead depends on default routing to external destinations.

After enabling OSPF, you need to configure advertisement of OSPF routes. For troubleshooting, you can limit OSPF propagation. You can display OSPF settings to verify the configuration.

Enabling and Disabling OSPF

To enable or disable OSPF, you must use either the command line interface or the configuration utility. When OSPF is enabled, the NetScaler starts the OSPF process. When OSPF is disabled, the NetScaler stops the OSPF routing process.

To enable or disable OSPF routing by using the command line interface

At the command prompt, type one of the following commands:

1. enable ns feature OSPF
2. disable ns feature OSPF

To enable or disable OSPF routing by using the configuration utility

1. Navigate to System > Settings, in Modes and Features group, click Change advanced features.
2. Select or clear the OSPF Routing option.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Advertising OSPF Routes

OSPF enables an upstream router to load balance traffic between two identical virtual servers hosted on two standalone NetScaler appliances. Route advertising enables an upstream router to track network entities located behind the NetScaler.

To configure OSPF to advertise routes by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Command	Specifies
VTYSH	Display VTYSH command prompt.
`configure terminal`	Enters global configuration mode.
`router OSPF`	Start OSPF routing process and enter configuration mode for the routing process.
`network A.B.C.D/M area <0-4294967295>`	Enable routing on an IP network.
`redistribute static`	Redistribute static routes.
`redistribute kernel`	Redistribute kernel routes.

Example

```
>VTYSH
NS# configure terminal
NS(config)# router OSPF
NS(config-router)# network 10.102.29.0/24 area 0
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
```

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Limiting OSPF Propagations

If you need to troubleshoot your configuration, you can configure listen-only mode on any given VLAN.

To limit OSPF propagation by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Command	Specifies
VTYSH	Display VTYSH command prompt.
`configure terminal`	Enter global configuration mode.
`router OSPF`	Start OSPF routing process and enters configuration mode for the routing process.
`passive-interface` < vlan_name>	Suppress routing updates on interfaces bound to the specified VLAN.

Example

```
>VTYSH
NS# configure terminal
NS(config)# router OSPF
NS(config-router)# passive-interface VLAN0
```

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Verifying the OSPF Configuration

You can display current OSPF neighbors, and OSPF routes.

To view the OSPF settings by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Command	Specifies
VTYSH	Display VTYSH command prompt.
`sh OSPF neighbor`	Displays current neighbors.
`sh OSPF route`	Displays OSPF routes.

Example

>VTYSH
NS# sh OSPF neighbor
NS# sh OSPF route

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring BGP

The NetScaler appliance supports BGP (RFC 4271). The features of BGP on the NetScaler are:

- The NetScaler advertises routes to BGP peers.
- The NetScaler injects host routes to virtual IP addresses (VIPs), as determined by the health of the underlying virtual servers.
- The NetScaler generates configuration files for running BGP on the secondary node after failover in an HA configuration.
- This protocol supports IPv6 route exchanges.

After enabling BGP, you need to configure advertisement of BGP routes. For troubleshooting, you can limit BGP propagation. You can display BGP settings to verify the configuration.

Prerequisites for IPv6 BGP

Before you begin configuring IPv6 BGP, do the following:

- Make sure that you understand the IPv6 BGP protocol.
- Install the IPv6PT license on the NetScaler appliance.
- After installing the IPv6PT license, enable the IPv6 feature.

Enabling and Disabling BGP

To enable or disable BGP, you must use either the command line interface or the configuration utility. When BGP is enabled, the NetScaler appliance starts the BGP process. When BGP is disabled, the appliance stops the BGP process.

To enable or disable BGP routing by using the command line interface

At the command prompt, type one of the following commands:

- enable ns feature BGP
- disable ns feature BGP

To enable or disable BGP routing by using the configuration utility

1. Navigate to System > Settings, in Modes and Features group, click Change advanced features.
2. Select or clear the BGP Routing option.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Advertising IPv4 Routes

You can configure the NetScaler appliance to advertise host routes to VIPs and to advertise routes to downstream networks.

To configure BGP to advertise IPv4 routes by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Command	Specifies
VTYSH	Display VTYSH command prompt.
`configure terminal`	Enter global configuration mode.
`router BGP` < ASnumber>	BGP autonomous system. < ASnumber> is a required parameter. Possible values: 1 to 4,294,967,295.
`Neighbor` < IPv4 address> remote-as < as-number>	Update the IPv4 BGP neighbor table with the link local IPv4 address of the neighbor in the specified autonomous system.
`Address-family ipv4`	Enter address family configuration mode.
`Neighbor` < IPv4 address> activate	Exchange prefixes for the IPv4 router family between the peer and the local node by using the link local address.
`redistribute kernel`	Redistribute kernel routes.
`redistribute static`	Redistribute static routes.

Example

```
>VTYSH
NS# configure terminal
NS(config)# router BGP 5
NS(config-router)# Neighbor a1bc::102 remote-as 100
NS(config-router)# Address-family ipv4
NS(config-router-af)# Neighbor 10.102.29.170 activate
NS(config-router)# redistribute kernel
NS(config-router)# redistribute static
```

Advertising IPv6 BGP Routes

Border Gateway Protocol (BGP) enables an upstream router to load balance traffic between two identical virtual servers hosted on two standalone NetScaler appliances. Route advertising enables an upstream router to track network entities located behind the NetScaler.

To configure BGP to advertise IPv6 routes by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Command	Specifies
VTYSH	Display VTYSH command prompt.
`configure terminal`	Enter global configuration mode.
`router BGP` < ASnumber>	BGP autonomous system. < ASnumber> is a required parameter. Possible values: 1 to 4,294,967,295.
`Neighbor` < IPv6 address> remote-as < as-number>	Update the IPv6 BGP neighbor table with the link local IPv6 address of the neighbor in the specified autonomous system.
`Address-family ipv6`	Enter address family configuration mode.
`Neighbor` < IPv6 address> activate	Exchange prefixes for the IPv6 router family between the peer and the local node by using the link local address.
`redistribute kernel`	Redistribute kernel routes.
`redistribute static`	Redistribute static routes.

Example

```
>VTYSH
NS# configure terminal
NS(config)# router BGP 5
NS(config-router)# Neighbor a1bc::102 remote-as 100
NS(config-router)# Address-family ipv6
NS(config-router-af)# Neighbor a1bc::102 activate
NS(config-router)# redistribute kernel
NS(config-router)# redistribute static
```

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Verifying the BGP Configuration

You can use VTYSH to display BGP settings.

To view the BGP settings using the VTYSH command line

At the command prompt, type:

VTYSH
You are now in the VTYSH command prompt. An output similar to the following appears:
NS170#
At the VTYSH command prompt, type:
NS170# sh ip BGP
NS170# sh BGP
NS170# sh ip BGP neighbors
NS170# sh ip BGP summary
NS170# sh ip BGP route-map <map-tag>

Configuring IPv6 RIP

IPv6 Routing Information Protocol (RIP) or RIPng is a Distance Vector protocol. This protocol is an extension of RIP to support IPv6. After enabling IPv6 RIP, you need to configure advertisement of IPv6 RIP routes. For troubleshooting, you can limit IPv6 RIP propagation. You can display IPv6 RIP settings to verify the configuration.

Prerequisites for IPv6 RIP

Before you begin configuring IPv6 RIP, do the following:

- Make sure that you understand the IPv6 RIP protocol.
- Install the IPv6PT license on the NetScaler appliance.
- Enable the IPv6 feature.

Enabling IPv6 RIP

You can enable or disable IPv6 RIP by using VTYSH. After you enable IPv6 RIP, the NetScaler starts the IPv6 RIP daemon. After you disable IPv6 RIP, the NetScaler stops the RIP daemon.

To enable IPv6 RIP by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Command	Specifies
VTYSH	Display VTYSH command prompt.
`configure terminal`	Enter global configuration mode.
`ns IPv6-routing`	Start IPv6 dynamic routing daemon.
`interface < vlan_name>`	Enter VLAN configuration mode.
`router ipv6 RIP`	Start IPv6 RIP routing process on the VLAN.

Example

```
> VTYSH
NS# configure terminal
NS(config)# ns IPv6-routing
NS(config)# interface vlan0
NS(config-if)# router ipv6 RIP
```

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Advertising IPv6 RIP Routes

IPv6 RIP enables an upstream router to load balance traffic between two identical vservers hosted on two standalone NetScaler devices. Route advertisement enables an upstream router to track network entities located behind the NetScaler.

To configure IPv6 RIP to advertise IPv6 routes by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Command	Specifies
VTYSH	Display VTYSH command prompt.
`configure terminal`	Enter global configuration mode.
`router ipv6 rip`	Start IPv6 RIP routing process and enter configuration mode for the routing process.
`redistribute static`	Redistribute static routes.
`redistribute kernel`	Redistribute kernel routes.

Example

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 rip
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
```

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Limiting IPv6 RIP Propagations

If you need to troubleshoot your configuration, you can configure the listen-only mode on any given interface.

To limit IPv6 RIP propagation by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Command	Specifies
VTYSH	Display VTYSH command prompt.
`configure terminal`	Enter global configuration mode.
`router ipv6 rip`	Start IPv6 RIP routing process and enter configuration mode for the routing process.
`passive-interface` < vlan_name>	Suppress routing updates on interfaces bound to the specified VLAN.

Example

>VTYSH
NS# configure terminal
NS(config)# router ipv6 rip
NS(config-router)# passive-interface VLAN0

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Verifying the IPv6 RIP Configuration

You can use VTYSH to display the IPv6 RIP routing table and IPv6 RIP information for a specified VLAN.

To view the IPv6 RIP settings by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Commands	Specifies
VTYSH	Display VTYSH command prompt.
`sh ipv6 rip`	Display updated IPv6 RIP routing table.
`sh ipv6 rip interface <vlan_name>`	Display IPv6 RIP information for the specified VLAN.

Example

```
NS# VTYSH
NS# sh ipv6 rip
NS# sh ipv6 rip interface VLAN0
```

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring IPv6 OSPF

IPv6 OSPF or OSPF version 3 (OSPF v3) is a link state protocol that is used to exchange IPv6 routing information. After enabling IPv6 OSPF, you need to configure advertisement of IPv6 OSPF routes. For troubleshooting, you can limit IPv6 OSPF propagation. You can display IPv6 OSPF settings to verify the configuration.

Prerequisites for IPv6 OSPF

Before you begin configuring IPv6 OSPF, do the following:

- Make sure that you understand the IPv6 OSPF protocol.
- Install the IPv6PT license on the NetScaler appliance.
- Enable the IPv6 feature.

Enabling IPv6 OSPF

To enable IPv6 OSPF, you must use the VTYSH command line. When IPv6 OSPF is enabled, the NetScaler appliance starts the IPv6 OSPF daemon. When IPv6 OSPF is disabled, the appliance stops the IPv6 OSPF daemon.

To enable IPv6 OSPF by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Command	Specifies
VTYSH	Display VTYSH command prompt.
`configure terminal`	Enter global configuration mode.
`ns IPv6-routing`	Start IPv6 dynamic routing process.
`interface < vlan_name>`	Enter the VLAN configuration mode.
`ipv6 router OSPF area <area-id>`	Start IPv6 OSPF routing process on a VLAN.

Example

```
>VTYSH
NS# configure terminal
NS(config)# ns IPv6-routing
NS(config)# interface vlan0
NS(config-if)# ipv6 router OSPF area 3
```

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Advertising IPv6 Routes

IPv6 OSPF enables an upstream router to load balance traffic between two identical vservers hosted on two standalone NetScaler devices. Route advertising enables an upstream router to track network entities located behind the NetScaler.

To configure IPv6 OSPF to advertise IPv6 routes by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Commands	Specifies
VTYSH	Display VTYSH command prompt.
`configure terminal`	Enter global configuration mode.
`router ipv6 OSPF`	Start IPv6 OSPF routing process and enter configuration mode for the routing process.
`redistribute static`	Redistribute static routes.
`redistribute kernel`	Redistribute kernel routes.

Example

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 OSPF
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
```

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Limiting IPv6 OSPF Propagations

If you need to troubleshoot your configuration, you use VTYSH to configure listen-only mode on any given VLAN.

To limit IPv6 OSPF propagation by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Commands	Specifies
VTYSH	Display VTYSH command prompt.
`configure terminal`	Enter global configuration mode.
`router ipv6 OSPF`	Start IPv6 OSPF routing process and enter configuration mode for the routing process.
`passive-interface` < vlan_name >	Suppress routing updates on interfaces bound to the specified VLAN.

Example

>VTYSH
NS# configure terminal
NS(config)# router ipv6 OSPF
NS(config-router)# passive-interface VLAN0

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Verifying the IPv6 OSPF Configuration

You use VTYSH to display IPv6 OSPF current neighbors and IPv6 OSPF routes.

To view the IPv6 OSPF settings by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Command	Specifies
VTYSH	Display VTYSH command prompt.
`sh ipv6 OSPF neighbor`	Display current neighbors.
`sh ipv6 OSPF route`	Display IPv6 OSPF routes.

Example

```
>VTYSH
NS# sh ipv6 OSPF neighbor
NS# sh ipv6 OSPF route
```

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring ISIS

The NetScaler appliance supports the Intermediate System-to-Intermediate System (IS-IS or ISIS) dynamic routing protocol. This protocol supports IPv4 as well as IPv6 route exchanges. IS▫IS is a link state protocol and is therefore less prone to routing loops. With the advantages of faster convergence and the ability to support larger networks, ISIS can be very useful in Internet Service Provider (ISP) networks.

Prerequisites for configuring ISIS

Before you begin configuring ISIS, do the following:

- Make sure that you understand the ISIS protocol.
- For IPV6 routes, enable:
  - IPv6 protocol translation feature.
  - IPv6 Dynamic Routing option on the VLANs on which you want to run ISIS protocol.

Enabling ISIS

Use either of the following procedures to enable the ISIS routing feature on the NetScaler appliance.

To enable ISIS routing by using the command line interface

At the command prompt, type:

```
enable ns feature ISIS
```

To enable ISIS routing by using the configuration utility

1. Navigate to System > Settings, in Modes and Features group, click Change advanced features.
2. Select or clear the ISIS Routing option.

Creating an ISIS Routing Process and Starting It on a VLAN

To create an ISIS routing process, you must use the VTYSH command line.

At the command prompt, type the following commands, in the order shown:

Command	Description
VTYSH	Displays VTYSH command prompt.
configure terminal	Enters the global configuration mode.
router ISIS [tag]	Creates an ISIS routing process and configuration mode for the routing process.
net XX....XXXX.YYYY.YYYY.YYYY.00	Specifies a NET value for the routing process, where: · · XX. .. .XXXX is the Area Address (can be 1-13 bytes) · · YYYY.YYYY.YYYY is the System ID (6 bytes) · · 00 is the N-selector (1 byte) A NET value can be 8 to 20 bytes in length. The last byte is always the n-selector, and must be zero. The n-selector indicates that there is no transport entity and means that the packet is for the routing software of the appliance. The six bytes directly preceding the n-selector are the system ID. The system ID length is fixed and cannot be changed. The system ID must be unique throughout each area (Level 1) and throughout the backbone (Level 2). The bytes preceding the system ID are the area ID, which can be from 1 to 13 bytes in length. A maximum of three NETs per routing process are allowed with different area ID, but the system ID should be the same for all NETs.
is-type (level-1|level-1-2|level-2-only)	Sets the ISIS routing process to the specified level of routing. Default: level-1-2.
ns IPv6-routing	Starts the IPv6 dynamic routing daemon.
interface <vlan_name>	Enters the VLAN configuration mode.
ip router ISIS	Enables the ISIS routing process on the VLAN for IPv4 route exchanges.
ipv6 router ISIS	Enables the ISIS routing process on the VLAN for IPv6 route exchanges.

Example

```
> VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# net 15.aabb.ccdd.0097.00
```

```
NS(config-router)# is-type level-1
NS(config-router)# exit
NS(config)# ns IPv6-routing
NS(config)# interface vlan0
NS(config-if)#  ip router isis 11
NS(config-if)# ipv6 router isis 11
```

Advertising Routes

Route advertisement enables an upstream router to track network entities located behind the NetScaler appliance.

To configure ISIS to advertise routes by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Command	Description
VTYSH	Displays the VTYSH command prompt.
configure terminal	Enters the global configuration mode.
router ISIS [tag]	Starts the ISIS routing instance and enter configuration mode for the routing process.
redistribute connected (level-1|level-1-2|level-2)	Redistributes connected routes, where · **level-1** : Redistribute connected routes into Level-1. · **level-1-2** : Redistribute connected routes into Level-1 and Level-2. · **level-2** : Redistribute connected routes into Level-2.
redistribute kernel(level-1|level-1-2|level-2)	Redistributes kernel routes, where: · **level-1** : Redistribute kernel routes into Level-1. · **level-1-2** : Redistribute kernel routes into Level-1 and Level-2. · **level-2** : Redistribute kernel routes into Level-2.

Example

```
>VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# redistribute connected level-1
NS(config-router)# redistribute kernel level-1
```

Limiting ISIS Propagations

If you need to troubleshoot your configuration, you can configure the listen-only mode on any given VLAN.

To limit ISIS propagation by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Command	Description
VTYSH	Displays the VTYSH command prompt.
configure terminal	Enters the global configuration mode.
router isis [tag]	Enters the configuration mode for the routing process.
passive-interface <*vlan_name*>	Suppresses routing updates on interfaces bound to the specified VLAN.

Example

```
>VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# passive-interface VLAN0
```

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Verifying the ISIS Configuration

You can use VTYSH to display the ISIS routing table and ISIS information for a specified VLAN.

To view the ISIS settings by using the VTYSH command line

At the command prompt, type the following commands, in the order shown:

Commands	Description
VTYSH	Displays the VTYSH command prompt.
show ip isis route	Displays updated IPv4 ISIS routing table.
show ipv6 isis route	Displays updated IPv6 ISIS routing table.
sh isis interface <*vlan_name*>	Displays IPv6 ISIS information for the specified VLAN.

Example

```
NS# VTYSH
NS#  show ip isis route
NS#  show ipv6 isis route
NS# sh isis interface VLAN0
```

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Installing Routes to the NetScaler Routing Table

The NetScaler appliance can use routes learned by various routing protocols after you install the routes in the appliance's routing table.

To install various routes to the internal routing table by using the VTYSH command line

At the command prompt, type the following commands as appropriate for the routes that you want to install:

Commands	Specifies
VTYSH	Display VTYSH command prompt.
`configure terminal`	Enter global configuration mode.
`ns route-install Default`	Install IPv4 default routes to the internal routing table.
`ns route-install RIP`	Install IPv4 RIP specific routes to the internal routing table.
`ns route-install BGP`	Install IPv4 BGP specific routes to the internal routing table.
`ns route-install OSPF`	Install IPv4 OSPF specific routes to the internal routing table.
`ns route-install IPv6 Default`	Install IPv6 default routes to the internal routing table.
`ns route-install IPv6 RIP`	Install IPv6 RIP specific routes to the internal routing table.
`ns route-install IPv6 BGP`	Install IPv6 BGP specific routes to the internal routing table.
`ns route-install IPv6 OSPF`	Install IPv6 OSPF specific routes to the internal routing table.

Example

```
>VTYSH
NS# configure terminal
NS# ns route-install Default
NS(config)# ns route-install RIP
NS(config)# ns route-install BGP
NS(config)# ns route-install OSPF
NS# ns route-install IPv6 Default
```

```
NS(config)# ns route-install IPv6 RIP
NS(config)# ns route-install IPv6 BGP
NS(config)# ns route-install IPv6 OSPF
```

Parameter Descriptions (of commands listed in the CLI procedure)

VTYSH

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Static Routes

Static routes are manually created to improve the performance of your network. You can monitor static routes to avoid service disruptions. Also, you can assign weights to ECMP routes, and you can create null routes to prevent routing loops.

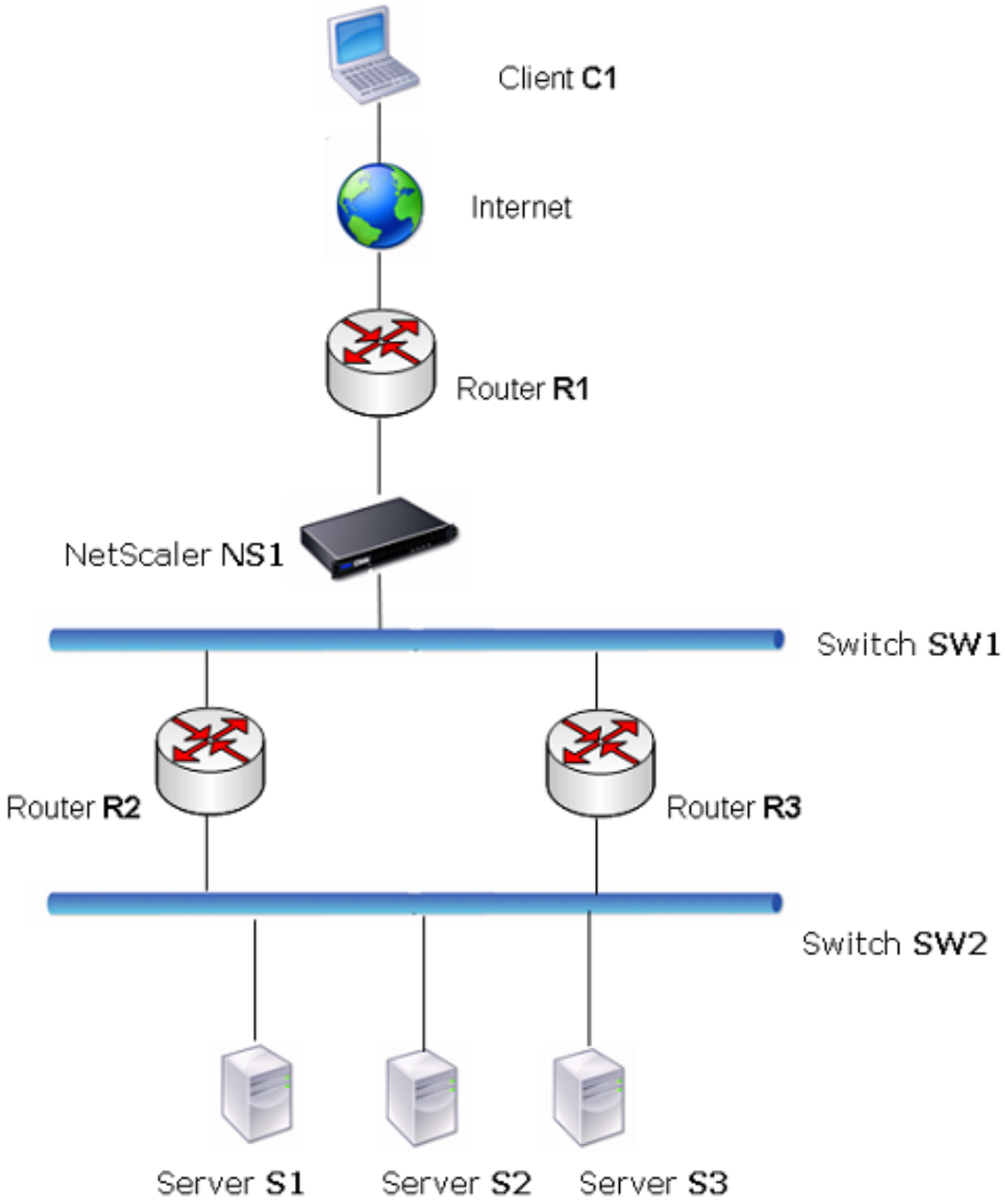
Monitored Static Routes

If a manually created (static) route goes down, a backup route is not automatically activated. You must manually delete the inactive primary static route. However, if you configure the static route as a monitored route, the NetScaler appliance can automatically activate a backup route.

Static route monitoring can also be based on the accessibility of the subnet. A subnet is usually connected to a single interface, but it can be logically accessed through other interfaces. Subnets bound to a VLAN are accessible only if the VLAN is up. VLANs are logical interfaces through which packets are transmitted and received by the NetScaler. A static route is marked as DOWN if the next hop resides on a subnet that is unreachable.

Note: In a high availability (HA) setup, the default value for monitored state routes (MSRs) on the secondary node is UP. The value is set to avoid a state transition gap upon failover, which could result in dropping packets on those routes.

Consider the following simple topology, in which a NetScaler is load balancing traffic to a site across multiple servers.



Router R1 moves traffic between the client and the NetScaler appliance. The appliance can reach servers S1 and S2 through routers R2 or R3. It has two static routes through which to reach the servers' subnet, one with R2 as the gateway and another with R3 as the gateway. Both these routes have monitoring enabled. The administrative distance of the static route with gateway R2 is lower than that of the static route with gateway R3. Therefore, R2 is preferred over R3 to forward traffic to the servers. Also, the default route on the NetScaler points to R1 so that all Internet traffic exits properly.

If R2 fails while monitoring is enabled on the static route, which uses R2 as the gateway, the NetScaler marks it as DOWN. The NetScaler now uses the static route with R3 as the gateway and forwards the traffic to the servers through R3.

The NetScaler supports monitoring of IPv4 and IPv6 static routes. You can configure the NetScaler to monitor an IPv4 static route either by creating a new ARP or PING monitor or by using existing ARP or PING monitors. You can configure the NetScaler to monitor an IPv6 static route either by creating a new Neighbor discovery for IPv6 (ND6) or PING monitor or by using the existing ND6 or PING monitors.

Weighted Static Routes

When the NetScaler appliance makes routing decisions involving routes with equal distance and cost, that is, Equal Cost Multi-Path (ECMP) routes, it balances the load between them by using a hashing mechanism based on the source and destination IP addresses. For an ECMP route, however, you can configure a weight value. The NetScaler then uses both the weight and the hashed value for balancing the load.

Null Routes

If the route chosen in a routing decision is inactive, the NetScaler appliance chooses a backup route. If all the backup routes become inaccessible, the appliance might reroute the packet to the sender, which could result in a routing loop leading to network congestion. To prevent this situation, you can create a null route, which adds a null interface as a gateway. The null route is never the preferred route, because it has a higher administrative distance than the other static routes. But it is selected if the other static routes become inaccessible. In that case, the appliance drops the packet and prevents a routing loop.

Configuring IPv4 Static Routes

You can add a simple static route or a null route by setting a few parameters, or you can set additional parameters to configure a monitored or monitored and weighted static route. You can change the parameters of a static route. For example, you might want to assign a weight to an unweighted route, or you might want to disable monitoring on a monitored route.

To create a static route by using the command line interface

At the command prompt, type the following commands to create a static route and verify the configuration:

- add route <network> <netmask> <gateway>[-cost <positive_integer>] [-advertise (DISABLED | ENABLED)]
- show route [<network> <netmask> [<gateway>]] [<routeType>] [-detail]

Example

```
> add route 10.102.29.0 255.255.255.0 10.102.29.2 -cost 2 -advertise ENABLED
 Done
```

To create a monitored static route by using the command line interface

At the command prompt, type the following commands to create a monitored static route and verify the configuration:

- add route <network> <netmask> <gateway> [-distance <positive_integer>] [-weight <positive_integer>][-msr (ENABLED | DISABLED) [-monitor <string>]]
- show route [<network> <netmask> [<gateway>]] [<routeType>] [-detail]

Example

```
> add route 10.102.29.0 255.255.255.0 10.102.29.3 -distance 5 -weight 6 -msr ENBLED -monitor PING
 Done
```

To create a null route by using the command line interface

At the command prompt type:

- `add route` <network> <netmask> null
- show route <network> <netmask>

Example

```
> add route 10.102.29.0 255.255.255.0 null
 Done
```

To remove a static route by using the command line interface

At the command prompt, type:

rm route <network> <netmask> <gateway>

Example

```
> rm route 10.102.29.0 255.255.255.0 10.102.29.3
 Done
```

To configure a static route by using the configuration utility

Navigate to Network > Routes and, on the Basic tab, add a new static route, or edit an existing static route.

To remove a route by using the configuration utility

Navigate to Network > Routes and, on the Basic tab, delete the static route.

Parameter Descriptions (of commands listed in the CLI procedure)

add route

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show route

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

rm route

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring IPv6 Static Routes

You can configure a maximum of six default IPv6 static routes. IPv6 routes are selected on the basis of whether the MAC address of the destination device is reachable. This can be determined by using the IPv6 Neighbor Discovery feature. Routes are load balanced and only source/destination-based hash mechanisms are used. Therefore, route selection mechanisms such as round robin are not supported. The next hop address in the default route need not belong to the NSIP subnet.

To create an IPv6 route by using the command line interface

At the command prompt, type the following commands to create an IPv6 route and verify the configuration:

- add route6 <network> <gateway> [-vlan <positive_integer>]
- show route6 [<network> [<gateway>]

Example

```
> add route6 ::/0 FE80::67 -vlan 5
 Done
```

To create a monitored IPv6 static route by using the command line interface

At the command prompt, type the following commands to create a monitored IPv6 static route and verify the configuration:

- add route6 <network> <gateway> [-msr (ENABLED | DISABLED) [-monitor <string>]
- show route6 [<network> [<gateway>]

Example

```
> add route6 ::/0 2004::1 -msr ENABLED -monitor PING
 Done
```

To remove an IPv6 route by using the command line interface

At the command prompt, type:

rm route6 <network> <gateway>

Example

```
> rm route6 ::/0 FE80::67
 Done
```

To configure an IPv6 route by using the configuration utility

Navigate to Network > Routes and, on the IPV6 tab, add a new IPv6 route, or edit an existing IPv6 route.

To remove an IPv6 route by using the configuration utility

Navigate to Network > Routes and, on the IPV6 tab, delete the IPv6 route.

Parameter Descriptions (of commands listed in the CLI procedure)

add route6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show route6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

rm route6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring Policy-Based Routes

Policy-based routing bases routing decisions on criteria that you specify. A policy-based route (PBR) specifies criteria for selecting packets and, typically, a next hop to which to send the selected packets. For example, you can configure the NetScaler appliance to route outgoing packets from a specific IP address or range to a particular next hop router. Each packet is matched against each configured PBR, in the order determined by the specified priorities, until a match is found. If no match is found, or if the matching PBR specifies a DENY action, the NetScaler applies the routing table for normal destination-based routing.

A PBR bases routing decisions for the data packets on parameters such as source IP address, source port, destination IP address, destination port, protocol, and source MAC address. A PBR defines the conditions that a packet must satisfy for the NetScaler to route the packet. These actions are known as "processing modes." The processing modes are:

- ALLOW - The NetScaler sends the packet to the designated next-hop router.
- DENY - The NetScaler applies the routing table for normal destination-based routing.

The NetScaler process PBRs before processing the RNAT rules.

You can create PBRs for outgoing IPv4 and IPv6 traffic.

Many users begin by creating PBRs and then modifying them. To activate a new PBR, you must apply it. To deactivate a PBR, you can either remove or disable it. You can change the priority number of a PBR to give it a higher or lower precedence.

Configuring a Policy-Based Routes (PBR) for IPv4 Traffic

Configuring PBRs involves the following tasks:

- Create a PBR.
- Apply PBRs.
- (Optional) Disable or enable a PBR.
- (Optional) Renumber the priority of the PBR.

Creating or Modifying a PBR

You cannot create two PBRs with the same parameters. If you attempt to create a duplicate, an error message appears.

You can configure the priority of a PBR. The priority (an integer value) defines the order in which the NetScaler appliance evaluates PBRs. When you create a PBR without specifying a priority, the NetScaler automatically assigns a priority that is a multiple of 10.

If a packet matches the condition defined by the PBR, the NetScaler performs an action. If the packet does not match the condition defined by the PBR, the NetScaler compares the packet against the PBR with the next highest priority.

Instead of sending the selected packets to a next hop router, you can configure the PBR to send them to a link load balancing virtual server to which you have bound multiple next hops. This configuration can provide a backup if a next hop link fails.

Consider the following example. Two PBRs, p1 and p2, are configured on the NetScaler and automatically assigned priorities 20 and 30. You need to add a third PBR, p3, to be evaluated immediately after the first PBR, p1. The new PBR, p3, must have a priority between 20 and 30. In this case, you can specify the priority as 25.

To create a PBR by using the command line interface

At the command prompt, type:

- add ns pbr <name> <action> [-srcIP [<operator>] <srcIPVal>] [-srcPort [<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-destPort [<operator>] <destPortVal>] [-nextHop <nextHopVal>] [-srcMac <mac_addr>] [-protocol <protocol> |-protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-msr (ENABLED | DISABLED) [-monitor <string>]] [-state (ENABLED | DISABLED)]

- show ns pbr

Example

> add ns pbr pbr1 allow -srcip 10.102.37.252 -destip 10.10.10.2 -nexthop 10.102.29.77
 Done

To modify the priority of a PBR by using the command line interface

At the command prompt, type the following commands to modify the priority and verify the configuration:

- set ns pbr <name> [-action (ALLOW | DENY)] [-srcIP [<operator>] <srcIPVal>] [-srcPort [<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-destPort [<operator>] <destPortVal>] [-nextHop <nextHopVal>] [-srcMac <mac_addr>] [-protocol <protocol> | -protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-msr (ENABLED | DISABLED) [-monitor <string>]] [-state (ENABLED | DISABLED)]

- show ns pbr [<name>]

Example

```
> set ns pbr pbr1 -priority 23
 Done
```

To remove one or all PBRs by using the command line interface

At the command prompt, type one of the following commands:

- rm ns pbr <name>

- clear ns pbrs

Example

```
> rm ns pbr pbr1
 Done
> clear ns PBRs
 Done
```

To create a PBR by using the configuration utility

Navigate to Network > PBRs, on the PBRs tab, add a new PBR, or edit an existing PBR.

To remove one or all PBRs by using the configuration utility

Navigate to Network > PBRs, on the PBRs tab, delete the PBR.

Parameter Descriptions (of commands listed in the CLI procedure)

add ns pbr

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns pbr

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

set ns pbr

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

rm ns pbr

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

clear ns pbrs

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Applying a PBR

You must apply a PBR to activate it. The following procedure reapplies all PBRs that you have not disabled. The PBRs constitute a memory tree (lookup table). For example, if you create 10 PBRs (p1 - p10), and then you create another PBR (p11) and apply it, all of the PBRs (p1 - p11) are freshly applied and a new lookup table is created. If a session has a DENY PBR related to it, the session is destroyed.

You must apply this procedure after every modification you make to any PBR. For example, you must follow this procedure after disabling a PBR.

Note: PBRs created on the NetScaler appliance do not work until they are applied.

To apply a PBR by using the command line interface

At the command prompt, type:

apply ns PBRs

To apply a PBR by using the configuration utility

1. Navigate to Network > PBRs.
2. On the PBRs tab, select the PBR, and click Apply.

Parameter Descriptions (of commands listed in the CLI procedure)

apply ns PBRs

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Enabling or Disabling PBRs

By default, the PBRs are enabled. This means that when PBRs are applied, the NetScaler appliance automatically compares incoming packets against the configured PBRs. If a PBR is not required in the lookup table, but it needs to be retained in the configuration, it must be disabled before the PBRs are applied. After the PBRs are applied, the NetScaler does not compare incoming packets against disabled PBRs.

To enable or disable a PBR by using the command line interface

At the command prompt, type one of the following commands:

- enable ns pbr <name>
- disable ns pbr <name>

Examples

```
> enable ns PBR pbr1
 Done
> show ns PBR pbr1
1)      Name: pbr1
        Action: ALLOW                   Hits: 0
        srcIP = 10.102.37.252
        destIP = 10.10.10.2
        srcMac:                      Protocol:
        Vlan:                       Interface:
        Active Status: ENABLED              Applied Status: APPLIED
        Priority: 10
        NextHop: 10.102.29.77

 Done

> disable ns PBR pbr1
Warning: PBR modified, use 'apply pbrs' to commit this operation
> apply pbrs
 Done
> show ns PBR pbr1
1)      Name: pbr1
        Action: ALLOW                   Hits: 0
        srcIP = 10.102.37.252
        destIP = 10.10.10.2
        srcMac:                      Protocol:
        Vlan:                       Interface:
        Active Status: DISABLED             Applied Status: NOTAPPLIED
        Priority: 10
```

```
        NextHop: 10.102.29.77
Done
```

To enable or disable a PBR by using the configuration utility

1. Navigate to Network > PBRs.
2. On the PBRs tab, select the PBR, and click Enable or Disable.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns pbr

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable ns pbr

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Renumbering PBRs

You can automatically renumber the PBRs to set their priorities to multiples of 10.

To renumber PBRs by using the command line interface

At the command prompt, type:

renumber ns pbrs

To renumber PBRs by using the configuration utility

Navigate to Network > PBRs, on the PBRs tab, and click Renumber Priority (s).

Parameter Descriptions (of commands listed in the CLI procedure)

renumber ns pbrs

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Use Case - PBR with Multiple Hops

Consider a scenario in which two PBRs, PBR1 and PBR2, are configured on NetScaler appliance NS1. PBR1 routes all the outgoing packets, with source IP address as 10.102.29.30, to next hop router R1. PBR2 routes all the outgoing packets, with source IP address as 10.102.29.90, to next hop router R2. R3 is another next hop router connected to NS1.

If router R1 fails, all the outgoing packets that matched against PBR1 are dropped. To avoid this situation, you can specify a link load balancing (LLB) virtual server in the next hop field while creating or modifying a PBR. Multiple next hops are bound to the LLB virtual server as services (for example R1, R2, and R3). Now, if R1 fails, all the packets that matched against PBR1 are routed to R2 or R3 as determined by the LB method configured on the LLB virtual server.

The NetScaler appliance throws an error if you attempt to create a PBR with an LLB virtual server as the next hop in the following cases:

- Adding another PBR with the same LLB virtual server.
- Specifying a nonexistent LLB virtual server.
- Specifying an LLB virtual server for which the bound services are not next hops.
- Specifying an LLB virtual server for which the LB method is not set to one of the following:
  - LEASTPACKETS
  - LEASTBANDWIDTH
  - DESTIPHASH
  - SOURCEIPHASH
  - WEIGHTDRR
  - SRCIPDESTIP_HASH
  - LTRM
  - CUSTOM LOAD
- Specifying an LLB virtual server for which the LB persistence type is not set to one of the following:
  - DESTIP
  - SOURCEIP
  - SRCDSTIP

The following table lists the names and values of the entities configured on the NetScaler appliance:

Table 1. Sample Values for Creating Entities

Entity Type	Name	IP Address
Link load balancing virtual server	LLB1	NA
Services (next hops)	Router1	1.1.1.254
	Router2	2.2.2.254
	Router3	3.3.3.254
PBRs	PBR1	NA
	PBR2	NA

To implement the configuration described above, you need to:

1. Create services Router1, Router2, and Router3 that represent next hop routers R1, R2, and R3.
2. Create link load balancing virtual server LLB1 and bind services Router1, Router2, and Router3 to it.
3. Create PBRs PBR1 and PBR2, with next hop fields set as LLB1 and 2.2.2.254 (IP address of the router R2), respectively.

To create a service by using the command line interface

At the command prompt, type:

- add service <name> <IP> <serviceType> <port>
- show service <name>

Example

```
> add service Router1 1.1.1.254 ANY *
 Done
> add service Router2 2.2.2.254 ANY *
 Done
> add service Router3 3.3.3.254 ANY *
 Done
```

To create a service by using the configuration utility

Navigate to Traffic Management > Load Balancing > Services, and create a service.

To create a link load balancing virtual server and bind a service by using the command line interface

At the command prompt, type:

- add lb vserver <name> <serviceType>
- bind lb vserver < name> <serviceName>
- show lb vserver < name>

Example

```
> add lb vserver LLB1 ANY
 Done
> bind lb vserver LLB1 Router1 Router2 Router3
 Done
```

To create a link load balancing virtual server and bind a service by using the configuration utility

1. Navigate to Traffic Management > Load Balancing > Virtual Servers, and create a virtual server for link load balancing. Specify **ANY** in the **Protocol** field.

   Note: Make sure that **Directly Addressable** is unchecked.

2. Under the **Services** tab, in the **Active** column, select the check box for the service that you want to bind to the virtual server.

To create a PBR by using the command line interface

At the command prompt, type:

- add ns pbr <name> <action> [-srcIP [<operator>] <srcIPVal>] [-nextHop <nextHopVal>]
- show ns pbr

Example

```
> add pbr PBR1 ALLOW -srcIP 10.102.29.30 -nextHop LLB1
 Done
> add pbr PBR2 ALLOW -srcIP 10.102.29.90 -nextHop 2.2.2.254
 Done
```

To create a PBR by using the configuration utility

Navigate to Network > PBRs, on the PBRs tab, add a new PBR.

Parameter Descriptions (of commands listed in the CLI procedure)

add service

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show service

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add ns pbr

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns pbr

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring a Policy-Based Routes (PBR6) for IPv6 Traffic

Configuring PBR6s involves the following tasks:

- Create a PBR6.
- Apply PBR6s.
- (Optional) Disable or enable a PBR6.
- (Optional) Renumber the priority of the PBR6.

Creating or Modifying a PBR6

You cannot create two PBR6s with the same parameters. If you attempt to create a duplicate, an error message appears.

You can configure the priority of a PBR6. The priority (an integer value) defines the order in which the NetScaler appliance evaluates PBR6s. When you create a PBR6 without specifying a priority, the NetScaler automatically assigns a priority that is a multiple of 10.

If a packet matches the condition defined by the PBR6, the NetScaler performs an action. If the packet does not match the condition defined by the PBR6, the NetScaler compares the packet against the PBR6 with the next highest priority.

To create a PBR6 by using the command line interface

At the command prompt, type:

- add ns pbr6 <name> <action> [-srcIPv6 [<operator>] <srcIPv6Val>] [-srcPort [<operator>] <srcPortVal>] [-destIPv6 [<operator>] <destIPv6Val>] [-destPort [<operator>] <destPortVal>] [-srcMac <mac_addr>] [-protocol <protocol> |-protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-state (ENABLED | DISABLED)] [-msr (ENABLED | DISABLED) [-monitor <string>]] [-nextHop <nextHopVal>] [-nextHopVlan <positive_integer>]
- show ns pbr

To modify or remove a PBR6 by using the command line interface

To modify a PBR6, type the set pbr6 <name> command and the parameters to be changed, with their new values.

To remove one or all PBR6s by using the command line interface

At the command prompt, type one of the following commands:

- rm ns pbr6 <name>
- clear ns pbr6

To create or modify a PBR6 by using the configuration utility

Navigate to Network > PBRs and, on the PBR6s tab, add a new PBR6, or edit an existing PBR6.

To remove one or all PBR6s by using the configuration utility

Navigate to Network > PBRs > PBR6s and, on the PBR6s tab, delete the PBR6.

Parameter Descriptions (of commands listed in the CLI procedure)

add ns pbr6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns pbr

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

rm ns pbr6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

clear ns pbr6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Applying PBR6s

You must apply a PBR6 to activate it. The following procedure reapplies all PBR6s that you have not disabled. The PBR6s constitute a memory tree (lookup table). For example, if you create 10 PBR6s (p6_1 - p6_10), and then you create another PBR6 (p6_11) and apply it, all of the PBR6s (p6_1 - p6_11) are freshly applied and a new lookup table is created. If a session has a DENY PBR6 related to it, the session is destroyed.

You must apply this procedure after every modification you make to any PBR6. For example, you must follow this procedure after disabling a PBR6.

Note: PBR6s created on the NetScaler appliance do not work until they are applied.

To apply PBR6s by using the command line interface

At the command prompt, type:

apply ns PBR6

To apply PBR6s by using the configuration utility

1. Navigate to Network > PBRs.
2. On the PBR6s tab, select the PBR6, and click Apply.

Parameter Descriptions (of commands listed in the CLI procedure)

apply ns PBR6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Enabling or Disabling a PBR6

By default, the PBR6s are enabled. This means that when PBR6s are applied, the NetScaler appliance automatically compares outgoing IPv6 packets against the configured PBR6s. If a PBR6 is not required in the lookup table, but it needs to be retained in the configuration, it must be disabled before the PBR6s are applied. After the PBR6s are applied, the NetScaler does not compare incoming packets against disabled PBR6s.

To enable or disable a PBR6 by using the command line interface

At the command prompt, type one of the following commands:

- enable ns pbr <name>
- disable ns pbr <name>

To enable or disable a PBR6 by using the configuration utility

1. Navigate to Network > PBRs.
2. On the PBR6s tab, select the PBR6, and click Enable or Disable.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns pbr

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable ns pbr

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Renumbering PBR6s

You can automatically renumber the PBR6s to set their priorities to multiples of 10.

To renumber PBR6s by using the command line interface

At the command prompt, type:

renumber ns pbr6

To renumber PBR6s by using the configuration utility

Navigate to Network > PBRs, on the PBR6s tab, click Renumber Priority (s).

Parameter Descriptions (of commands listed in the CLI procedure)

renumber ns pbr6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Troubleshooting Routing Issues

To make your troubleshooting process as efficient as possible, begin by gathering information about your network. You need to obtain the following information about the NetScaler appliance and other systems in the Network:

- Complete Topology diagram, including interface connectivity and intermediate switch details.
- Running Configuration. You can use the `show running` command to get the running configuration for ns.conf and ZebOS.conf.
- Output of the `History` command, to determine whether any configuration changes were made when the issue arose.
- Output of the `Top` and `ps -ax` commands, to determine whether any routing daemon is over utilizing the CPU or is misbehaving.
- Any routing related core files in /var/core - nsm, bgpd, ospfd, or ripd. Check the time stamp to see if they are relevant.
- dr_error.log and dr_info.log files from /var/log.
- Output of the `date` command and time details for all relevant systems. Print dates across all devices one after another, so that the times on the log messages can be correlated with various events.
- Relevant ns.log, newnslog files.
- Configuration files, log files and command history details from upstream and downstream routers.

Generic Routing FAQs

Users typically have the following questions about how to troubleshoot generic routing issues:

- How do I save the config files?

  The `write` command from VTYSH saves only ZebOS.conf. Run the save ns config command from NetScaler CLI to save both ns.conf and ZebOS.conf files.

- If I have configured both a static default route and a dynamically learned default route, which is the preferred default route?

  The dynamically learned route is the preferred default route. This behavior is unique to default routes. However, in case of the Network Services Module (NSM), unless the administrative distances are modified, a statically configured route in the RIB is preferred over a dynamic route. The route that is downloaded to the NSM FIB is the static route.

- How do I block the advertisement of default routes?

  After release 7.0, the default route is not injected into ZebOS.

  However, if you are working with 7.0 or an earlier release, you must apply a suitable route map with the

  However, if you are working with 7.0 or an earlier release, you must apply a suitable route map with the `redistribute kernel` command for each protocol to block default route advertisement. For example:

```
ns(config)#access-list 1 deny 0.0.0.0
ns(config)#access-list 2 permit any
ns(config)#route-map redist-kernel permit 5
ns(config-route-map)#match ip address 1
ns(config)#route-map redist-kernel permit 10
ns(config-route-map)#match ip address 2
ns(config-route-map)#q
ns(config)#router ospf 1
ns(config-router)#redistribute kernel route-map redist-kernel
ns(config-router)#q
ns(config)#q
ns#show route-map
route-map redist-kernel, permit, sequence 5
  Match clauses:
    ip address 1
  Set clauses:
route-map redist-kernel, permit, sequence 10
  Match clauses:
    ip address 2
```

```
  Set clauses:
ns#show access-list
Standard IP access list 1
   deny 0.0.0.0
Standard IP access list 2
   permit any
ns#
```

- How do I view the debug output of networking daemons?

  You can write debugging output from networking daemons to a file by entering the following `log file` command from the global configuration view in VTYSH:

  ```
  ns(config)#log file /var/ZebOS.log
  ```

  With release 8.1, you can direct debug output to the console by entering the `terminal monitor` command from VTYSH user view:

  ```
  ns#terminal monitor
  ```

- How do I collect cores of running daemons?

  You can use the gcore utility to collect cores of running daemons for processing by gdb. This might be helpful in debugging misbehaving daemons without bringing the whole routing operation to a standstill.

  ```
  gcore [-s] [-c core] [executable] pid
  ```

  The -s option temporarily stops the daemon while gathering the core image. This is a recommended option, because it guarantees that the resulting image shows the core in a consistent state.

  ```
  root@ns#gcore -s -c nsm.core /netscaler/nsm 342
  ```

- How do I run a batch of ZebOS commands?

  You can run a batch of ZebOS commands from a file by entering the `VTYSH -f` <file-name> command. This does not replace the running configuration, but appends to it. However, by including commands to delete the existing configuration in the batch file and then add those for the new, desired configuration, you can use this mechanism to replace a specific configuration:

  ```
  !
  router bgp 234
  network 1.1.1.1 255.255.255.0
  ```

```
!
route-map bgp-out2 permit 10
 set metric 9900
 set community 8602:300
!
```

Troubleshooting OSPF-Specific Issues

Before you start debugging any OSPF specific issue, you must collect information from the NetScaler appliance and all systems in the affected LAN, including upstream and downstream routers. To begin, enter the following commands:

1. show interface from both nscli and VTYSH
2. `show ip ospf interface`
3. `show ip ospf neighbor detail`
4. show ip route
5. `show ip ospf route`
6. `show ip ospf database summary`
    a. If there are only few LSAs in the database, then enter `show ip ospf database router`, `show ip ospf database A`. network, `show ip ospf database external`, and other commands to get the full details of LSAs.
    b. If there are a large number of LSAs in the database, enter the `show ip ospf database self-originated` command.
7. show ip ospf
8. show ns ip. This ensures that the details of all VIPs of interest are included.
9. Get the logs from peering devices and run the following command:

```
gcore -s -c xyz.core /netscaler/ospfd <pid>
```

Note: The `gcore` command is non-disruptive.

Collect additional information from the NetScaler as follows:

1. Enable logging of error messages by entering the following command from the global configuration view in VTYSH:

```
ns(config)#log file /var/ospf.log
```

2. Enable debugging ospf events and log them by using the following command:

```
ns(config)#log file /var/ospf.log
```

Enable debug ospf lsa packet only if the number of LSAs in the database is relatively small (< 500).

Parameter Descriptions (of commands listed in the CLI procedure)

show interface

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show ns ip

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Internet Protocol version 6 (IPv6)

A NetScaler appliance supports both server-side and client-side IPv6 and can therefore function as an IPv6 node. It can accept connections from IPv6 nodes (both hosts and routers) and from IPv4 nodes, and can perform Protocol Translation (RFC 2765) before sending traffic to the services. You have to license the IPv6 feature before you can implement it.

The following table lists some of the IPv6 features that the NetScaler appliance supports.

Table 1. Some Supported IPv6 Features

IPv6 features
IPv6 addresses for SNIPs (NSIP6, VIP6, and SNIP6)
Neighbor Discovery (Address Resolution, Duplicated Address Detection, Neighbor Unreachability Detection, Router Discovery)
Management Applications (ping6, telnet6, ssh6)
Static Routing and Dynamic routing (OSPF)
Port Based VLANs
Access Control Lists for IPv6 addresses (ACL6)
IPv6 Protocols (TCP6, UDP6, ICMP6)
Server Side Support (IPv6 addresses for vservers, services)
USIP (Use source IP) and DSR (Direct Server Return) for IPv6
SNMP and CVPN for IPv6
HA with native IPv6 node address
IPv6 addresses for MIPs
Path-MTU discovery for IPv6

The following table lists NetScaler components that support IPv6 addresses and provides references to the topics that document the components.

Table 2. NetScaler Components That Support IPv6 Addresses and the Corresponding Documentation

NetScaler component	Topic that documents IPv6 support
Network	Adding, Customizing, Removing, Removing all, and Viewing routes.
SSL Offload	Creating IPv6 vservers for SSL Offload
SSL Offload	Specifying IPv6 SSL Offload Monitors
SSL Offload	Creating IPv6 SSL Offload Servers
Load Balancing	Creating IPv6 vservers for Load Balancing
Load Balancing	Specifying IPv6 Load Balancing Monitors

Load Balancing	Creating IPv6 Load Balancing Servers
DNS	Creating AAAA Records

You can configure IPv6 support for the above features after implementing the IPv6 feature on your NetScaler appliance. You can configure both tagged and prefix-based VLANs for IPv6. You can also map IPv4 addresses to IPv6 addresses.

Implementing IPv6 Support

IPv6 support is a licensed feature, which you have to enable before you can use or configure it. If IPv6 is disabled, the NetScaler does not process IPv6 packets. It displays the following warning when you run an unsupported command:

"Warning: Feature(s) not enabled [IPv6PT]"

The following message appears if you attempt to run IPv6 commands without the appropriate license:

"ERROR: Feature(s) not licensed"

After licensing the feature, use either of the following procedures to enable or disable IPv6.

To enable or disable IPv6 by using the command line interface

At the command prompt, type one of the following commands:

- enable ns feature ipv6pt
- disable ns feature ipv6pt

To enable or disable IPv6 by using the configuration utility

1. Navigate to System > Settings, in the Modes and Features group, click Configure Advanced Features.
2. Select or clear the IPv6 Protocol Translation option.

Parameter Descriptions (of commands listed in the CLI procedure)

enable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

disable ns feature

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

VLAN Support

If you need to send broadcast or multicast packets without identifying the VLAN (for example, during DAD for NSIP, or ND6 for the next hop of the route), you can configure the NetScaler appliance to send the packet on all the interfaces with appropriate tagging. The VLAN is identified by ND6, and a data packet is sent only on the VLAN.

For more information about ND6 and VLANs, see "Configuring Neighbor Discovery."

Port-based VLANs are common for IPv4 and IPv6. Prefix-based VLANs are supported for IPv6.

Simple Deployment Scenario

Following is an example of a simple load balancing set-up consisting of an IPv6 vserver and IPv4 services, as illustrated in the following topology diagram.

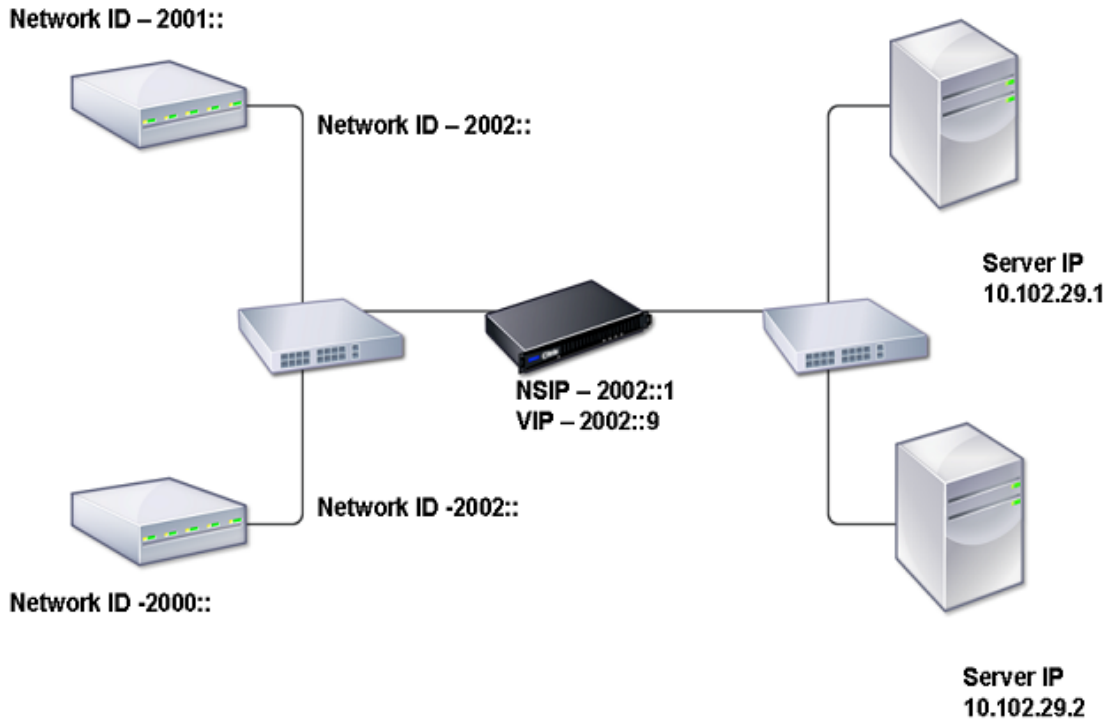
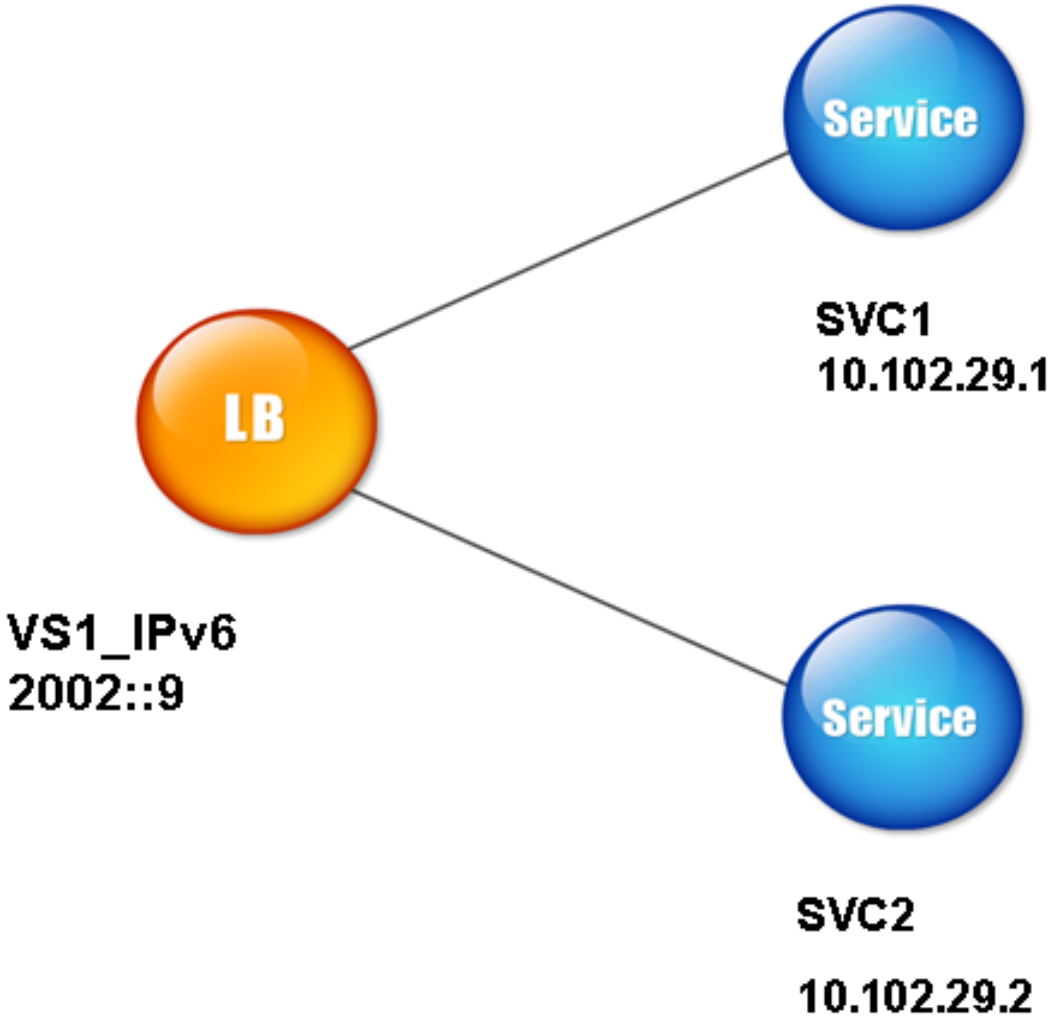


Figure 1. IPv6 Sample Topology

The following table summarizes the names and values of the entities that must be configured on the NetScaler.

Table 1. Sample Values for Creating Entities

Entity type	Name	Value
LB Vserver	VS1_IPv6	2002::9
Services	SVC1	10.102.29.1
	SVC2	10.102.29.2



The following figure shows the entities and values of the parameters to be configured on the NetScaler. Figure 2. IPv6 Entity Diagram

To configure this deployment scenario, you need to do the following:

1. Create an IPv6 service.
2. Create an IPv6 LB vserver.
3. Bind the services to the vserver.

To create IPv4 services by using the command line interface

At the command prompt, type:

add service <Name> <IPAddress> <Protocol> <Port>

Example

add service SVC1 10.102.29.1 HTTP 80
add service SVC2 10.102.29.2 HTTP 80

To create IPv4 services by using the configuration utility

Navigate to Load Balancing > Services, click Add, and then set the following parameters:

- Service Name
- IP Address
- Protocol
- Port

To create IPv6 vserver by using the command line interface

At the command prompt, type:

add lb vserver <Name> <IPAddress> <Protocol> <Port>

Example

add lb vserver VS1_IPv6 2002::9 HTTP 80

To create IPv6 vserver by using the configuration utility

1. Set the following parameters:
   - Name
   - Protocol
   - IP Address Type
   - IP Address
   - Port

To bind a service to an LB vserver by using the command line interface

At the command prompt, type:

bind lb vserver <name> <service>

Example

bind lb vserver VS1_IPv6 SVC1

The vservers receive IPv6 packets and the NetScaler performs Protocol Translation (RFC 2765) before sending traffic to the IPv4-based services.

To bind a service to an LB vserver by using the configuration utility

1. Navigate to Load Balancing > Virtual Servers.
2. In the Load Balancing Virtual Servers page, select the vserver for which you want to bind the service (for example, VS1_IPv6).
3. Click Open.
4. In the Configure Virtual Server (Load Balancing) dialog box, on the Services tab, select the Active check box corresponding to the service that you want to bind to the vserver (for example, SVC1).
5. Click OK.
6. Repeat Steps 1-4 to bind the service (for example, SVC2 to the vserver).

Parameter Descriptions (of commands listed in the CLI procedure)

add service

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Host Header Modification

When an HTTP request has an IPv6 address in the host header, and the server does not understand the IPv6 address, you must map the IPv6 address to an IPv4 address. The IPv4 address is then used in the host header of the HTTP request sent to the vserver.

To change the IPv6 address in the host header to an IPv4 address by using the command line interface

At the command prompt, type:

set ns ip6 <IPv6Address> -map <IPAddress>

Example

set ns ip6 2002::9 -map 200.200.200.200

To change the IPv6 address in the host header to an IPv4 address by using the configuration utility

1. Navigate to Network > IPs and, on the IPV6s tab, select the IP address for which you want to configure a mapped IP address, for example, 2002:0:0:0:0:0:0:9, and click Open.
2. In the Mapped IP text box, type the mapped IP address that you want to configure, for example, 200.200.200.200.

Parameter Descriptions (of commands listed in the CLI procedure)

set ns ip6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

VIP Insertion

If an IPv6 address is sent to an IPv4-based server, the server may not understand the IP address in the HTTP header, and may generate an error. To avoid this, you can map an IPv4 address to the IPv6 VIP and enable VIP insertion.

To configure a mapped IPv6 address by using the command line interface

At the command prompt, type:

set ns ip6 <IPv6Address> -map <IPAddress>

Example

```
> set ns ip6 2002::9 -map 200.200.200.200
 Done
```

To configure a mapped IPv6 address by using the configuration utility

1. Navigate to Network > IPs, on the IPV6s tab, select the IP address for which you want to configure a mapped IP address, for example, 2002:0:0:0:0:0:0:9, and click Open.
2. In the Mapped IP text box, type the mapped IP address that you want to configure, for example, 200.200.200.200.

Use either of the following procedures to enable insertion of an Ipv4 VIP address and port number in the HTTP requests sent to the servers.

To enable VIP insertion by using the command line interface

At the command prompt, type:

set lb vserver <name> -insertVserverIPPort <Value>

Example

```
> set lb vserver VS1_IPv6 -insertVserverIPPort ON
 Done
```

To enable VIP insertion by using the configuration utility

1. In the Advanced tab, under Traffic Settings, in the Vserver IP Port Insertion drop-down list box, select VIPADDR.
2. In the Vserver IP Port Insertion text box, type the vip header.

Parameter Descriptions (of commands listed in the CLI procedure)

set ns ip6

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

set lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Traffic Domains

Traffic domains are a way to segment network traffic for different applications. You can use traffic domains to create multiple isolated environments within a NetScaler appliance. An application belonging to a specific traffic domain communicates with entities and processes traffic within that domain. The traffic belonging to one traffic domain cannot cross the boundary of another traffic domain.

Benefits of using Traffic Domains

The main benefits of using traffic domains on a NetScaler appliance are the following:

- **Use of duplicate IP addresses in a Network**. Traffic domains allow you to use duplicate IP address on the network. You can assign the same IP address or network address to multiple devices on a network, or multiple entities on a NetScaler appliance, as long as each of the duplicate address belongs to a different traffic domain.
- **Use of Duplicate entities on the NetScaler appliance**. Traffic domains also allow you to use duplicate NetScaler feature entities on the appliance. You can create entities with the same settings as long as each entity is assigned to a separate traffic domain.

  Note: Duplicate entities with same name is not supported.
- **Multitenancy**. Using traffic domains, you can provide hosting services for multiple customers by isolating each customer's type of application traffic within a defined address space on the network.

A traffic domain is uniquely identified by an identifier, which is an integer value. Each traffic domain needs a VLAN or a set of VLANs. The isolation functionality of the traffic domain depends on the VLANs bound to the traffic domain. More than one VLAN can be bound to a traffic domain, but the same VLAN cannot be a part of multiple traffic domains. Therefore, the maximum number of traffic domains that can be created depends on the number of VLANS configured on the appliance.

Default Traffic Domain

A NetScaler appliance has a preconfigured traffic domain, called the *default traffic domain*, which has an ID of 0. All factory settings and configurations are part of the default traffic domain. You can create other traffic domains and then segment traffic between the default traffic domain and each of the other traffic domains. You cannot remove the default traffic domain from the NetScaler appliance. Any feature entity that you create without setting the traffic domain ID is automatically associated with the default traffic domain.

Note: Some features and configurations are supported only in the default traffic domain. They do not work in nondefault traffic domains. For a list of the features supported in all traffic domains, see "Supported NetScaler Features in Traffic Domains."

How Traffic Domains Work

As an illustration of traffic domains, consider an example in which two traffic domains, with IDs 1 and 2, are configured on NetScaler appliance NS1.

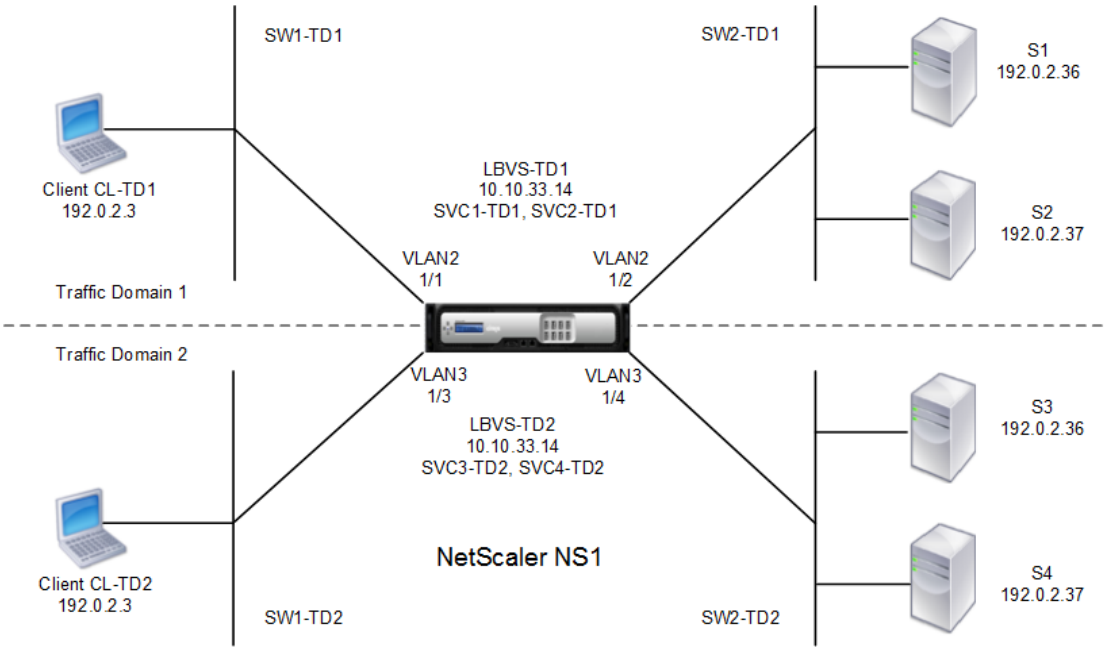
In traffic domain 1, load balancing virtual server LBVS-TD1 is configured to load balance traffic across servers S1 and S2. On the NetScaler appliance, servers S1 and S2 are represented by services SVC1-TD1 and SVC2-TD1, respectively. Servers S1 and S2 are connected to NS1 through L2 switch SW2-TD1. Client CL-TD1 is on a private network connected to NS1 through L2 switch SW1-TD1. SW1-TD1 and SW2-TD1 are connected to VLAN 2 of NS1. VLAN 2 is bound to traffic domain 1, which means that client CL-TD1 and servers S1 and S2 are part of traffic domain 1.

Similarly in traffic domain 2, load balancing virtual server LBVS-TD2 is configured to load balance traffic across S3 and S4. On the NetScaler appliance, servers S3 and S4 are represented by services SVC3-TD2 and SVC4-TD2, respectively. Servers S3 and S4 are connected to NS1 through L2 switch SW2-TD2. Client CL-TD2 is on a private network connected to NS1 through L2 switch SW1-TD2. SW1-TD2 and SW2-TD2 are connected to VLAN 3 of NS1. VLAN 3 is bound to traffic domain 2, which means that client CL-TD2 and servers S3 and S4 are part of traffic domain 2.

On the NetScaler appliance, entities LBVS-TD1 and LBVS-TD2 share the same settings, including the IP address. The same is true for SVC1-TD1 and SVC3-TD2, and for SVC2-TD1 and SVC4-TD2. This is possible because these entities are in different traffic domains.

Similarly, servers S1 and S3, S2 and S4 share the same IP address, and clients CL-TD1 and CL-TD2 each have the same IP address.

Figure 1. How traffic domains work



The following table lists the settings used in the example.

Entity	Name	Details
Settings in traffic domain 1		
VLANs bound to traffic domain 1	VLAN 2	VLAN Id: 2 Interfaces bound: 1/1, 1/2
Client connected to TD1	CL-TD1 (for reference purposes only)	IP address: 192.0.2.3
Load balancing virtual server in TD1	LBVS-TD1	IP address: 192.0.2.15
Service bound to virtual server LBVS-TD1	SVC1-TD1	IP address: 192.0.2.36
	SVC2-TD1	IP address: 192.0.2.37
SNIP	SNIP-TD1 (for reference purposes only)	IP address: 192.0.2.27
Settings in traffic domain 2		
VLAN bound to traffic domain 2	VLAN 3	VLAN Id: 3 Interfaces bound: 1/3, 1/4
Client connected to TD2	CL-TD2 (for reference purposes only)	IP address: 192.0.2.3
Load balancing virtual server in TD2	LBVS-TD2	IP address: 192.0.2.15
Service bound to virtual server LBVS-TD2	SVC3-TD2	IP address: 192.0.2.36
	SVC4-TD2	IP address: 192.0.2.37
SNIP in TD2	SNIP-TD2 (for reference purposes only)	IP address: 192.0.2.29

Following is the traffic flow in traffic domain 1:

1. Client CL-TD1 broadcasts an ARP request for the IP address of 192.0.2.15.
2. The ARP request reaches NS1 on interface 1/1, which is bound to VLAN 2. Because VLAN 2 is bound to traffic domain 1, NS1 updates the ARP table of traffic domain 1 for the IP address of client CL-TD1.
3. Because the ARP request is received on traffic domain 1, NS1 looks for an entity configured on traffic domain 1 that has an IP address of 192.0.2.15. NS1 finds that a load balancing virtual server LBVS-TD1 is configured on traffic domain 1 and has the IP address 192.0.2.15.
4. NS1 sends an ARP response with the MAC address of interface 1/1.
5. The ARP reply reaches CL-TD1. CL-TD1 updates its ARP table for the IP address of LBVS-TD1 with the MAC address of interface 1/1 of NS1.
6. Client CL-TD1 sends a request to 192.0.2.15. The request is received by LBVS-TD1 on port 1/1 of NS1.
7. LBVS-TD1's load balancing algorithm selects server S2, and NS1 opens a connection between a SNIP in traffic domain 1 (192.0.2.27) and S2.

8. S2 replies to SNIP 192.0.2.27 on NS1.

9. NS1 sends S2's reply to client CL-TD1.

Following is the traffic flow in traffic domain 2:

1. Client CL-TD2 broadcasts an ARP request for the IP address of 192.0.2.15.

2. The ARP request reaches NS1 on interface 1/3, which is bound to VLAN 3. Because VLAN 3 is bound to traffic domain 2, NS1 updates traffic-domain 2's ARP-table entry for the IP address of client CL-TD2, even though an ARP entry for the same IP address (CL-TD1) is already present in the ARP table of traffic domain 1.

3. Because the ARP request is received in traffic domain 2, NS1 searches traffic domain 2 for an entity that has an IP address of 192.0.2.15. NS1 finds that load balancing virtual server LBVS-TD2 is configured in traffic domain 2 and has the IP address 192.0.2.15. NS1 ignores LBVS-TD1 in traffic domain 1, even though it has the same IP address as LBVS-TD2.

4. NS1 sends an ARP response with the MAC address of interface 1/3.

5. The ARP reply reaches CL-TD2. CL-TD2 updates its ARP table entry for the IP address of LBVS-TD2 with the MAC address of interface 1/3 of NS1.

6. Client CL-TD2 sends a request to 192.0.2.15. The request is received by LBVS-TD2 on interface 1/3 of NS1.

7. LBVS-TD2's load balancing algorithm selects server S3, and NS1 opens a connection between a SNIP in traffic domain 2 (192.0.2.29) and S3.

8. S2 replies to SNIP 192.0.2.29 on NS1.

9. NS1 sends S2's reply to client CL-TD2.

Supported NetScaler Features in Traffic Domains

The NetScaler features in the following list are supported in all traffic domains.

Supported features in traffic domains	
· ARP table	· Persistency
· ND6 table	· Service
· Bridge table	· Servicegroup
· All types of IPv4 and IPv6 addresses	· Policies (*)
· IPv4 and IPv6 routes	· PING
· ACL and ACL6	· TRACEROUTE
· PBR & PBR6	· PMTU
· INAT	· High Availability (connection mirroring is not supported)
· RNAT	· Cookie Persistency
· MSR	· MSS
· MSR6	· Logging
· Net profiles	· Priority Queuing
· SNMP MIBs	· Surge Protection
· Fragmentation	· HTTP DOSP (*)
· Monitors	· Load balancing (all types of load balancing virtual servers except of type TFTP)
· Content Switching	
· Cache Redirection	

Any NetScaler feature not listed above is supported only in the default traffic domain.
Traffic domains are not supported in a cluster configuration.

Configuring Traffic Domains

Configuring a traffic domain on the NetScaler appliance consists of the following tasks:

- **Add VLANs.** Create VLANs and bind specified interfaces to them.
- **Create a traffic domain entity and bind VLANs to it.** This involves the following two tasks:
  - Create a traffic domain entity uniquely identified by an ID, which is an integer value.
  - Bind the specified VLANs to the traffic domain entity. All the interfaces that are bound to the specified VLANs are associated with the traffic domain. More than one VLAN can be bound to a traffic domain, but a VLAN cannot be a part of multiple traffic domains.
- **Create feature entities on the traffic domain**. Create the required feature entities in the traffic domain. The CLI commands and configuration dialog boxes of all the supported features in a nondefault traffic domain include a parameter called a *traffic domain identifier* (td). When configuring a feature entity, if you want the entity to be associated with a particular traffic domain, you must specify the td. Any feature entity that you create without setting the td is automatically associated with the default traffic domain.

To give you an idea of how feature entities are associated with a traffic domain, this topic covers the procedures for configuring all the entities mentioned in the figure titled "How traffic domains work."

The command line interface has two commands for these two tasks, but the configuration utility combines them in a single dialog box.

To create a VLAN and bind interfaces to it by using the command line interface

At the command prompt, type:

- add vlan <id>
- bind vlan <id> -ifnum <slot/port>
- show vlan <id>

To create a traffic domain entity and bind VLANs to it by using the command line interface

At the command prompt, type:

- add ns trafficdomain <td>
- bind ns trafficdomain <td> -vlan <id>
- show ns trafficdomain <td>

To create a service by using the command line interface

At the command prompt, type:

- add service <name> <IP> <serviceType> <port> -td <id>
- show service <name>

To create a load balancing virtual server and bind services to it by using the command line interface

At the command prompt, type:

- add lb vserver <name> <serviceType> <IPAddress> <port> -td <id>
- bind lb vserver <name> <serviceName>
- show lb vserver <name>

To create a VLAN by using the configuration utility

Navigate to Network > VLANs, click Add, and set the parameters.

To create a traffic domain entity by using the configuration utility

Navigate to Network > Traffic Domains, click Add, and in the Create Traffic Domain dialog box, set the parameters.

To create a service by using the configuration utility

Navigate to Load Balancing > Services, click Add, and set the parameters.

To create a load balancing virtual server by using the configuration utility

Navigate to Load Balancing > Virtual Servers, click Add, and set the parameters.

Parameter Descriptions (of commands listed in the CLI procedure)

add vlan

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind vlan

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show vlan

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add service

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show service

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

show lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Web Interface

The Web Interface on Citrix NetScaler appliances is based on Java Server Pages (JSP) technology and provides access to Citrix XenApp and Citrix XenDesktop applications. Users access resources through a standard Web browser or by using the Citrix XenApp plug-in.

The Web Interface runs as a service on port 8080 on the NetScaler appliance. To create Web Interface sites, Java is executed on Apache Tomcat Web server version 6.0.35 on the NetScaler appliance. The Web Interface sites provide user access to the XenApp and XenDesktop resources, which include applications, content, and desktops.

The Web Interface installation includes installing the Web Interface tar file and JRE tar file on the NetScaler appliance. To configure the Web Interface, you create a Web Interface site and bind one or more XenApp or XenDesktop farms to it.

How Web Interface Works

The following figure illustrates a basic Web interface session.

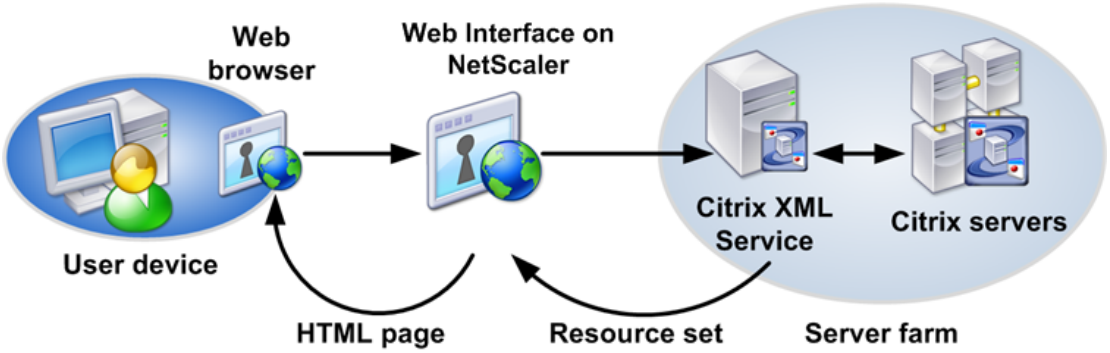


Figure 1. *A Basic Web Interface Session*

Following is a typical set of interactions among a user device, a NetScaler running the Web interface, and a server farm.

1. A user authenticates to the Web interface through a Web browser or by using the XenApp plug-in.
2. The Web interface reads the user's credentials and forwards the information to the Citrix XML Service running on servers in the server farm.
3. The Citrix XML Service on the designated server retrieves from the servers a list of resources that the user can access. These resources constitute the user's resource set and are retrieved from the Independent Management Architecture (IMA) system.
4. The Citrix XML Service then returns the user's resource set to the Web interface running on the NetScaler.
5. The user clicks an icon that represents a resource on the HTML page.
6. The Web interface queries the Citrix XML Service for the least busy server.
7. The Citrix XML Service returns the address of this server to the Web interface.
8. The Web interface sends the connection information to the Web browser.
9. The Web browser initiates a session with the server.

Prerequisites

The following prerequisites are required before you begin installing and configuring the Web interface.

- XenApp or XenDesktop farms are set up and running in your environment. For more information about XenApp, see the XenApp documentation at http://edocs.citrix.com/. For more information about XenDesktop, see the XenDesktop farms documentation at http://edocs.citrix.com/.
- Conceptual knowledge of the Web interface. For more information about Web interface running on a server, see the Web interface documentation at http://edocs.citrix.com/.

Installing the Web Interface

To install the Web interface, you need to install the following files:

- **Web interface tar file**. The setup file for installing the Web interface on the NetScaler appliance. This tar file also includes Apache Tomcat Web server version 6.0.35. The file name has the following format: nswi-<version number>.tgz (for example, nswi-1.5.tgz).

- **JRE tar file**. The JRE tarball. You can use the Diablo Latte JRE version 1.6.0-7 for 64-bit FreeBSD 6.x/amd64 platform available on FreeBSD Foundation Web site at http://www.freebsdfoundation.org/java/java16. Alternatively, you can use OpenJDK6 package for FreeBSD 6.x/amd63. You can download openjdk6-b17_2.tbz from https://citrix.sharefile.com/d/c85aeefcc05643f8.

Note: On a high availability setup, when installing the web interface with tar files (web interface and JRE) that are already available on the appliance, ensure that the files are available in the same location on both the primary and secondary appliances; otherwise, the web interface will not be installed on the secondary appliance.

Copy the tar files to a local workstation or to the /var directory of the appliance.

These files install all the Web interface components and JRE on the hard drive and configure automatic startup of the Tomcat Web server with Web interface at appliance startup time. Both tar files are internally expanded in the /var/wi directory on the hard drive.

Note: After installing web interface on the appliance and before creating a web interface site, you must place the client plugin in the appliance by using the appropriate Upload Plugins utility provided on the web interface details pane.

To install the Web interface and JRE tar files by using the command line interface

At the command prompt, type:

install wi package -wi <URL> -jre <URL>

Examples

> install wi package -wi sftp://username:password@10.102.29.12/var/nswi-1.5.tgz -jre <url>

> install wi package -wi ftp://username:password@10.102.29.15/var/nswi-1.5.tgz -jre <url>

To install the Web interface and JRE tar files by using the configuration utility

In the navigation pane, click Web Interface, and select Install Web Interface, and then specify the install path for web interface tar file and JRE tar file.

Parameter Descriptions (of commands listed in the CLI procedure)

install wi package

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring the Web Interface

To configure the web interface, you create a web interface site and bind one or more XenApp or XenDesktop farms to it. You then configure the web interface to work behind an HTTP or an HTTPS virtual server or Access Gateway.

- **Using an HTTP or an HTTPS virtual server**. You create an HTTP or an HTTPS virtual server on the NetScaler appliance and bind the web interface service, running on port 8080 of the NetScaler appliance, to the virtual server. Clients on the LAN use the virtual server IP address to access the web interface. When using this access method, the URL format for the web interface site is as follows:

  ```
  <HTTP or HTTPS>://<HTTP or HTTPS vserver IP address>:<vserver port number>/<web interface site path>
  ```

  The following access methods are available for clients accessing the web interface site when it is configured using an HTTP or an HTTPS virtual server:

  - **Direct**. Actual address of a XenApp or XenDesktop server is sent to the clients.
  - **Alternate**. Alternate address of a XenApp or XenDesktop server is sent to the clients.
  - **Translated**. Translated address, from the defined internal addresses to external addresses and ports mapping table, is sent to the clients from a specified network. When you use this option, you have to define internal address to external address and port mappings.
- **Using Access Gateway**. You associate the web interface site with Access Gateway. You associate the web interface site with Access Gateway. Remote clients use the Access Gateway URL to access the web interface site. With this access method, the URL format for the web interface site is as follows:

  ```
  HTTPS://<Access Gateway URL>/<web interface site path>
  ```

  The following access methods are available for clients accessing the web interface site when it is configured using an Access Gateway:

  - **Gateway Direct**. Actual address of a XenApp or XenDesktop server is sent to Access Gateway.
  - **Gateway Alternate**. Alternate address of a XenApp server is sent to Access Gateway. You cannot use this mode to access XenDesktop servers.
  - **Gateway Translated**. Translated address, from the defined internal addresses to external addresses and ports mapping table, is sent to Access Gateway. When you use this option, you have to define internal address to external address and port mappings.

Configuring a Web Interface Site for LAN Users Using HTTP

In this scenario, user and the Web interface setup are on the same enterprise LAN. The enterprise has both a XenApp and a XenDesktop farm. Users access the Web interface by using an HTTP vserver. The Web interface exposes its own login page for authentication. The vserver IP address is used to access the Web interface.

The following figure illustrates the Web interface running on the NetScaler appliance NS1. A Web interface site WINS1 is created and a XenApp farm XA1 and a XenDesktop farm XD1 are bound to it. An HTTP vserver HTTP_WI is also created. Client C1 uses the IP address of the HTTP_WI vserver to access the WINS1 site.

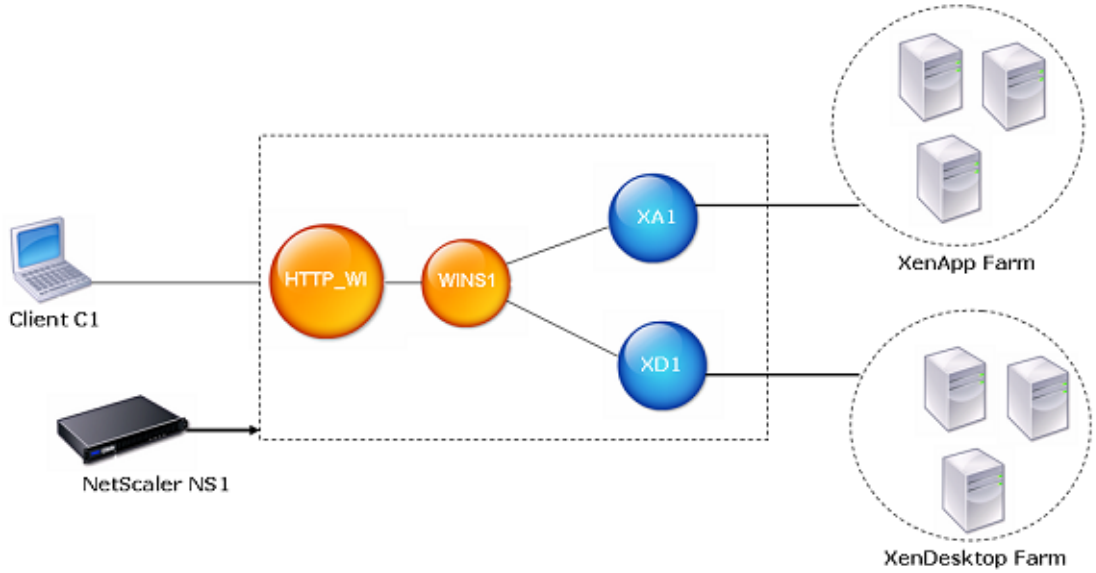


Figure 1. A Web Interface Site Configured for LAN Users Using HTTP

To configure a Web interface site for LAN users using HTTP by using the configuration utility

1. In the navigation pane, click Web Interface.
2. In the details pane, click Web Interface Wizard.
3. On the wizard Introduction page, click Next.
4. On the wizard Configure Web Interface Site page, configure the following parameters:
   - Site Path* (You cannot change the name of an existing Web interface site.)
   - Site Type
   - Published Resource Type
   - Kiosk Mode
   - Authentication Methods
   - Login Title
   - Web Session Timeout
   - Enable access through receiver client

   * A required parameter.
5. In Default Access Methods, select the Direct or Alternate or Translated option and configure the following parameters:
   - Virtual Server
   - Protocol (select **HTTP**)
   - IP Address
   - Port

   Note:

   When you create the HTTP vserver by using the configuration utility, the configuration utility automatically creates a service, which logically represents the Web interface service running on the NetScaler appliance, and binds the service to the HTTP virtual server.

   For more information about services and virtual servers, see the "Traffic Management."
6. Click Next.
7. On the wizard's Configure Access Methods page, do one of the following:
   - To set an access method for a client IP address or network, click Add.

- To change the access method for a client IP address or network, select the association, and then click Open.

8. In the Configure Access Method dialog box, configure the following parameters:

   - Client IP Address* (You cannot change this parameter after setting it.)
   - Netmask (You cannot change this parameter after setting it.)
   - Access Method

   * A required parameter.

   Note: Before you configure access method based on the client IP address, you must enable USIP mode on the web interface service to make the client's IP address available with the web interface.

9. Click Next.
10. On the wizard's Configure Address Translations page, click Add for adding a mapping between an Internal IP address and an external IP address.

    Note: The Configure Address Translations page appears on the wizard when you set the Translated access method for a Client's IP address or network.

11. In the Configure Address Translations dialog box, configure the following parameters:

    - Internal IP Address
    - Internal Port
    - External IP Address
    - External Port
    - Access Type

    * A required parameter.

12. Click Next.
13. On the wizard's Configure XenApp/XenDesktop Farm page, do one of the following:

    - To add a XenApp or XenDesktop farm, click Add.
    - To modify an existing XenApp or XenDesktop farm, select the farm, and then click Open.

14. In the Create XenApp/XenDesktop Farm or Configure XenApp/XenDesktop Farm dialog box, configure the following parameters:

    - Name* (You cannot change the name of an existing XenApp or XenDesktop farm.)
    - XML Service Addresses*
    - XML Service Port
    - Transport

- Load Balance

* A required parameter.

15. Click Next, and then click Finish.

16. Verify that the Web interface site you configured is correct by selecting the site and viewing the Details section at the bottom of the pane. To view the Web interface site, in the navigation pane, expand System, expand Web Interface, and then click Sites.

To configure a Web interface site for LAN users using HTTP by using the command line interface

1. Add a Web interface site. Set Direct or Alternate or Translated for the defaultAccessMethod parameter. At the command prompt, type:

   add wi site <sitePath> -siteType (XenAppWeb | XenAppServices) -publishedResourceType (Online | Offline | DualMode) -kioskMode (ON | OFF) -wiAuthenticationMethods (Explicit | Anonymous) -webSessionTimeout <positive_integer> -defaultAccessMethod <defaultAccessMethod> -loginTitle <string>

   Example

   > add wi site WINS1 -siteType XenAppWeb -publishedResourceType Online -kioskMode ON -defaultAccess

2. (Optional) Set an access method for a Client's IP address or network. At the command prompt, type:

   bind wi site <sitePath> -accessMethod <accessMethod> -clientIpAddress <ip_addr> -clientNetMask <netmask>

3. If you have set the Translated access method for a Client's IP address or network then provide Internal IP and external IP address mappings. At the command prompt, type:

   bind wi site <sitePath> -translationInternalIp <ip_addr> -translationInternalPort <port|*> -translationExternalIp <ip_addr> -translationExternalPort <port|*> [-accessType <accessType>]

4. Bind XenApp or XenDesktop farms to the Web interface site. At the command prompt, type:

   bind wi site <sitePath> <farmName> <xmlServerAddresses> -xmlPort <value> -transport (HTTP | HTTPS) -loadBalance (ON | OFF)

   Example

   > bind wi site WINS1 XA1 10.102.46.6 -xmlPort 80 -transport HTTP -LoadBalance OFF
   > bind wi site WINS1 XD1 10.102.46.50 -xmlPort 80 -transport HTTP -LoadBalance OFF

5. Create a service that is a logical representation of the Web interface service running on the NetScaler appliance. At the command prompt, type:

   add service <name> <IP address> <serviceType> <port>

   Example

   > add service WI_Loopback_Service 127.0.0.1 HTTP 8080

6. Add an HTTP vserver. At the command prompt, type:

   add lb vserver <virtualServerName> <protocol> <IPAddress> <port>

   Example

> add lb vserver HTTP_WI HTTP 10.102.29.5 80

7. Bind the Web interface service to the HTTP vserver. At the command prompt, type:

   bind lb vserver <virtualServerName> <serviceName>

   Example

   > bind lb vserver HTTP_WI WI_Loopback_Service

Parameter Descriptions (of commands listed in the CLI procedure)

add wi site

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind wi site

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add service

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring a Web Interface Site for LAN Users Using HTTPS

In this scenario, user accounts and the Web interface setup are on the same enterprise LAN. Users access the Web interface by using an SSL-based (HTTPS) vserver. The Web interface exposes its own login page for authentication. SSL offloading is done by this vserver on the NetScaler. The vserver IP address is used to access the Web interface instead of the NetScaler IP address (NSIP).

The following figure illustrates the Web interface running on the NetScaler appliance NS1. A Web interface site WINS1 is created and a XenApp farm XA1 and a XenDesktop farm XD1 are bound to it. An HTTPS vserver HTTPS_WI is also created. Client C1 uses the IP address of the HTTPS_WI vserver to access the WINS1 site.

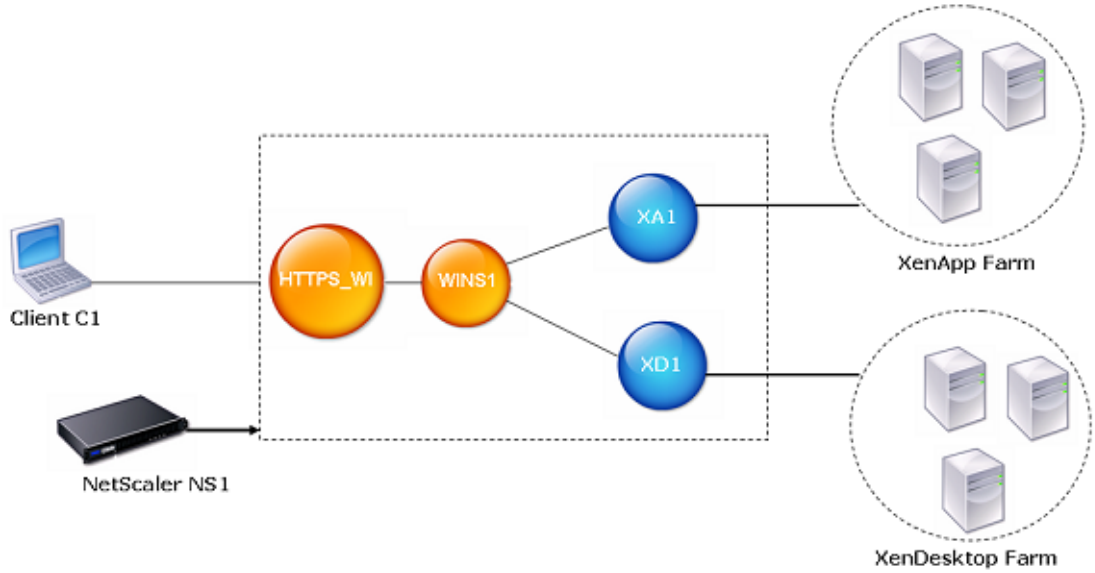


Figure 1. A Web Interface Site Configured for LAN Users Using HTTPS

To configure a Web interface site for LAN users using HTTPS by using the configuration utility

1. In the navigation pane, click Web Interface.
2. In the details pane, click Web Interface Wizard.
3. On the wizard Introduction page, click Next.
4. On the wizard Configure Web Interface Site page, configure the following parameters:
   - Site Path* (You cannot change the name of an existing Web interface site.)
   - Site Type
   - Published Resource Type
   - Kiosk Mode
   - Authentication Methods
   - Login Title
   - Web Session Timeout
   - Enable access through receiver client

   * A required parameter.
5. In Default Access Methods, select the Direct or Alternate or Translated option and configure the following parameters:
   - Virtual Server
   - Protocol (select **HTTPs**)
   - IP Address
   - Port

   Note:

   When you create the HTTPS vserver by using the configuration utility, the configuration utility automatically creates a service, which logically represents the Web interface service running on the NetScaler appliance, and binds the service to the HTTPS virtual server.

   For more information about services and virtual servers, see the "Traffic Management."
6. Click Next.
7. On the wizard's Specify a server Certificate page, you create or specify an existing SSL certificate-key pair. The SSL certificate-key pair is automatically bound to the HTTPS vserver.

For more information, see "Binding an SSL Certificate Key Pair to the Virtual Server."

8. Click Next.
9. On the wizard's Configure Access Methods page, do one of the following:
   - To set an access method for a client IP address or network, click Add.
   - To change the access method for a client IP address or network, select the association, and then click Open.
10. In the Configure Access Method dialog box, configure the following parameters:
    - Client IP Address* (You cannot change this parameter after setting it.)
    - Netmask (You cannot change this parameter after setting it.)
    - Access Method

    * A required parameter.

    Note: Before you configure access method based on the client IP address, you must enable USIP mode on the web interface service to make the client's IP address available with the web interface.
11. Click Next.
12. On the wizard's Configure Address Translations page, click Add for adding a mapping between an Internal IP address and an external IP address.

    Note: The Configure Address Translations page appears on the wizard when you set the Translated access method for a Client's IP address or network.
13. In the Configure Address Translations dialog box, configure the following parameters:
    - Internal IP Address
    - Internal Port
    - External IP Address
    - External Port
    - Access Type

    * A required parameter.
14. On the wizard's Configure XenApp/XenDesktop Farm page, do one of the following:
    - To add a XenApp or XenDesktop farm, click Add.
    - To modify an existing XenApp or XenDesktop farm, select the farm, and then click Open.
15. In the Create XenApp/XenDesktop Farm or Configure XenApp/XenDesktop Farm dialog box, configure the following parameters:
    - Name* (You cannot change the name of an existing XenApp or XenDesktop farm.)
    - XML Service Addresses*

- XML Service Port
- Transport
- Load Balance

* A required parameter.

16. Click Next, and then click Finish.
17. Verify that the Web interface site you configured is correct by selecting the site and viewing the Details section at the bottom of the pane. To view the Web interface site, in the navigation pane, expand System, expand Web Interface, and then click Sites.

To configure a Web interface site for LAN users using HTTPS by using the command line

1. Add a Web interface site. Set Direct or Alternate or Translated for the defaultAccessMethod parameter. At the command prompt, type:

   add wi site <sitePath> -siteType (XenAppWeb | XenAppServices) -publishedResourceType (Online | Offline | DualMode) -kioskMode (ON | OFF) -wiAuthenticationMethods (Explicit | Anonymous) -webSessionTimeout <positive_integer> -defaultAccessMethod <defaultAccessMethod> -loginTitle <string>

   Example

   > add wi site WINS1 -siteType XenAppWeb -publishedResourceType Online -kioskMode ON -defaultAccess

2. (Optional) Set an access method for a Client's IP address or network. At the command prompt, type:

   bind wi site <sitePath> -accessMethod <accessMethod> -clientIpAddress <ip_addr> -clientNetMask <netmask>

3. If you have set the Translated access method for a Client's IP address or network then provide Internal IP and external IP address mappings. At the command prompt, type:

   bind wi site <sitePath> -translationInternalIp <ip_addr> -translationInternalPort <port|*> -translationExternalIp <ip_addr> -translationExternalPort <port|*> [-accessType <accessType>]

4. Bind XenApp or XenDesktop farms to the Web interface site. At the command prompt, type:

   bind wi site <sitePath> <farmName> <xmlServerAddresses> -xmlPort <value> -transport (HTTP | HTTPS) -loadBalance (ON | OFF)

   Example

   > bind wi site WINS1 XA1 10.102.46.6 -xmlPort 80 -transport HTTP -LoadBalance OFF
   > bind wi site WINS1 XD1 10.102.46.50 -xmlPort 80 -transport HTTP -LoadBalance OFF

5. Create a service that is a logical representation of the Web interface service running on the NetScaler appliance. At the command prompt, type:

   add service <name> <IPAddress> <serviceType> <port>

   Example

   > add service WI_Loopback_Service 127.0.0.1 HTTP 8080

6. Add an HTTPS vserver. At the command prompt, type:

   add lb vserver <name>@ <protocol> <IPAddress> <port>

   Example

> add lb vserver HTTPS_WI SSL 10.102.29.3 443

7. Bind the Web interface service to the HTTPS vserver. At the command prompt, type:

   bind lb vserver <name>@ <serviceName>

   Example

   > bind lb vserver HTTPS_WI WI_Loopback_Service

8. Create an SSL certificate key pair. At the command prompt, type:

   add ssl certkey <certificate-KeyPairName> -cert <certificateFileName> -key <privateKeyFileName>

   Example

   > add ssl certkey SSL-Certkey-1 -cert /nsconfig/ssl/test1.cer -key /nsconfig/ssl/test1

9. Bind the SSL certificate key pair to the HTTPS vserver. At the command prompt, type:

   bind ssl vserver <vserverName> -certkeyName <certificate- KeyPairName>

   Example

   > bind ssl vserver HTTPS_WI -certkeyName SSL-Certkey-1

10. Add a rewrite action. At the command prompt, type:

    add rewrite action <name> <type> <target> [<stringBuilderExpr>] [(-pattern <expression>]

    Example

    > add rewrite action Replace_HTTP_to_HTTPS INSERT_AFTER "HTTP.RES.HEADER(\"Location\").Value(0).R

11. Create a rewrite policy and bind the rewrite action to it. At the command prompt, type:

    add rewrite policy <name> <rule> <action>

    Example

    > add rewrite policy rewrite_location "HTTP.RES.STATUS == 302 && HTTP.RES.HEADER(\"Location\").Valu

12. Bind the rewrite policy to the HTTPS vserver. At the command prompt, type:

    bind lb vserver <VserverName> -policyname <rewritePolicyName> -priority <value> -type response

    Example

    > bind lb vserver HTTPS_WI -policyname rewrite_location -priority 10 -type response

Parameter Descriptions (of commands listed in the CLI procedure)

add wi site

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind wi site

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add service

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind lb vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add ssl certkey

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind ssl vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add rewrite action

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add rewrite policy

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Configuring a Web Interface Site for Remote Users Using Access Gateway

In this scenario, user accounts and the Web interface setup are on different networks. Users access a Web interface site by using the Access Gateway URL. SmartAccess is automatically enabled.

The following figure illustrates the Web interface running on the NetScaler appliance NS1. A Web interface site WINS1 is created and a XenApp farm XA1 and a XenDesktop XD1 are bound to it. An Access Gateway VPN vserver AGEE_WI is also configured. The client uses the Access Gateway URL of the AGEE_WI to access the WINS1 site.

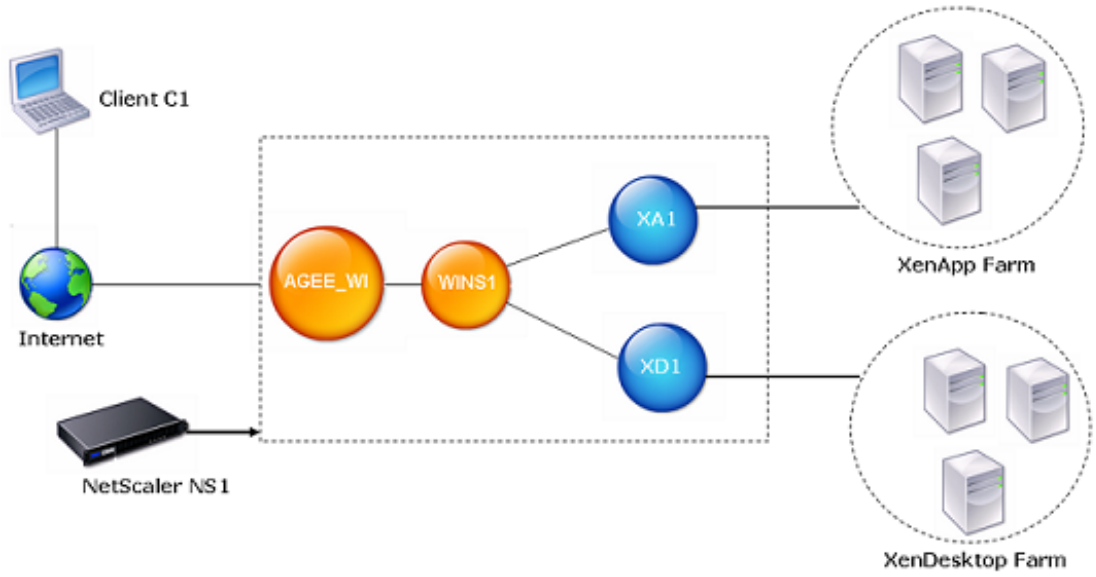


Figure 1. A Web Interface Site Configured for Remote Users Using Access Gateway

To configure a Web interface site for remote users using Access Gateway by using the configuration utility

1. In the navigation pane, click Web Interface.
2. In the details pane, click Web Interface Wizard.
3. On the wizard Introduction page, click Next.
4. On the wizard Configure Web Interface Site page, configure the following parameters:
   - Site Path* (You cannot change the name of an existing Web interface site.)
   - Site Type
   - Published Resource Type
   - Kiosk Mode
   - Authentication Methods
   - Login Title
   - Web Session Timeout
   - Enable access through receiver client

   * A required parameter.
5. In Default Access Methods, select the Gateway Direct or Gateway Alternate or Gateway Translated option and configure the following parameters:
   - Authentication Point
   - Access Gateway URL
   - Add DNS Entry
   - Trust SSL Certificate
   - STA Server URL
   - STA Server URL (2)
   - Session Reliability
   - Use two STA Servers
6. Click Next.
7. On the wizard's Configure Access Methods page, do one of the following:
   - To set an access method for a client IP address or network, click Add.

- To change the access method for a client IP address or network, select the association, and then click Open.

8. In the Configure Access Method dialog box, configure the following parameters:
   - Client IP Address* (You cannot change this parameter after setting it.)
   - Netmask (You cannot change this parameter after setting it.)
   - Access Method

   * A required parameter.

   Note: Before you configure access method based on the client IP address, you must enable USIP mode on the web interface service to make the client's IP address available with the web interface.
9. Click Next.
10. On the wizard's Configure Address Translations page, click Add for adding a mapping between an Internal IP address and an external IP address.

    Note: The Configure Address Translations page appears on the wizard when you set the Translated access method for a Client's IP address or network.
11. In the Configure Address Translations dialog box, configure the following parameters:
    - Internal IP Address
    - Internal Port
    - External IP Address
    - External Port
    - Access Type

    * A required parameter.
12. Click Next.
13. On the wizard's Configure XenApp/XenDesktop Farm page, do one of the following:
    - To add a XenApp or XenDesktop farm, click Add.
    - To modify an existing XenApp or XenDesktop farm, select the farm, and then click Open.
14. In the Create XenApp/XenDesktop Farm or Configure XenApp/XenDesktop Farm dialog box, configure the following parameters:
    - Name* (You cannot change the name of an existing XenApp or XenDesktop farm.)
    - XML Service Addresses*
    - XML Service Port
    - Transport

- Load Balance

* A required parameter.

15. Click Next, and then click Finish.

16. Verify that the Web interface site you configured is correct by selecting the site and viewing the Details section at the bottom of the pane. To view the Web interface site, in the navigation pane, expand System, expand Web Interface, and then click Sites.

To configure a Web interface site for remote users using Access Gateway by using the command line interface

1. Add a Web interface site. Set GatewayDirect or GatewayAlternate or GatewayTranslated for the defaultAccessMethod parameter. At the command prompt, type:

   add wi site <sitePath> <agURL> <staURL> -sessionReliability (ON | OFF) -useTwoTickets (ON | OFF) -secondSTAURL <string> -authenticationPoint (WebInterface | AccessGateway) -siteType (XenAppWeb | XenAppServices) -publishedResourceType (Online | Offline | DualMode) -kioskMode (ON | OFF)-wiAuthenticationMethods (Explicit | Anonymous) -webSessionTimeout <positive_integer> -defaultAccessMethod <defaultAccessMethod> -loginTitle <string>

   Example

   > add wi site WINS1 https://ag.mycompany.com http://ag.staserver.com -sessionReliability OFF -auther

2. (Optional) Set an access method for a Client's IP address or network. At the command prompt, type:

   bind wi site <sitePath> -accessMethod <accessMethod> -clientIpAddress <ip_addr> -clientNetMask <netmask>

3. If you have set the Translated access method for a Client's IP address or network then provide Internal IP and external IP address mappings. At the command prompt, type:

   bind wi site <sitePath> -translationInternalIp <ip_addr> -translationInternalPort <port|*> -translationExternalIp <ip_addr> -translationExternalPort <port|*> [-accessType <accessType>]

4. Bind XenApp or XenDesktop farms to the Web interface site. At the command prompt, type:

   bind wi site <sitePath> <farmName> <xmlServerAddresses> -xmlPort <value> -transport (HTTP | HTTPS) -loadBalance (ON | OFF)

   Example

   > bind wi site WINS1 XA1 10.102.46.6 -xmlPort 80 -transport HTTP -LoadBalance OFF
   > bind wi site WINS1 XD1 10.102.46.50 -xmlPort 80 -transport HTTP -LoadBalance OFF

Parameter Descriptions (of commands listed in the CLI procedure)

add wi site

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind wi site

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Using Smart Card Authentication for Web Interface through Access Gateway

The web interface on the NetScaler appliance supports single sign-on with a smart card through Access Gateway. You log on to Access Gateway by using a valid client certificate, either served from the local certificate store or from a smart card. After successful authentication, you are redirected to the web interface.

Requirements

- Make sure that you install the latest web interface tar file (nswi-1.5.tgz). This tar file provides support for smart card authentication.
- You must configure Delegation on the Active Directory. Follow the **Active Directory Configuration** section under **Procedure**, as described in the article at http://support.citrix.com/article/CTX124603.

To use smart card authentication for a web interface site through Access Gateway by using the configuration utility

1. In the navigation pane, click Web Interface.
2. In the details pane, click Web Interface Wizard.
3. On the wizard Introduction page, click Next.
4. On the wizard Configure Web Interface Site page, configure the following parameters:
   - Site Type
   - Site Path
   - Published Resource Type
   - Authentication Methods
   - Login Title
   - Language
   - Web Session Timeout
   - Kiosk Mode
5. Select GatewayDirect as the Default Access Method.
6. Select Access Gateway as the Authentication Point.
7. Select or create a Access Gateway Vserver. For more information, see "http://support.citrix.com/proddocs/topic/access-gateway-10/agee-config-settings-ag-wizard-tsk.html."
8. Click Settings to set the ICA mode, SSO, and WIhome.
9. Select SmartCard as the Access Gateway Authentication Method.
10. Click the SmartCard Settings link to configure certificate-based authentication on Access Gateway. You can skip these steps if certificate-based authentication is already configured on Access Gateway. In the Smart Card Settings wizard do the following:
    a. Specify the CA certificate. Install a CA certificate or use an already installed certificate for the Access Gateway virtual server to authenticate the client certificate.
    b. Configure authentication policies. Create a certificate-based authentication policy and bind it to Access Gateway vserver as follows:
       i. Click Insert Policy. In the Policy Name column, select New Policy.
       ii. In the Create Authentication Policy dialog box, specify a name for the policy, select Authentication Type as CERT, and click New.

iii. In the Create Authentication Server dialog box, specify the server Name and the User Name Field and click Create.

iv. Bind the policy to the Access Gateway Vserver with **ns_true** as expression and default priority.

c. Configure SSL-based client authentication with Client Certificate set as Optional.

d. Click Finish.

11. Continue with the wizard as described in "Configuring a Web Interface Site for Remote Users Using Access Gateway."

To use smart card authentication for a web interface site through Access Gateway by using the command line interface

At the command prompt, type:

add wi site <sitePath> <agURL> <staURL> -authenticationPoint AccessGateway -agAuthenticationMethod SmartCard -defaultAccessMethod GatewayDirect

Additionally, smart card support on web interface requires certificate-based authentication on the Access GatewayAdditionally, smart card support on web interface requires certificate-based authentication on the Access Gateway. If you do not have certificate-based authentication already configured on the Access Gateway vserver, do the following:

1. Configure an Access Gateway vserver and bind the server and CA certificate to it.

   add vpn vserver <*vpnvserver_name*> SSL <*AccessGateway_VIP*> <*port*>

   bind ssl vserver <*vpnvserver_name*> -certkeyName <*Server_Cert_Key_Pair*>

   bind ssl vserver <*vpnvserver_name*> -certkeyName <*Root_Cert_as_CKP*> -CA

   set ssl vserver <*vpnvserver_name*> -clientAuth ENABLED -clientCert Optional

   add dns nameserver <*dns_server_ip*>

2. Configure a certificate-based authentication policy and bind itcertAction_name to the Access Gateway vserver.

   add authentication certAction <certAction_name> -userNameField <string>

   add authentication certPolicy <*certPolicy_name*> <*rule*> <*certAction_name*>

   bind vpn vserver <vserver_name> -policy <*certPolicy_name*>

3. Configure the web interface site in ICA proxy mode through a session policy and then bind it to Access Gateway vserver.

add vpn sessionAction <*sessionAction_name*> -defaultAuthorizationAction ALLOW -SSO ON -wihome "<WI_URL>" -wiPortalMode NORMAL -icaproxy ON

add vpn sessionPolicy <*sessionPolicy_name*> <*rule*> <*sessionAction_name*>

bind vpn vserver <*vpnvserver_name*> -policyName <*sessionPolicy_name*>

bind vpn vserver <*vpnvserver_name*> -staServer *"<sta_server_url>"*

Parameter Descriptions (of commands listed in the CLI procedure)

add wi site

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add vpn vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind ssl vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

set ssl vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add dns nameserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add authentication certAction

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add authentication certPolicy

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

bind vpn vserver

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add vpn sessionAction

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

add vpn sessionPolicy

No parameters provided in this topic or the command has no parameters. View description(s) in command reference Top

Using the WebInterface.conf Dialog Box

The WebInterface.conf dialog box in the configuration utility displays the content of the webinterface.conf file for a Web Interface site.

You can do the following from this dialog box:

- Edit the WebInterface.conf file and save the changes.
- Search the file's content for instances of a text string.
- Easily save the WebInterface.conf file to your local computer.

To search a string in the webinterface.conf file by using the configuration utility

1. In the navigation pane, expand Web Interface, and then click Sites, select the web interface site, and click WebInterface.conf.
2. In the WebInterface.conf dialog box, use the following controls:
    - Find. Displays the following search options that you can use to find one or more instances of a text string in a configuration:
        - Look for. Provides a space for you to type the text string that you want to locate in the configuration. As you type the text, the first instance is displayed. If the word you are looking for is not in the file, the Look for text box will change color.
        - Next. Finds and highlights the next occurrence of the text string you typed in Look for.
        - Previous. Finds and highlights the previous occurrence of the text string you typed in Look for.
        - Mark All. Highlights all instances of the text string at one time you typed in Look for. Scroll to review each highlighted instance.

To save the content of the webinterface.conf to your local system by using the configuration utility

1. In the navigation pane, expand Web Interface, and then click Sites, click WebInterface.conf and select Save output text to a file.

Using the config.xml Dialog Box

The Config.xml dialog box in the configuration utility displays the content of the config.xml file for a Web Interface site of site type XenApp/XenDesktop Services Site.

You can do the following from this dialog box:

- Edit the config.xml file and save the changes.
- Search the file's content for instances of a text string.
- Easily save the config.xml file to your local computer.

To search a string in the config.xml file by using the configuration utility

1. In the navigation pane, expand Web Interface, and then click Sites, select XenApp/XenDesktop services site, and click Config.xml.
2. In the Config.xml dialog box, use the following controls:
    - Find. Displays the following search options that you can use to find one or more instances of a text string in a configuration:
        - Look for. Provides a space for you to type the text string that you want to locate in the configuration. As you type the text, the first instance is displayed. If the word you are looking for is not in the file, the Look for text box will change color.
        - Next. Finds and highlights the next occurrence of the text string you typed in Look for.
        - Previous. Finds and highlights the previous occurrence of the text string you typed in Look for.
        - Mark All. Highlights all instances of the text string at one time you typed in Look for. Scroll to review each highlighted instance.

To save the content of the config.xml to the local system by using the configuration utility

1. In the navigation pane, expand Web Interface, and then click Sites, select XenApp/XenDesktop Services Site.
2. Click Config.xml and select Save output text to a file.

Traffic Management

2015-05-17 05:04:23 UTC

Contents

Traffic Management

The following topics cover configuration and installation information for NetScaler traffic management features.

Cache Redirection	Analyzes incoming requests and forwards the requests for already cached data to cache servers. Dynamic HTTP requests and non-cacheable requests are forwarded to the origin servers. Cache redirection is a policy-based feature.
Content Switching	Analyzes client requests and redirects the requests to specific servers on the basis of geographical area, authorization credentials, and device from which the request was initiated.
DataStream	Ensures optimal distribution of traffic from the application and web servers to the database servers. Enables you to segment traffic according to information in the SQL query and on the basis of database names, user names, character sets, and packet size.
Domain Name System	Provides authoritative domain name server (ADNS server) functionality for a domain. The NetScaler appliance functions as a DNS end resolver and forwarder, and also helps in name resolution when fully qualified domain names are not configured.
Firewall Load Balancing	Distributes the traffic across multiple firewalls, providing fault tolerance, increased throughput, and high availability.
Global Server Load Balancing	Enables disaster recovery and ensures continuous availability of applications by protecting against points of failure in a wide area network (WAN).
Link Load Balancing	Load balances outbound traffic across multiple Internet connections to transmit packets seamlessly over the best possible link.
Load Balancing	Distributes user requests for web pages and other protected applications across multiple servers to prevent server overloading and failure. Load balancing also provides fault tolerance.
SSL Offload and Acceleration	Offloads SSL processing from a server to the NetScaler appliance to accelerate SSL transactions.
Web 2.0 Push	Offloads connection management from Web 2.0 servers. Instead of having to maintain a long-lived connection to each client, a Web 2.0 server can maintain a single connection to the NetScaler appliance. The appliance relays the server's data to waiting clients over the connections that it maintains with them.

Cache Redirection

In a typical deployment, different clients ask web servers for the same content repeatedly. To relieve the origin web server of processing each request, a NetScaler® appliance with cache redirection enabled can serve this content from a cache server instead of from the origin server.

The NetScaler analyzes incoming requests, sends requests for cacheable data to cache servers, and sends non-cacheable requests and dynamic HTTP requests to origin servers.

Cache redirection is a policy-based feature. By default, requests that match a policy are sent to the origin server, and all other requests are sent to a cache server. For testing or maintenance, you might want to skip policy evaluation and direct all requests to the cache or to the origin server.

You can combine content switching with cache redirection to cache selective content and serve content from specific cache servers for specific types of requested content.

A NetScaler configured for cache redirection can be deployed at the edge of a network, in front of the origin server, or anywhere along the network backbone. In an edge deployment, commonly used by Internet Service Providers (ISPs), cable companies, content delivery distribution networks, and enterprise networks, the NetScaler resides directly in front of the clients. In a server-side deployment, the NetScaler is closer to the origin servers.

Cache redirection is used most commonly with the HTTP service type, but it also supports the secure HTTPS protocol.

Cache Redirection

In a typical deployment, different clients ask web servers for the same content repeatedly. To relieve the origin web server of processing each request, a NetScaler® appliance with cache redirection enabled can serve this content from a cache server instead of from the origin server.

The NetScaler analyzes incoming requests, sends requests for cacheable data to cache servers, and sends non-cacheable requests and dynamic HTTP requests to origin servers.

Cache redirection is a policy-based feature. By default, requests that match a policy are sent to the origin server, and all other requests are sent to a cache server. For testing or maintenance, you might want to skip policy evaluation and direct all requests to the cache or to the origin server.

You can combine content switching with cache redirection to cache selective content and serve content from specific cache servers for specific types of requested content.

A NetScaler configured for cache redirection can be deployed at the edge of a network, in front of the origin server, or anywhere along the network backbone. In an edge deployment, commonly used by Internet Service Providers (ISPs), cable companies, content delivery distribution networks, and enterprise networks, the NetScaler resides directly in front of the clients. In a server-side deployment, the NetScaler is closer to the origin servers.

Cache redirection is used most commonly with the HTTP service type, but it also supports the secure HTTPS protocol.

Cache Redirection Policies

A cache redirection virtual server applies cache redirection policies to each incoming request. By default, if a request matches one of the configured policies, it is considered non-cacheable, and the NetScaler appliance sends it to the origin server. Other requests are sent to a cache server. This behavior can be reversed, so that requests that match configured cache redirection policies are sent to cache servers.

The NetScaler provides a set of policies for cache redirection. If these built-in policies are not adequate for your deployment, you can configure user-defined cache redirection policies.

Note: Once you have determined which built-in cache redirection policies to use, or have created user-defined policies, proceed with configuring cache redirection. To use this feature, you must configure at least one cache redirection virtual server, and, for normal operation, you must bind at least one cache redirection policy to that virtual server.

Displaying the Built-in Cache Redirection Policies

You can display the available cache redirection polices by using the command line interface or the configuration utility.

To display the built-in cache redirection policies by using the command line interface

At the command prompt, type:

show cr policy [<policyName>]

Example

```
> show cr policy
1)      Cache-By-Pass RULE: NS_NON_GET          Policy:bypass-non-get
2)      Cache-By-Pass RULE: (NS_CACHECONTROL_NOSTORE || NS_CACHECONTROL_NOCACHE || NS_HEADER_
3)      Cache-By-Pass RULE: (NS_EXT_CGI || NS_EXT_ASP || NS_EXT_EXE || NS_EXT_CFM || NS_EXT_EX || N
4)      Cache-By-Pass RULE: NS_URL_TOKENS       Policy:bypass-urltokens
5)      Cache-By-Pass RULE: (NS_HEADER_COOKIE && NS_EXT_NOT_GIF && NS_EXT_NOT_JPEG)     Policy:byp
 Done
>
```

To display the built-in cache redirection policies by using the configuration utility

1. In the navigation pane, expand Cache Redirection, and then click Policies. The configured cache redirection policies appear in the details pane.

2. Select one of the configured policies to view details.

Configuring a Cache Redirection Policy

A cache redirection policy includes one or more expressions (also called *rules*). Each expression represents a condition that is evaluated when the client request is compared to the policy.

You do not explicitly configure actions for cache redirection policies. By default, the NetScaler considers any request that matches a policy to be non-cacheable and directs the request to the origin server instead of the cache.

Cache redirection uses the *classic policy* format. Each policy has a name and includes an expression or a set of expressions that are combined by using logical operators.

To add a cache redirection policy by using the command line interface

At the command prompt, type the following commands to add a cache redirection policy and verify the configuration:

- add cr policy <policyName> -rule <expression>
- show cr policy [<policyName>]

Examples

Policy with a simple expression:

```
> add cr policy Policy-CRD-1 -rule "REQ.HTTP.URL != /*.jpeg"
 Done
> show cr policy Policy-CRD-1
        Cache-By-Pass RULE: REQ.HTTP.URL != '/*.jpeg'   Policy:Policy-CRD-1
 Done
>
```

Policy with a compound expression:

```
> add cr policy Policy-CRD-2 -rule "REQ.HTTP.METHOD == POST && (REQ.HTTP.URL == /*.cgi || REQ.HTTP.U
 Done
> show cr policy Policy-CRD-2
        Cache-By-Pass RULE: REQ.HTTP.METHOD == POST && (REQ.HTTP.URL == '/*.cgi' || REQ.HTTP.URL != '/
 Done
>
```

Policy that evaluates a header:

```
> add cr policy Policy-CRD-3 -rule "REQ.HTTP.HEADER If-Modified-Since EXISTS"
 Done
> show cr policy Policy-CRD-3
        Cache-By-Pass RULE: REQ.HTTP.HEADER If-Modified-Since EXISTS    Policy:Policy-CRD-3
 Done
>
```

To modify or remove a cache redirection policy by using the command line interface

- To modify a cache redirection policy, use the set cr policy command, which is just like using the add cr policy command, except that you enter the name of an existing policy.
- To remove a policy, use the rm cr policy command, which accepts only the <name> argument. You can only remove a cache redirection policy that is not bound to a cache redirection virtual server. If the policy is bound to a virtual server, you must first unbind the policy, and then remove it from the NetScaler.

For details on unbinding a cache redirection policy, see "Unbinding a Policy from a Cache Redirection Virtual Server."

Parameters for creating a cache redirection policy

policyName

Name of the cache redirection policy. This is a mandatory parameter, and the value cannot be changed after the policy is created.

rule

An expression that the NetScaler evaluates to identify non-cacheable requests. Can consist of multiple expressions joined by `AND` and `OR` operators.

To configure a cache redirection policy with a simple expression by using the configuration utility

1. In the navigation pane, expand Cache Redirection, and then click Policies.
2. In the details pane, click Add.
3. In the Create Cache Redirection Policy dialog box, in the Name* text box, type the name of the policy, and then in the Expression area, click Add.
4. To configure a simple expression, enter the expression. Following is an example of an expression that checks for a .jpeg extension in a URL:
   - Expression Type-General
   - Flow Type -REQ
   - Protocol -HTTP
   - Qualifier -URL
   - Operator - !=
   - Value* - /*.jpeg

   The simple expression in the following example checks for an If-Modified-Since header in a request:
   - Expression Type -General
   - Flow Type -REQ
   - Protocol -HTTP
   - Qualifier -HEADER
   - Operator -EXISTS
   - Header Name -If-Modified-Since
5. When you are finished entering the expression, click OK or Create, and then click Close.

To configure a cache redirection policy with a compound expression by using the configuration utility

1. In the navigation pane, expand Cache Redirection, and then click Policies.
2. In the details pane, click Add.
3. In the Name text box, enter a name for the policy.

   The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), and underscore (_) symbols. You should choose a name that will make it easy for others to tell what type of content this policy was created to detect.

4. Choose the type of compound expression that you want to create. Your choices are:

   - **Match Any Expression**. The policy matches the traffic if one or more individual expressions match the traffic.
   - **Match All Expressions**. The policy matches the traffic only if every individual expression matches the traffic.
   - **Tabular Expressions**. Switches the Expressions list to a tabular format with three columns. In the rightmost column, you place one of the following operators:
     - The AND [&&] operator, to require that, to match the policy, a request match both the current expression and the following expression.
     - The OR [||] operator, to require that, to match the policy, a request match either the current expression or the following expression, or both. Only if the request does not match either expression does it not match the policy.

     You can also group expressions in nested subgroups by selecting an existing expression and clicking one of the following operators:

     - The BEGIN SUBGROUP [+ ( ] operator, which tells the NetScaler appliance to begin a nested subgroup with the selected expression. (To remove this operator from the expression, click -(.)
     - The END SUBGROUP [+)] operator, which tells the NetScaler appliance to end the current nested subgroup with the selected expression. (To remove this operator from the expression, click -) .)
   - **Advanced Free-Form**. Switches off the Expressions Editor entirely and turns the Expressions list into a text area in which you type your compound expression. This is both the most powerful and the most difficult method of creating a policy expression, and is recommended only for those thoroughly familiar with the NetScaler classic expressions language.

     For more information about creating classic expressions in the Advanced Free-Form text area, see "Configuring Classic Policies and Expressions".

     Caution: If you switch to Advanced Free Form expression editing mode, you cannot switch back to any of the other modes. Do not choose this expression

editing mode unless you are sure that is what you want to do.

5. If you chose Match Any Expression, Match All Expressions, or Tabular Expressions, click Add to display the Add Expression dialog box.

   You should leave the expression type set to General for cache redirection policies.

6. In the Flow Type drop-down list, choose a flow type for your expression.

   The flow type determines whether the policy examines incoming or outgoing connections. You have two choices:

   - **REQ**. Configures the NetScaler appliance to examine incoming connections, or requests.
   - **RES**. Configures the appliance to examine outgoing connections, or responses.

7. In the Protocol drop-down list, choose a protocol for your expression.

   The protocol determines the type of information that the policy examines in the request or response. Depending upon whether you chose REQ or RES in the previous drop-down list, either all four of the following choices, or three of them, are available:

   - **HTTP**. Configures the appliance to examine the HTTP header.
   - **SSL**. Configures the appliance to examine the SSL client certificate. Available only if you chose REQ (requests) in the previous drop-down list.
   - **TCP**. Configures the appliance to examine the TCP header.
   - **IP**. Configures the appliance to examine the source or destination IP.

8. Choose a qualifier for your expression from the Qualifier drop-down list.

   The contents of the Qualifier drop-down list depend on which protocol you chose. The following table describes the choices available for each protocol.

   Table 1. Cache Redirection Policy Qualifiers Available for Each Protocol

Protocol	Qualifier	Definition
HTTP	METHOD	The HTTP method used in the request.

	URL	The contents of the URL header.
	URLTOKENS	The URL tokens in the HTTP header.
	VERSION	The HTTP version of the connection.
	HEADER	The header portion of the HTTP request.
	URLLEN	The length of the contents of the URL header.
	URLQUERY	The query portion of the contents of the URL header.
	URLQUERYLEN	The length of the query portion of the URL header.
SSL	CLIENT.CERT	The SSL client certificate as a whole.
	CLIENT.CERT.SUBJECT	The contents of the client certificate subject field.
	CLIENT.CERT.ISSUER	The client certificate issuer.
	CLIENT.CERT.SIGALGO	The signature algorithm used in the client certificate.
	CLIENT.CERT.VERSION	The client certificate version.
	CLIENT.CERT.VALIDFROM	The date from which the client certificate is valid. (The start date.)
	CLIENT.CERT.VALIDTO	The date after which the client certificate is no longer valid. (The end date.)
	CLIENT.CERT.SERIALNUMBER	The client certificate serial number.
	CLIENT.CIPHER.TYPE	The encryption method used in the client certificate.
	CLIENT.CIPHER.BITS	The number of significant bits in the encryption key.
	CLIENT.SSL.VERSION	The SSL version of the client certificate.

TCP	SOURCEPORT	The source port of the TCP connection.
	DESTPORT	The destination port of the TCP connection.
	MSS	The maximum segment size (MSS) of the TCP connection.
IP	SOURCEIP	The source IP of the connection.
	DESTIP	The destination IP of the connection.

9. Choose the operator for your expression from the Operator drop-down list.

   Your choices depend on the qualifier you chose in the previous step. The complete list of operators that can appear in this drop-down list is:

   - == . Matches the following text string exactly.
   - != . Does not match the following text string.
   - > . Is greater than the following integer.
   - CONTAINS . Contains the following text string.
   - CONTENTS . The contents of the designated header, URL, or URL query.
   - EXISTS . The specified header or query exists.
   - NOTCONTAINS . Does not contain the following text string.
   - NOTEXISTS . The specified header or query does not exist.

   If you want this policy to operate on requests sent to a specific Host, you can leave the default, the equals (==) sign.

10. If the Value text box is visible, type the appropriate string or number into the text box.

    For example, if you want this policy to select requests sent to the host `shopping.example.com`, you would type that string in the Value text box.

11. If you chose HEADER as the qualifier, type the header you want in the Header Name text box.

12. Click OK to add your expression to the Expression list.

13. Repeat steps 4 through 11 to create additional expressions.

14. Click Close to close the Add Expression dialog box and return to the Create Cache Redirection Policy dialog box.

Built-in Cache Redirection Policies

The NetScaler appliance provides built-in cache redirection policies that handle typical cache requests. These policies are based on HTTP methods, the URL or URL tokens of the incoming request, the HTTP version, or the HTTP headers in the request and their values.

Built-in cache redirection policies can be directly bound to a virtual server and do not need further configuration.

Cache redirection policies use the simpler of two NetScaler expressions languages, called *classic expressions*. For a complete description of classic expressions and how to configure them, see http://support.citrix.com/article/CTX132362.

The NetScaler provides the following built-in cache redirection policies

built in Policy Name	Description
bypass-non-get	Bypass the cache if the request uses an HTTP method other than GET.
bypass-cache-control	Bypass the cache if the request header contains a Cache-Control: no-cache or Cache-Control: no-store header, of if the HTTP request contains a pragma header.
bypass-dynamic-url	Bypass the cache if the URL suggests that the content is dynamic, as indicated by the presence of any of the following extensions: · cgi · asp · exe · cfm · ex · shtml · htx Also bypass the cache if the URL starts with any of the following: · /cgi-bin/ · /bin/ · /exec/
bypass-urltokens	Bypass the cache because the request is dynamic, as indicated by one of the following tokens in the URL: ?, !, or =.

bypass-cookie	Bypass the cache for any URL that has a cookie header and an extension other than .gif or .jpg.

Cache Redirection Configurations

Depending on your deployment and network topology, you can configure one of the following types of cache redirection:

- **Transparent**. A transparent cache can reside on a variety of points along a network backbone to alleviate traffic along the delivery route. In transparent mode, the cache redirection virtual server intercepts all traffic flowing to the NetScaler appliance and applies cache redirection policies to determine whether content should be served from the cache or from the origin server.

- **Forward proxy**. A forward proxy cache server resides on the edge of an enterprise LAN and faces the WAN. In the forward proxy mode, the cache redirection virtual server resolves the hostname of the incoming request by using a DNS server and forwards requests for non-cacheable content to the resolved origin servers. Cacheable requests are sent to the configured cache servers.

- **Reverse proxy**. Reverse proxy caches are configured for specific origin servers. Incoming traffic directed to the reverse proxy, can either be served from a cache server or be sent to the origin server with or without modification to the URL.

Configuring Transparent Redirection

When you configure transparent cache redirection, the NetScaler appliance evaluates all traffic it receives, to determine whether it is cacheable. This mode alleviates traffic along the delivery route and is often used when the cache server resides on the backbone of an ISP or carrier.

By default, cacheable requests are sent to a cache server, and non-cacheable requests to the origin server. For example, when the NetScaler appliance receives a request that is directed to a web server, it compares the HTTP headers in the request with a set of policy expressions. If the request does not match the policy, the appliance forwards the request to a cache server. If the response does match a policy, the appliance forwards the request, unchanged, to the web server.

For details on how to modify this default behavior, see "Directing Policy Hits to the Cache instead of the Origin."

To configure transparent redirection, first enable cache redirection and load balancing, and configure edge mode. Then, create a cache redirection virtual server with a wildcard IP address (*), so that this virtual server can receive traffic coming to the NetScaler on any IP address the appliance owns. To this virtual server, bind cache redirection policies that describe the types of requests that should not be cached. Then, create a load balancing virtual server that will receive traffic from the cache redirection virtual server for cacheable requests. Finally, create a service that represents a physical cache server and bind it to the load balancing virtual server.

Enabling Cache Redirection and Load Balancing

The NetScaler cache redirection and load balancing features are not enabled by default. They must be enabled before any cache redirection configuration can take effect.

To enable cache redirection and load balancing by using the command line interface

At the command prompt, type the following command to enable cache redirection and load balancing and verify the settings:

- enable ns feature `cr lb`
- show ns feature

Example

```
> enable ns feature cr lb
 Done
> show ns feature

      Feature                Acronym          Status
      -------                -------          ------
 1)   Web Logging              WL               ON
 2)   Surge Protection         SP               ON
 3)   Load Balancing           LB               ON
 4)   Content Switching         CS               ON
 5)   Cache Redirection         CR               ON
 6)   Sure Connect

         ...
         ...
         ...

 23)   HTML Injection           HTMLInjection       ON
 24)   NetScaler Push           push                OF
 Done
>
```

To enable cache redirection and load balancing by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. To enable cache redirection, in the details pane, under Modes and Features, click Configure advanced features.
    a. In Configure Advanced Features dialog box, select the check box next to the Cache Redirection, and then click OK.
    b. In Enable/Disable Feature(s)? dialog box, click Yes.
3. To enable load balancing, in the details pane, under Modes and Features, click Configure basic features.
    a. In Configure Basic Features dialog box, select the check box next to the Load Balancing, and then click OK.
    b. In Enable/Disable Feature(s)? dialog box, click Yes.

Configuring Edge Mode

When deployed at the edge of a network, the NetScaler appliance dynamically learns about the servers on that network. Edge mode enables the appliance to dynamically learn about up to 40,000 HTTP servers and proxy TCP connections for these servers.

This mode turns off collection of statistics for the dynamically learned services and is typically used in transparent deployments for cache redirection.

To enable edge mode by using the command line interface

At the command prompt, type the following commands to enable edge mode and verify the setting:

- enable ns mode Edge
- show ns mode

Example

```
> enable ns mode edge
 Done

> show ns mode

      Mode                    Acronym          Status
      -------                 -------          ------
        ...
        ...
        ...
 6)   MAC-based forwarding       MBF              ON
 7)   Edge configuration         Edge             ON
 8)   Use Subnet IP              USNIP            OFF
        ...
        ...
        ...
 16)  Bridge BPDUs               BridgeBPDUs      OFF
 Done
>
```

Parameters for enabling edge mode

Mode

The name of the mode to be enabled. This is a mandatory argument.

To enable edge mode by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features, click Configure modes.
3. In Configure Modes dialog box, select the check box next to the Edge Configuration, and then click OK.
4. In Enable/Disable Feature(s)? dialog box, click Yes.

Configuring a Cache Redirection Virtual Server

By default, a cache redirection virtual server forwards cacheable requests to the load balancing virtual server for the cache, and forwards non-cacheable requests to the origin server (except in a reverse proxy configuration, in which non-cacheable requests are sent to a load balancing virtual server). There are three types of cache redirection virtual servers: transparent, forward proxy, and reverse proxy.

A transparent cache redirection virtual server uses an IP address of * and a port number, usually 80, that can accept HTTP traffic sent to any IP address that the NetScaler represents. As a result, you can configure only one transparent cache redirection virtual server. Any additional cache redirection virtual servers that you configure must be forward proxy or reverse proxy redirection servers.

To add a cache redirection virtual server in transparent mode by using the command line interface

At the command prompt, type the following commands to add a cache redirection virtual server and verify the configuration:

- add cr vserver <name> <serviceType> [<IPAddress> <port>] [-cacheType <cacheType>] [-redirect <redirect>] [-cacheVserver <string>]
- show cr vserver [<name>]

Example

```
add cr vserver Vserver-CRD-1 HTTP * 80 -cacheType TRANSPARENT -redirect POLICY -cacheVserver Vserver-L
> show cr vserver Vserver-CRD-1
      Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
      State: UP  ARP:DISABLED
      Client Idle Timeout: 180 sec
      Down state flush: ENABLED
      Disable Primary Vserver On Down : DISABLED
      Default:       Content Precedence: RULE       Cache: TRANSPARENT
      On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
      Redirect: POLICY       Reuse: ON       Via: ON ARP: OFF
 Done
>
```

To modify or remove a cache redirection virtual server by using the command line interface

- To modify a virtual server, use the set cr vserver command, which is just like using the add cr vserver command, except that you enter the name of an existing virtual server.
- To remove a virtual server, use the rm cr vserver command, which accepts only the <name> argument.

Parameters for adding a cache redirection virtual server

name

Name of the cache redirection virtual server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the cache redirection virtual server is created. You should choose a name that helps identify the type of service being added. Maximum length of the name can be 127 characters.

serviceType

The type of data that the virtual server will handle. For typical web traffic, the protocol is HTTP. Possible Values: HTTP, SSL.

IPAddress

The IP address of the virtual server that you are adding. For transparent cache redirection, assign an asterisk (*) as the IP address, so that the virtual server listens on all IP addresses configured on the NetScaler.

port

The port number on which the virtual server receives traffic.

cacheType

The type of cache redirection you are configuring. Possible values: TRANSPARENT, REVERSE, FORWARD.

redirect

The redirect method to be used. Possible values: CACHE, ORIGIN, POLICY.

For normal operation, specify POLICY based redirection and bind appropriate cache redirection policies to the virtual server.

cacheVserver

The name of a load balancing virtual server to which this redirection virtual server sends cache requests.

To add a cache redirection virtual server in transparent mode by using the configuration utility

1. In the navigation pane, click Cache Redirection, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Cache Redirection) dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for adding a cache redirection virtual server” as shown:
   - Name*—name
   - Port*—port

   * A required parameter
4. In the Protocol drop-down list, select a supported protocol (for example, **HTTP**). If the virtual server is to receive traffic on a port other than the standard port for the selected protocol, enter a new value in the Port field.
5. Click the Advanced tab.
6. Verify that Cache Type is set to TRANSPARENT and Redirect is set to POLICY.
7. If you have already configured load balancing virtual servers for cache redirection, select a virtual server from the Cache Server drop-down list.
8. Click Create, and then click Close. The Cache Redirection Virtual Servers pane displays the new virtual server.
9. Select the new cache redirection virtual server to display the details of its configuration.

Binding Policies to the Cache Redirection Virtual Server

Cache redirection policies are not automatically bound to the cache redirection virtual server. A policy based cache redirection virtual server cannot function unless you bind at least one policy to it.

To bind policies to a cache redirection virtual server by using the command line interface

At the command prompt, type:

- bind cr vserver <name> -policyName <string>
- show cr vserver [<name>]

Example

```
> bind cr vserver Vserver-CRD-1 -policyName bypass-cache-control
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-dynamic-url
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-urltokens
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-cookie
 Done

> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: RULE        Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: bypass-dynamic-url
3)      Cache bypass  Policy: bypass-urltokens
4)      Cache bypass  Policy: bypass-cookie
 Done
>
```

Parameters for binding policies to a cache redirection virtual server

name

The name of the cache redirection virtual server you are binding the policy to.

policyName

The name of the policy being bound to the cache redirection virtual server. The policy must already be created on the NetScaler appliance before it is bound.

To bind a user-defined policy to a cache redirection virtual server by using the configuration utility

1. In the navigation pane, expand Cache Redirection and click Virtual Servers.
2. Click the virtual server that you want to configure, and click Open.
3. On the Policies tab, select type of the policy and then click Insert Policy.
4. Under Policy Name column, select the policy that you want to bind.
5. Click OK.

Unbinding a Policy from a Cache Redirection Virtual Server

When you unbind a policy from the cache redirection virtual server, the NetScaler appliance no longer applies the policy when evaluating client requests.

To unbind a policy from a cache redirection virtual server by using the command line interface

At the command prompt, type:

- unbind cr vserver <name> -policyName <string>
- show cr vserver [<name>]

Example

```
unbind cr vserver Vserver-CR-1 -policyName bypass-non-get
> show cr vserver Vserver-CRD-1
      Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
      State: UP  ARP:DISABLED
      Client Idle Timeout: 180 sec
      Down state flush: ENABLED
      Disable Primary Vserver On Down : DISABLED
      Default:       Content Precedence: RULE       Cache: TRANSPARENT
      On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
      Redirect: POLICY       Reuse: ON       Via: ON ARP: OFF

1)     Cache bypass  Policy: bypass-cache-control
 Done
>
```

To unbind a user-defined policy from a cache redirection virtual server by using the configuration utility

1. In the navigation pane, expand Cache Redirection and click Virtual Servers.
2. Click the virtual server that you want to configure, and then click Open.
3. On the Policies tab, under Policy Name, select the policy that you want to unbind.
4. Click Unbind Policy, and then click OK.

Creating a Load Balancing Virtual Server

The cache redirection virtual server on the NetScaler appliance can send requests to either a cache server farm, if the request is cacheable, or to the origin server farm if the request is not cacheable.

Each cache server is represented on the appliance by a service, which is bound to a load balancing virtual server that receives requests from the cache redirection virtual server and forwards those requests to the servers.

For details on configuring load balancing virtual servers and other configuration options, see "Load Balancing."

To create a load balancing virtual server by using the command line interface

At the command prompt, type the following commands to create a load balancing virtual server and verify the configuration:

- add lb vserver <name> <serviceType> [<IPAddress>] [<port>]
- show lb vserver [<name>]

Example

```
> add lb vserver Vserver-LB-CR HTTP 10.102.20.30 80
 Done
> show lb vserver Vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 00:00:08.470
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none
 Done
>
```

Parameters for creating a load balancing virtual server

name

The name of the virtual server being created.

serviceType

The type of traffic the virtual server will be receiving. For all web traffic, create virtual servers of type HTTP or, for secure Web traffic, HTTPS.

IPAddress

The IP address of the virtual server. This is the IP address that will receive incoming traffic.

port

The port number on which the incoming traffic will be received.

To create a load balancing virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Load Balancing) dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for creating a load balancing virtual server" as shown:
   - Name*-name
   - IP Address*- IPAddress
   - Port*-port

   * A required parameter
4. In the Protocol* drop down list, select a supported protocol (for example, **HTTP**). If the virtual server is to receive traffic on a port other than the well-known port for the selected protocol, enter a new value in the Port field.
5. Click Create, and then click Close. The Load Balancing Virtual Servers pane displays the new virtual server.

Configuring an HTTP Service

On the NetScaler appliance, a service represents a physical server on the network. In the transparent cache redirection configuration, the service represents the cache server. Cacheable requests are sent by the cache redirection virtual server to the load balancing virtual server, which in turn forwards each request to the correct service, which passes it on to the cache server.

To configure an HTTP service by using the command line interface

At the command prompt, type the following commands to create an HTTP service and verify the configuration:

- add service <name> <IP> <serviceType> <port> -cacheType <cacheType>
- show service [<name>]

Example

```
> add service Service-HTTP-1 10.102.29.40 HTTP 80 -cacheType TRANSPARENT
 Done
> show service Service-HTTP-1
      Service-HTTP-1 (10.102.29.40:80) - HTTP
      State: DOWN
      Last state change was at Fri Jul  2 09:14:17 2010
      Time since last state change: 0 days, 00:00:13.820
      Server Name: 10.102.29.40
      Server ID : 0   Monitor Threshold : 0
      Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
      Use Source IP: NO
      Client Keepalive(CKA): NO
      Access Down Service: NO
      TCP Buffering(TCPB): NO
      HTTP Compression(CMP): YES
      Idle timeout: Client: 180 sec   Server: 360 sec
      Client IP: DISABLED
      Cache Type: TRANSPARENT Redirect Mode:
      Cacheable: NO
      SC: OFF
      SP: ON
      Down state flush: ENABLED

1)     Monitor Name: tcp-default
            State: DOWN     Weight: 1
            Probes: 3       Failed [Total: 3 Current: 3]
            Last response: Failure - Time out during TCP connection establishment stage
```

```
                Response Time: N/A
 Done
>
```

To modify or remove a service by using the command line interface

- To modify a service, use the set service command, which is just like using the add service command, except that you enter the name of an existing service.
- To remove a service, use the rm service command, which accepts only the <name> argument.

Parameters for adding an HTTP service

name

The name of the service you are configuring. The name can begin with a letter, a number, or the underscore symbol, and can consist of from one to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should choose a name that helps identify the type of service being added. (Cannot be changed after the service has been created.)

IP

The physical IP address of the server that the service you are configuring represents. Make sure that the server is reachable by the NetScaler.

port

The port number on which the service sends and receives data to and from the server.

serviceType

The type of data that will be transferred between the NetScaler and the server. Typically, for web server caches, the serviceType is HTTP.

cacheType

The type of cache redirection you are configuring.

To add an HTTP service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for adding an HTTP service" as shown:
   - Service Name*—name
   - Server*— IP
   - Port*—port

   * A required parameter
4. In the Protocol* drop-down list, select a supported protocol (for example, **HTTP**).
5. Click Create, and then click Close.

Binding/Unbinding a Service to/from a Load Balancing Virtual Server

You must bind a service to the load balancing virtual server. This enables the load balancer to forward the request to the server that the service represents. If your configuration changes, you can unbind a service from the load balancing virtual server.

To bind a service to a load balancing virtual server by using the command line interface

At the command prompt, type:

- bind lb vserver <name> <serviceName>
- show lb vserver [<name>]

Example

```
> bind lb vserver vserver-LB-CR service-HTTP-1
 Done
> show lb vserver Vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 00:42:25.610
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1) Service-HTTP-1 (10.102.29.40: 80) - HTTP State: DOWN Weight: 1
 Done
>
```

To unbind a service from a load balancing virtual server by using the command line interface

To unbind a service, use the unbind lb vserver command instead of bind lb vserver.

Parameters for binding/unbinding a service to/from a load balancing virtual server

name

The virtual server name from which the service will be bound/unbound. This is a mandatory argument. Maximum Length: 127

serviceName

The service name (created with the addService command) that will be unbound. Maximum Length: 127

To bind/unbind a service from a load balancing virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server from which you want to bind/unbind the service, and then click Open.
3. On the Services tab, in the Active column, select/clear the check box next to the Service Name.
4. Click OK.

Disabling the Use the Proxy Port Setting for Transparent Caching

If the use source IP (USIP) option is disabled on a cache service configured on the NetScaler appliance, the appliance forwards client requests to the cache service by using a NetScaler-owned subnet IP (SNIP) address or mapped IP (MIP) address as the source IP address and a random port as the source port. The randomly selected port is called the proxy port.

However, if you want to configure a fully transparent cache (a cache configuration in which the cache service receives the client's IP address and port number), you must not only enable the USIP option, either globally or on the cache service, but also disable the Use Proxy Port setting, either globally or on the cache service. Disabling the Use Proxy Port setting enables the appliance to use the client's source port as the source port when it connects to the cache service, and ensures a fully transparent cache configuration.

For more information about configuring the Use Proxy Port option globally or on a service, see "Configuring the Source Port for Server-Side Connections."

Assigning a Port Range to the NetScaler

Sharing of the client IP address may create a conflict that makes network devices, such as routers, cache servers, origin servers, and other NetScaler appliances, unable to determine the appliance, and therefore the client, to which the response should be sent.

A method to solve this problem is to assign a source port range to the NetScaler appliance. This allotment enables network devices to unambiguously identify the NetScaler appliance that sent the request.

To assign a source port range to a NetScaler appliance by using the command line interface

At the command prompt, type:

set ns param -crPortRange <startPortNumber-endPortNumber>

Parameters for assigning source port range

startPortNumber

Lower limit of the port range

endPortNumber

Upper limit of the port range

The range should be from 1024 through 65535.

To assign a source port range to a NetScaler appliance by using the NetScaler configuration utility

1. In the navigation pane, click System, and then click Settings.
2. In the Settings group, click the Change global system settings link.
3. In the Cache Redirection Port Range group, specify the port range for the NetScaler by typing a port number for Start Port and a port number for End Port.
4. Click OK.

Enabling Load Balancing Virtual Servers to Redirect Requests to Cache

If a load balancing virtual server is configured to listen on a particular IP address and port combination, it takes precedence over the cache redirection virtual server for any requests destined for that address-port combination. Therefore, the cache redirection virtual server does not process those requests.

If you want to override this functionality and let the cache redirection virtual server decide whether the request should be served from the cache or not, configure the particular load balancing virtual server to be cacheable.

Such a configuration is typically used when an ISP uses a NetScaler appliance at the edge of its network and all traffic flows through the appliance.

To enable load balancing virtual servers to redirect requests to the cache by using the command line interface

At the command prompt, type:

- set lb vserver <name> [-cacheable (YES | NO)]
- show lb vserver [<name>]

Example

```
set lb vserver Vserver-LB-CR –cacheable YES
> show lb vserver vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 01:05:51.510
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Cacheable: YES  PQ: OFF SC: OFF
        Vserver IP and Port insertion: OFF
```

```
    Push: DISABLED  Push VServer:
    Push Multi Clients: NO
    Push Label Rule: none

1) Service-HTTP-1 (10.102.29.40: 80) - HTTP State: DOWN Weight: 1
 Done
```

For transparent cache redirection, the NetScaler intercepts all traffic and evaluates every request to determine whether it is cacheable. Non-cacheable requests are sent unchanged to the origin server.

When using transparent cache redirection, you may want to turn off cache redirection for load balancing virtual servers that always direct traffic to origin servers.

To turn off caching for a load balancing virtual server by using the command line interface

To turn off caching for a load balancing virtual, use the unset lb vserver command instead of set lb vserver. Specify a value of NO value for the **-cacheable** parameter**.**

To enable or disable load balancing virtual servers to redirect requests to the cache by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server from which you want to enable/disable the caching, and then click Open.
3. On the Advanced tab, select/clear Cache Redirection check box.
4. Click OK.

Configuring Forward Proxy Redirection

A forward proxy is a single point of contact for a client or group of clients. In this configuration, the NetScaler appliance redirects non-cacheable requests to an origin server and redirects cacheable requests to either a forward proxy cache or a transparent cache.

When the NetScaler is configured as a forward proxy, users must modify their browsers so that the browser sends requests to the forward proxy instead of the destination servers.

A forward proxy cache redirection virtual server on the NetScaler compares the request with a policy for caching. If the request is not cacheable, the NetScaler queries a DNS load balancing virtual server for resolution of the destination, and then sends the request to the origin server. If the request is cacheable, the NetScaler forwards the request to a load balancing virtual server for the cache.

The NetScaler relies on a host domain name or IP address in the request's HOST header to determine the requested destination. If there is no HOST header in the request, the appliance inserts a HOST header based on the destination IP address in the request.

Typically, the NetScaler appliance acts as a forward proxy in an enterprise LAN. In such a configuration, the appliance resides at the edge of an enterprise LAN and intercepts client requests before they are fanned out to the WAN. Configuring the appliance in the forward proxy mode reduces traffic on the WAN.

To configure forward proxy cache redirection, first enable load balancing and cache redirection on the NetScaler. Then, configure a DNS load balancing virtual server and associated services. Also configure a load balancing virtual server and bind to it appropriate services for the cache. Configure a forward proxy cache redirection virtual server and bind the DNS and load balancing virtual servers to it. You must also configure caching policies and bind them to the cache redirection virtual server. To complete the setup, configure the client browsers to use the forward proxy.

For details on how to enable cache redirection and load balancing on the NetScaler, see "Enabling Cache Redirection and Load Balancing."

For details on how to create a load balancing virtual server, see "Creating a Load Balancing Virtual Server."

For details on how to configure services that represent the cache server, see "Configuring an HTTP Service."

For details on how to bind the service to a virtual server, see "Binding Services to the Virtual Server."

For details on how to create a forward proxy cache redirection server, see "Configuring a Cache Redirection Virtual Server", and create a virtual server of type TRANSPARENT or FORWARD.

For details on binding cache redirection policies to the cache redirection virtual server, see "Configuring a Cache Redirection Policy."

Creating a DNS Service

A DNS service is a representation, on the NetScaler appliance, of a physical DNS server in the network. A DNS load balancing virtual server sends DNS requests to the DNS server in the network through such a service.

To create a DNS service by using the command line interface

At the command line, type the following commands to create a DNS service and verify the configuration :

- add service <name> <IP> <serviceType> <port>
- show service [<name>]

Example

```
add service Service-DNS-1 10.102.29.41 DNS 53
show service Service-DNS-1
        Service-DNS-1 (10.102.29.41:53) - DNS
        State: DOWN
        Last state change was at Fri Jul  2 10:14:32 2010
        Time since last state change: 0 days, 00:00:13.550
        Server Name: 10.102.29.41
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: ping-default
                State: DOWN     Weight: 1
                Probes: 3       Failed [Total: 3 Current: 3]
                Last response: Failure - Probe timed out.
                Response Time: 2000.0 millisec
 Done
```

Parameters for creating a DNS service

name

The name of the service you are configuring. The name can begin with a letter, a number, or the underscore symbol, and can consist of from one to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should choose a name that helps identify the type of service being added. (Cannot be changed after the service has been created.)

IP

The physical IP address of the server that the service you are configuring represents. Make sure that the server is reachable by the NetScaler.

port

The port number on which the service sends and receives data to and from the server.

serviceType

The type of data that will be transferred between the NetScaler and the server. Typically, for DNS service, the serviceType is DNS.

To add an DNS service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for creating a DNS service" as shown:
   - Service Name*—name
   - Server*—IP
   - Port*—port

   * A required parameter
4. In the Protocol* drop down list, select a supported protocol (for example, **DNS**).
5. Click Create, and then click Close.

Creating a DNS Load Balancing Virtual Server

The DNS virtual server enables the forward proxy to perform DNS resolution before forwarding a client request to an origin server. The DNS load balancing virtual server is associated with the DNS service that represents the physical DNS server on the network.

To create a DNS load balancing virtual server by using the command line interface

At the command line, type the following commands to create a DNS load balancing virtual server and verify the configuration:

- add lb vserver <name> <serviceType>
- show lb vserver [<name>]

Example

```
> add lb vserver Vserver-DNS-1 DNS
 Done
> show lb vserver Vserver-DNS-1
        Vserver-DNS-1 (0.0.0.0:0) - DNS Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 10:32:28 2010
        Time since last state change: 0 days, 00:00:08.10
        Effective State: DOWN  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
 Done
>
```

Parameters for creating a DNS load balancing virtual server

name

The name of the virtual server being created.

serviceType

The type of traffic the virtual server will be receiving.

To create a DNS load balancing virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Load Balancing) dialog box, in the Name box, type a name for the virtual server.
4. In the Protocol* drop down list, select a supported protocol (for example, **DNS**).
5. Click Create, and then click Close. The DNS Virtual Servers pane displays the new virtual server.

Binding the DNS Service to the Virtual Server

For the DNS server to respond to DNS requests, the service representing the DNS server must be bound to the DNS virtual server.

To bind the DNS service to the load balancing virtual server:

At the command prompt, type the following commands to bind the DNS service to the load balancing virtual server and verify the configuration:

- bind lb vserver <name> <serviceName>
- show lb vserver <name>

Example

```
> bind lb vserver Vserver-DNS-1 Service-DNS-1
 Done
> show lb vserver Vserver-DNS-1
        Vserver-DNS-1 (0.0.0.0:0) - DNS Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 10:32:28 2010
        Time since last state change: 0 days, 00:12:16.80
        Effective State: DOWN  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE

1) Service-DNS-1 (10.102.29.41: 53) - DNS State: DOWN   Weight: 1
 Done
>
```

To unbind a DNS service from the load balancing virtual server:

Use the unbind lb vserver command instead of bind lb vserver.

Parameters for Binding/Unbinding a DNS service to/from a load balancing virtual server

name

The name of the virtual server to/from which the service will be bound/unbound. This is a mandatory argument. Maximum Length: 127

serviceName

The name of the service (created with the addService command) that will be bound or unbound. Maximum Length: 127

To Bind/Unbind a DNS service to/from a load balancing virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server to/from which you want to bind/unbind the DNS service, and then click Open.
3. On the Services tab, in the Active column, select/clear the check box next to the Service Name.
4. Click OK.

Configuring a Client Web Browser to Use a Forward Proxy

When you configure the NetScaler appliance as forward proxy cache redirection virtual server in the network, you must configure the client Web browser to send requests to the forward proxy. Typically, when you use a forward proxy, the only route to the servers in the network is through the forward proxy.

Refer the documentation for your browser to configure the browser to use a forward proxy. Specify the IP address and port number of the forward proxy cache redirection virtual server for this configuration.

Configuring Reverse Proxy Redirection

A reverse proxy resides in front of one or more Web servers and shields the origin server from client requests. Often, a reverse proxy cache is a front-end for all client requests to a server. An administrator assigns a reverse proxy cache to a specific origin server. This is unlike transparent and forward proxy caches, which cache frequently requested content for all requests to any origin server, and the choice of a server is based on the request.

Unlike a transparent proxy cache, the reverse proxy cache has its own IP address and can replace destination domains and URLs in a non-cacheable request with new destination domains and URLs.

You can deploy reverse proxy cache redirection at the origin-server side or at the edge of a network. When deployed at the origin server, the reverse proxy cache redirection virtual server is a front-end for all requests to the origin server.

In the reverse proxy mode, when the NetScaler receives a request, a cache redirection virtual server evaluates the request and forwards it to either a load balancing virtual server for the cache or a load balancing virtual server for the origin. The incoming request can be transformed by changing the host header or the host URL before they it is sent to the backend server.

To configure reverse proxy cache redirection, first enable cache redirection and load balancing. Then, configure a load balancing virtual server and services to send cacheable requests to the cache servers. Also configure a load balancing virtual server and associated services for the origin servers. Then, configure a reverse proxy cache redirection virtual server and bind relevant cache redirection policies to it. Finally, configure mapping policies and bind them to the reverse proxy cache redirection virtual server.

The mapping policies have an associated action that enables the cache redirection virtual server to forward any non-cacheable request to the load balancing virtual server for the origin.

Be sure to create the default cache server destination.

For details on how to enable cache redirection and load balancing on the NetScaler, see "Enabling Cache Redirection and Load Balancing."

For details on how to create a load balancing virtual server, see "Creating a Load Balancing Virtual Server."

For details on how to configure services that represent the cache server, see "Configuring an HTTP Service."

For details on how to bind the service to a virtual server, see "Binding Services to the Virtual Server."

For details on how to create a reverse proxy cache redirection server, see "Configuring a Cache Redirection Virtual Server", and create a virtual server of type REVERSE.

For details on binding built-in cache redirection policies to the cache redirection virtual server, see "Binding Policies to the Cache Redirection Virtual Server."

Configuring Mapping Policies

If an incoming request is non-cacheable, the reverse-proxy cache redirection virtual server replaces the domain and URL in the request with the domain and URL of a target origin server and forwards the request to the load balancing virtual server for the origin.

A mapping policy enables the reverse proxy cache redirection virtual server to replace the destination domain and URL and forward the request to the load balancing virtual server for the origin.

A mapping policy must first translate the domain and the URL, and then pass the request on to the origin load balancing virtual server.

A mapping policy can map a domain, a URL prefix, and a URL suffix, as follows:

- Domain mapping: You can map a domain without a prefix or suffix. The domain mapping is the default mapping for the virtual server (for example, mapping www.mycompany.com to www.myrealcompany.com).
- Prefix mapping: You can replace a specified pattern prefixed as part of the URL (for example, mapping www.mycompany.com/sports/index.html to www.mycompany.com/news/index.html).
- Suffix mapping: You can replace the file suffix in the URL (for example, mapping www.mycompany.com/sports/index.html to www.mycompany.com/sports/index.asp).

The source and the destination strings being mapped must be similar. If you specify a source domain, you must specify a destination domain, and if you specify a source suffix, you must specify a destination suffix. Similarly, if you specify an exact URL from the source, the target URL must also be an exact URL.

Once you configure mapping policies for the reverse proxy mode, you must bind them to the cache redirection virtual server.

You can use combinations of the source URL, target URL, and source and target domains to configure all three types of domain mapping.

To configure a mapping policy for reverse proxy mode by using the command line interface

At the command prompt, type the following command to add a policy map and verify the configuration:

- add policy map <mapPolicyName> -sd <string> [-su <string>] [-td <string>] [-tu <string>]
- show policy map [<mapPolicyName>]

Example

The following command maps a domain in a client request to a target domain:

```
> add policy map myMappingPolicy -sd www.mycompany.com -td www.myrealcompany.com
 Done
> show policy map myMappingPolicy
1)      Name: myMappingPolicy
       Source Domain: www.mycompany.com       Source Url:
       Target Domain: www.myrealcompany.com    Target Url:
 Done
>
```

Following is an example of mapping a URL suffix to a different URL suffix:

```
> add policy map myOtherMappingPolicy -sd www.mycompany.com -td www.myrealcompany.com -su /news
 Done
> show policy map myOtherMappingPolicy
1)      Name: myOtherMappingPolicy
       Source Domain: www.mycompany.com       Source Url: /news.html
       Target Domain: www.myrealcompany.com    Target Url: /realnews.html
 Done
>
```

Parameters for creating a mapping policy

mapPolicyName

The name of the map policy you are creating.

sd

The publicly known source domain name. This is the domain name with which a client request arrives at a reverse proxy virtual server for cache redirection.

su

The source URL. Specify all or part of the source URL, in the following format: `/ [[prefix] [*]] [.suffix]`

td

The domain name sent to the server. The source domain name is replaced with this name.

tu

The target URL. Specify the target URL in the following format: `/ [[prefix] [*]] [.suffix]`

To configure a mapping policy for reverse proxy mode by using the configuration utility

1. In the navigation pane, expand Cache Redirection, and then click Map Policies.
2. In the details pane, click Add.
3. In the Create Map Policy dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for creating a mapping policy" as shown:
   - Name*- mapPolicyName
   - Source Domain*-sd
   - Target Domain*-td
   - Source URL-su
   - Target URL-tu

   * A required parameter
4. Click Create, and then click Close. The Map pane displays the new mapping policy.

To bind the mapping policy to the cache redirection virtual server by using the command line interface

At the command prompt, type the following commands to bind the mapping policy to the cache redirection virtual server and verify the configuration:

- bind cr vserver <name> -policyName <string> [<targetVserver>]
- show cr vserver <name>

Example

```
> bind cr vserver Vserver-CRD-3 -policyName myMappingPolicy Vserver-LB-CR
 Done
> show cr vserver Vserver-CRD-3
      Vserver-CRD-3 (10.102.29.50:88) - HTTP  Type: CONTENT
      State: UP
      Client Idle Timeout: 180 sec
      Down state flush: ENABLED
      Disable Primary Vserver On Down : DISABLED
      Default: Vserver-LB-CR  Content Precedence: RULE       Cache: REVERSE
      On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
      Redirect: POLICY       Reuse: ON       Via: ON ARP: OFF

1)     Policy:        Target: Vserver-LB-CR   Priority: 0     Hits: 0
1)     Map: myMappingPolicy Target: Vserver-LB-CR
 Done
```

>

To bind the mapping policy to the cache redirection virtual server by using the configuration utility

1. In the navigation pane, expand Cache Redirection, and then click Virtual Servers.
2. In the details pane, select the virtual server from which you want to bind the mapping policy, and then click Open.
3. In the Configure Virtual Server(Cache Redirection), on the Policies tab, select Map, and then click Insert Policy.
4. In the Policy Name column, select the policy from drop down list.
5. In the Target column, click the down arrow, and then select the vserver from drop down list.
6. Click OK.

Selective Cache Redirection

Selective cache redirection sends requests for particular types of content, for example, images, to one cache server or group of cache servers and sends other types of content to a different cache server or group of cache servers. You can configure advanced cache redirection in transparent, reverse proxy, or forward proxy modes.

In selective cache redirection, the NetScaler appliance intercepts a client request and forwards non-cacheable requests to the original destination in the client request. For cacheable requests, the appliance sends the requests to the destination cache server that can serve content of a specific content type.

Selective cache redirection involves configuring content switching policies in addition to cache redirection policies. The NetScaler first evaluates the cache redirection policies that are bound to the cache redirection virtual server. If a request matches a cache redirection policy, the cache redirection virtual server sends the request to the origin server or a load balancing virtual server for the origin. If no cache redirection policies match the request, the NetScaler evaluates the content switching policies bound to the cache redirection virtual server. If a content switching policy matches the request, the cache redirection virtual server redirects the request to a load balancing virtual server for the cache.

To configure selective cache redirection, first enable cache redirection, load balancing, and content switching on the NetScaler appliance. Then, configure a load balancing virtual server for the cache and an associated HTTP service. After this, configure a cache redirection virtual server and bind both the cache redirection and content switching policies to it. Once you have bound the policies, you can configure the virtual server to give precedence to either rule based or URL based content-switching policies.

When configured for transparent mode cache redirection in an edge deployment topology, the NetScaler sends all cacheable HTTP traffic to a transparent cache farm. Clients access the Internet through the NetScaler, which is configured as a Layer 4 switch that receives traffic on port 80.

The NetScaler can direct requests for images (for example, .gif and .jpg files) to one server in the transparent cache farm, and all other requests for static content to other servers in the farm. For this configuration, you configure content switching policies to send images to the image cache and send all other cacheable content to a default cache.

Note: The configuration described here is for transparent selective cache redirection. Therefore, it does not require a load balancing virtual server for the origin, as would a reverse proxy configuration.

To configure this type of selective cache redirection, first enable cache redirection, load balancing, and content switching. Then, configure a load balancing virtual server for the cache and configure an associated HTTP service. Then, configure a cache redirection virtual server and create and bind both cache redirection and content switching policies to this virtual server.

For details on how to enable cache redirection and load balancing on the NetScaler, see "Configuring Cache Redirection."

Enabling Content Switching

To configure selective cache redirection, after you enable both the load balancing and cache redirection features on the NetScaler, you must enable content switching.

To enable content switching by using the command line interface

At the command prompt, type:

- enable ns feature CS
- show ns feature

Example

```
> enable ns feature cs
 Done
> show ns feature

      Feature                Acronym          Status
      -------                -------          ------
 1)   Web Logging             WL               ON
 2)   Surge Protection        SP               ON
 3)   Load Balancing          LB               ON
 4)   Content Switching        CS               ON
 5)   Cache Redirection        CR               ON
       ...
       ...
       ...
23)   HTML Injection          HTMLInjection    ON
24)   NetScaler Push          push             OFF
Done
```

To enable cache redirection and load balancing by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features, click Configure basic features.
3. In Configure Basic Features dialog box, select the check box next to the Content Switching, and then click OK.
4. In Enable/Disable Feature(s)? dialog box, click Yes.

Configuring a Load Balancing Virtual Server for the Cache

Create a load balancing virtual server and an HTTP service for each type of cache server that will be used. For example, if you want to serve JPEG files from one cache server and GIF files from another cache server, and use a third cache server for the rest of the content, create an HTTP service and virtual server for each of the three types of cache servers. Then bind each service to its respective virtual server.

For details on how to create a load balancing virtual server, see "Creating a Virtual ServerCreating a Virtual Server."

For details on how to configure services that represent the cache server, see "Configuring an HTTP Service."

For details on how to bind the service to a virtual server, see "Binding/Unbinding a Service to/from a Load Balancing Virtual Server."

For details on how to create a transparent proxy cache redirection server, see "Configuring a Cache Redirection Virtual Server", and create a virtual server of type TRANSPARENT.

For details on binding built-in cache redirection policies to the cache redirection virtual server, see "Binding Policies to the Cache Redirection Virtual Server."

Configuring a Cache Redirection Policy for a Specific Type of Content

To identify requests that contain a .gif or .jpeg extension as cacheable, you configure a cache redirection policy and bind it to the cache redirection virtual server.

Note: If a request matches a policy, the NetScaler appliance forwards it to the origin server. As a result, in the following procedure, you configure policies to match requests that do *not* have ".gif" or ".jpeg" extensions.

To configure cache redirection for a specific type of content, configure a policy that uses a simple expression, as described in "Configuring a Cache Redirection Policy."

Configuring Policies for Content Switching

You must create a content switching policy to identify specific types of content to be cached in one cache server or farm and identify other types of content to serve from another cache server or farm. For example, you can configure a policy to determine the location for image files with .gif and .jpeg extensions.

After defining the content switching policy, you bind it to a cache redirection virtual server and specify a load balancing virtual server. Requests that match the policy are forwarded to the named load balancing virtual server. Requests that do not match the content switching policy are forwarded to the default load balancing virtual server for the cache.

For more details about the content switching feature and configuring content switching policies, see "Content Switching."

You must first create the content switching policy and then bind it to the cache redirection virtual server.

To create a content switching policy by using the command line interface

At the command line, type:

- add cs policy <policyName> [-url <string> | -rule <expression>]
- show cs policy [<policyName>]

Examples

```
> add cs policy Policy-CS-JPEG -rule "REQ.HTTP.URL == '/*.jpeg'"
 Done
> show cs policy Policy-CS-JPEG
        Rule: REQ.HTTP.URL == '/*.jpeg'         Policy: Policy-CS-JPEG
        Hits: 0
 Done
>

> add cs policy Policy-CS-GIF -rule "REQ.HTTP.URL == '/ *.gif'"
 Done
> show cs policy Policy-CS-GIF
        Rule: REQ.HTTP.URL == '/ *.gif'         Policy: Policy-CS-GIF
        Hits: 0
 Done
>

> add cs policy Policy-CS-JPEG-URL -url /*.jpg
 Done
```

```
> show cs policy Policy-CS-JPEG-URL
        URL: /*.jpg     Policy: Policy-CS-JPEG-URL
        Hits: 0
 Done
>

> add cs policy Policy-CS-GIF-URL -url /*.gif
 Done
> show cs policy Policy-CS-GIF-URL
        URL: /*.gif     Policy: Policy-CS-GIF-URL
        Hits: 0
 Done
>
```

Parameters for creating a content switching policy

policyName

Name of the content switching policy. This is a mandatory parameter, and the value cannot be changed after the policy is created.

url

The URL, with wildcards. Specify the string value in this format: // [[prefix] [*]] [.suffix]
Maximum value: 208

rule

An expression that the NetScaler evaluates to identify non-cacheable requests. Can consist of multiple expressions joined by `AND` and `OR` operators.

To create a URL-based content switching policy by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Policies.
2. In the details pane, click Add.
3. In the Create Content Switching Policy dialog box, in the Name text box, type a name for the policy.
4. Select the URL radio button.
5. In the Value text box, type the string value (for example, **/sports**).
6. Click Create and click Close. The policy you created appears in the Content Switching Policies page.

To create a rule-based content switching policy by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Policies.
2. In the details pane, click Add.
3. In the Create Content Switching Policy dialog box, in the Name text box, type a name for the policy.
4. Select the Expression radio button, and then click Configure.
5. In the Create Expression dialog box, choose the expression syntax that you want to use.
   - If you want to use default syntax, accept the default and proceed to the next step.
   - If you want to use classic syntax, click Switch to Classic Syntax.

   The Expression portion of the dialog box changes to match your choice. The default syntax Expression view has fewer elements than does the classic syntax Expression view. In the default syntax Expression view, instead of a preview window, a button provides access to an expression evaluator. The evaluator evaluates the expression you entered, to verify that it is valid, and displays an analysis of the expression's effect.
6. Enter your policy expressions.
   - If you are using classic syntax and need further instructions, see "Configuring Classic Policies and Expressions."
   - If you are using the default syntax and need further instructions, see "Configuring Default Syntax Expressions: Getting Started."
7. Click Create and click Close. The policy you created appears in the Content Switching Policies pane.

To bind the content switching policy to a cache redirection virtual server by using the command line interface

At the command prompt, type the following commands to bind the content switching policy to a cache redirection virtual server and verify the configuration:

- bind cs vserver <name> <targetVserver> [-policyName <string>]
- show cs vserver [<name>]

Example

```
> bind cs vserver Vserver-CR-1 lbcachejpeg -policyName Policy-CS-JPEG
 Done
> bind cs vserver Vserver-CR-1 lbcachegif -policyName Policy-CS-GIF
```

```
 Done
> show cs vserver Vserver-CR-1
        Vserver-CR-1 (10.102.29.60:80) - HTTP   Type: CONTENT
        State: UP
        Last state change was at Fri Jul  2 12:53:45 2010
        Time since last state change: 0 days, 00:00:58.920
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        State Update: DISABLED
        Default:        Content Precedence: RULE
        Cacheable: YES
        Vserver IP and Port insertion: OFF
        Case Sensitivity: ON
        Push: DISABLED  Push VServer:
        Push Label Rule: none

1)      Policy: Policy-CS-JPEG  Target: lbcachejpeg     Priority: 0     Hits: 0
2)      Policy: Policy-CS-GIF   Target: lbcachegif      Priority: 0     Hits: 0
 Done
>
```

Parameters for binding a content switching policy to a cache redirection virtual server

name

The name of the cache redirection virtual server to which you are binding the content switching policy.

targetVserver

The name of the load balancing virtual server to which cacheable requests that match the content switching policy are sent.

policyName

The name of the content switching policy that decides the cache server to which cacheable content of a specific type is sent.

Note: You are binding the content switching policy to a cache redirection virtual server and not to a content switching virtual server, even though you are using the ' bind cs vserver ' command.

To bind the content switching policy to a cache redirection virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to bind the policy (for example, **Vserver-CS-1**), and then click Open.
3. In the Configure Virtual Server (Content Switching) dialog box, on the Policies tab, click CSW, and then click Insert Policy.
4. In the Policy Name column, select the policy that you want to configure for the content switching virtual server.
5. In the Target column, click the green arrow, and select the target load balancing virtual server from the list.
6. Click OK.

Configuring Precedence for Policy Evaluation

You can configure a content switching policy based on either a rule, which is a generic configuration to accommodate various content types, or a URL, which is more specific and defines exactly the type of content that has to be sent to a particular cache server. Essentially, the same content can be defined by either a rule based policy or a URL based policy.

Once you bind content switching policies of either type to a cache redirection virtual server, you can configure the virtual server to give precedence to either rule based or URL based policies. This will, in turn, decide which servers the particular requests are directed to.

To configure precedence for policy evaluation, use the precedence parameter, which specifies the type of policy (URL or RULE) that takes precedence on the content redirection virtual server.

Possible values: RULE, URL

Default value: RULE

To configure precedence for policy evaluation by using the command line interface

At the command prompt, type the following commands to configure precedence for policy evaluation and verify the configuration:

- set cr vserver <name> [-precedence (RULE | URL)]
- show cr vserver <name>

Example

```
> set cr vserver Vserver-CRD-1 -precedence URL
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
```

```
1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
>
```

To configure precedence for policy evaluation by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure precedence, (for example, **Vserver-CS-1**), and then click Open.
3. In the Configure Virtual Server (Content Switching) dialog box, on the Advanced tab, next to Precedence, click Rule or URL, and then click OK.

Administering a Cache Redirection Virtual Server

To administer a cache redirection virtual server, you need to view cache redirection statistics. You might need to enable or disable cache redirection servers, or direct policy hits to the cache instead of the origin. Administrative tasks also include backing up a cache redirection virtual server and managing client connections.

Viewing Cache Redirection Virtual Server Statistics

You can view properties of a cache redirection virtual server and statistics on the traffic that has passed through a cache redirection virtual server. You can also view the cache redirection virtual servers and policies that you have bound to load balancing virtual servers.

To view statistics for a specific cache redirection virtual servers, use the name parameter to specify the name of the virtual server for which statistics will be displayed. Otherwise, statistics for all cache redirection virtual servers are displayed. Maximum Length: 127

To view statistics for a cache redirection virtual server by using the command line interface

At the command prompt, type:

stat cr vserver [<name>]

Example

```
> stat cr vserver Vserver-CRD-1

Vserver Summary
                    IP  port    Protocol       State
Vser...CRD-1        0.0.0.0   80        HTTP          UP

VServer Stats:
                              Rate (/s)             Total
Requests                              0                 0
Responses                             0                 0
Request bytes                         0                 0
Response bytes                        0                 0

 Done
>
```

To view statistics for a cache redirection virtual server by using the configuration utility

1. In the navigation pane, expand Cache Redirection, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to view statistics, (for example, **Vserver-CRD-1**), and then click Statistics.

Omit the server name to display basic statistics for all cache redirection virtual servers. Include the server name to display detailed statistics for that virtual server, including number and size of requests and responses that pass through the virtual server

To view the statistics of a cache redirection virtual server by using the monitoring and dashboard utilities

1. To view the statistics by using the monitoring utilities, click the Monitoring tab.
2. In the Select Group drop-down menu, choose CR Virtual Servers. A list of cache redirection virtual servers appears.
3. To view the statistics by using the dashboard utilities, click the Dashboard tab.
4. Click Applet Client or Web Start Client next to Statistical Utility.
5. In the Select Group drop-down menu, choose CR Virtual Servers. The dashboard displays summary statistics for the cache redirection virtual servers.
6. To see a chart of virtual server activity, click Chart. A graphical representation of the virtual server statistics appears.

Enabling or Disabling a Cache Redirection Virtual Server

When you create a cache redirection virtual server, it is enabled by default. If you disable a cache redirection virtual server, its state changes to OUT OF SERVICE and it stops redirecting cacheable client requests. However, the NetScaler appliance continues to respond to ARP and ping requests for the IP address of this virtual server.

To Enable or Disable a cache redirection virtual servers by using the command line interface

At the command line, type one of the following commands:

- enable cr vserver <name>
- show cr vserver <name>
- disable cr vserver <name>
- show cr vserver <name>

Examples

```
> enable cr vserver Vserver-CRD-1
 Done
> show cr vserver Vserver-CRD-1
       Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
       State: UP  ARP:DISABLED
       Client Idle Timeout: 180 sec
       Down state flush: ENABLED
       Disable Primary Vserver On Down : DISABLED
       Default:        Content Precedence: URL Cache: TRANSPARENT
       On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
       Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)     Cache bypass  Policy: bypass-cache-control
2)     Cache bypass  Policy: Policy-CRD
 Done
>

> disable cr vserver Vserver-CRD-1
 Done
> show cr vserver Vserver-CRD-1
       Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
       State: OUT OF SERVICE  ARP:DISABLED
```

```
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
>
```

To Enable or Disable a cache redirection virtual servers by using the configuration utility

1. Navigate to Traffic Management > Cache Redirection > Virtual Servers.
2. In the navigation pane, expand Cache Redirection, and then click Virtual Servers.
3. In the details pane, select the virtual server that you want to enable or disable, (for example, **Vserver-CRD-1**), and then click Statistics.
4. In the Proceed dialog box, click Yes.

Directing Policy Hits to the Cache Instead of the Origin

By default, when a request matches a policy, the NetScaler appliance forwards the request either to the origin server directly, or to a load balancing virtual server for the origin, depending on how you have configured cache redirection.

You can change the default behavior so that when a request matches a policy, the request is forwarded to a load balancing virtual server for the cache.

To change the destination for a policy hit to the origin or the cache, use the onPolicyMatch parameter, which specifies where to send requests that match the cache redirection policy.

The valid options are:

1. CACHE - Directs all matching requests to the cache.

2. ORIGIN - Directs all matching requests to the origin server.

Note: For this option to work, you must select the cacheredirection type as POLICY.

Possible values: CACHE, ORIGIN

Default value: ORIGIN

To change the destination for a policy hit to the origin or the cache by using the command line interface

At the command prompt, type the following commands to change the destination for a policy hit and verify the configuration:

- set cr vserver <name> [-onPolicyMatch (ORIGIN | CACHE)]

- show cr vserver <name>

Example

```
> set cr vserver Vserver-CRD-1 -onPolicyMatch CACHE
 Done
> show cr vserver Vserver-CRD-1
      Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
      State: UP  ARP:DISABLED
      Client Idle Timeout: 180 sec
      Down state flush: ENABLED
      Disable Primary Vserver On Down : DISABLED
```

```
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
```

To change the destination for a policy hit to the origin or the cache by using the configuration utility

1. In the navigation pane, expand Cache Redirection, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to change the destination for a policy hit, (for example, **Vserver-CRD-1**), and then click Open.
3. In Configure Virtual Server (Cache Redirection) dialog box, click Advanced tab.
4. Select CACHE or ORIGIN from the Redirect To drop-down list.
5. Click OK.

Backing Up a Cache Redirection Virtual Server

Cache redirection can fail if the primary virtual server fails, or if it is unable to handle excessive traffic. You can specify a backup virtual server to take over the processing of traffic when the primary virtual server fails.

To specify a backup cache redirection virtual server, use the backupVServer parameter, which specifies Backup Virtual Server. Maximum Length: 127

To specify a backup cache redirection virtual server by using the command line interface

At the command prompt, type the following commands to specify a backup cache redirection virtual server and verify the configuration:

- set cr vserver <name> [-backupVServer <string>]
- show cr vserver <name>

Example

```
> set cr vserver Vserver-CRD-1 -backupVServer Vserver-CRD-2
 Done
> show cr vserver Vserver-CRD-1
      Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
      State: UP  ARP:DISABLED
      Client Idle Timeout: 180 sec
      Down state flush: ENABLED
      Disable Primary Vserver On Down : DISABLED
      Default:       Content Precedence: URL Cache: TRANSPARENT
      On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
      Redirect: POLICY       Reuse: ON       Via: ON ARP: OFF
      Backup: Vserver-CRD-2

1)     Cache bypass  Policy: bypass-cache-control
2)     Cache bypass  Policy: Policy-CRD
 Done
```

To specify a backup cache redirection virtual server by using the configuration utility

1. In the navigation pane, expand Cache Redirection, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to change the destination for a policy hit, (for example, **Vserver-CRD-1**), and then click Open.
3. In Configure Virtual Server (Cache Redirection) dialog box, select the Advanced tab.
4. In the Backup Virtual Server drop-down list, select the virtual server.
5. Click OK.

Managing Client Connections for a Virtual Server

You can configure timeouts on a cache redirection virtual server so that client connections are not kept open indefinitely. You can also insert Via headers in requests. To possibly reduce network congestion, you can reuse open TCP connections. You can enable or disable delayed cleanup of cache redirection virtual server connections.

You can configure the NetScaler to send ICMP responses to PING requests according to your settings. On the IP address corresponding to the virtual server, set the ICMP RESPONSE to VSVR_CNTRLD, and on the virtual server, set the ICMP VSERVER RESPONSE.

The following settings can be made on a virtual server:

- When you set ICMP VSERVER RESPONSE to PASSIVE on all virtual servers, NetScaler always responds.
- When you set ICMP VSERVER RESPONSE to ACTIVE on all virtual servers, NetScaler responds even if one virtual server is UP.
- When you set ICMP VSERVER RESPONSE to ACTIVE on some and PASSIVE on others, NetScaler responds even if one virtual server set to ACTIVE is UP.

Configuring Client Timeout

You can specify expiration of client requests by setting a timeout value for the cache redirection virtual server. The timeout value is the number of seconds for which the cache redirection virtual server waits to receive a response for the client request.

To configure a time-out value, use the cltTimeout parameter, which specifies the time, in seconds, after which the NetScaler appliance closes any idle client connections. The default value is 180sec for HTTP/SSL-based services and 9000sec for TCP-based services.

To configure client timeout by using the command line interface

At the command prompt, type the following commands to configure client timeout and verify the configuration:

- set cr vserver <name> [-cltTimeout <secs>]
- show cr vserver <name>

Example

```
> set cr vserver Vserver-CRD-1 -cltTimeout 6000
 Done
> show cr vserver Vserver-CRD-1
      Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
      State: UP  ARP:DISABLED
      Client Idle Timeout: 6000 sec
      Down state flush: ENABLED
      Disable Primary Vserver On Down : DISABLED
      Default:       Content Precedence: URL Cache: TRANSPARENT
      On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
      Redirect: POLICY       Reuse: ON       Via: ON ARP: OFF
      Backup: Vserver-CRD-2

1)     Cache bypass  Policy: bypass-cache-control
2)     Cache bypass  Policy: Policy-CRD
 Done
```

To configure client timeout by using the configuration utility

1. In the navigation pane, expand Cache Redirection, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure client timeout, (for example, **Vserver-CRD-1**), and then click Open.
3. In Configure Virtual Server (Cache Redirection) dialog box, select the Advanced tab.
4. In the Client Time-out(secs) text box, enter the time-out value in seconds.
5. Click OK.

Inserting Via Headers in the Requests

A Via header lists the protocols and recipients between the start and end points for a request or a response and informs the server of proxies through which the request was sent. You can configure the cache redirection virtual server to insert a Via header in each HTTP request. The via parameter is enabled by default when you create a cache redirection virtual server.

To enable or disable Via-header insertion in client requests, use the via parameter, which specifies the state of the system in inserting a Via header in the HTTP requests.

Possible values: ON, OFF

Default value: ON

To enable or disable Via-header insertion in client requests by using the command line interface

At the command prompt, type:

- set cr vserver <name> [-via (ON|OFF)]
- show cr vserver <name>

Example

```
> set cr vserver Vserver-CRD-1 -via ON
 Done
> show cr vserver Vserver-CRD-1
       Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
       State: UP  ARP:DISABLED
       Client Idle Timeout: 6000 sec
       Down state flush: ENABLED
       Disable Primary Vserver On Down : DISABLED
       Default:        Content Precedence: URL Cache: TRANSPARENT
       On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
       Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
       Backup: Vserver-CRD-2

1)     Cache bypass  Policy: bypass-cache-control
2)     Cache bypass  Policy: Policy-CRD
 Done
>
```

To enable or disable Via-header insertion in client requests by using the configuration utility

1. In the navigation pane, expand Cache Redirection, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure client timeout, (for example, **Vserver-CRD-1**), and then click Open.
3. In Configure Virtual Server (Cache Redirection) dialog box, select the Advanced tab.
4. Select the Via check box.
5. Click OK.

Reusing TCP Connections

You can configure the NetScaler appliance to reuse TCP connections to the cache and origin servers across client connections. This can improve performance by saving the time required to establish a session between the server and the NetScaler. The reuse option is enabled by default when you create a cache redirection virtual server.

To enable or disable the reuse of TCP connections, use the reuse parameter, which specifies the state of reuse of TCP connections to the cache or origin servers across client connections.

Possible values: ON, OFF

Default value: ON

To enable or disable the reuse of TCP connections by using the command line interface

At the command prompt, type:

- set cr vserver <name> [-reuse (ON|OFF)]
- show cr vserver <name>

Example

```
> set cr vserver Vserver-CRD-1 -reuse ON
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
```

To enable or disable the reuse of TCP connections by using the configuration utility

1. In the navigation pane, expand Cache Redirection, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure client timeout, (for example, **Vserver-CRD-1**), and then click Open.
3. In Configure Virtual Server (Cache Redirection) dialog box, select the Advanced tab.
4. Select the Reuse check box.
5. Click OK.

Configuring Delayed Connection Cleanup

The down state flush option performs delayed cleanup of connections on a cache redirection virtual server. The down state flush option is enabled by default when you create a cache redirection virtual server.

To enable or disable the down state flush option, set the downStateFlush parameter.

Possible values: ENABLED, DISABLED

Default value: ENABLED

To enable of disable the down state flush option by using the command line interface

At the command prompt, type the following commands to configure delayed connection clean up and verify the configuration:

- set cr vserver <name> [-downStateFlush (ENABLED | DISABLED)]
- show cr vserver <name>

Example

```
> set cr vserver Vserver-CRD-1 -downStateFlush ENABLED
 Done
> show cr vserver Vserver-CRD-1
       Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
       State: UP  ARP:DISABLED
       Client Idle Timeout: 6000 sec
       Down state flush: ENABLED
       Disable Primary Vserver On Down : DISABLED
       Default:        Content Precedence: URL Cache: TRANSPARENT
       On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
       Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
       Backup: Vserver-CRD-2

1)     Cache bypass  Policy: bypass-cache-control
2)     Cache bypass  Policy: Policy-CRD
 Done
```

To enable or disable the reuse of TCP connections by using the configuration utility

1. In the navigation pane, expand Cache Redirection, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure client timeout, (for example, **Vserver-CRD-1**), and then click Open.
3. In Configure Virtual Server (Cache Redirection) dialog box, click Advanced tab.
4. Select the Down state flush check box.
5. Click OK.

N-Tier Cache Redirection

To efficiently handle large amounts of cached data, typically several gigabytes per second, an Internet Service Provider (ISP) deploys several dedicated cache servers. The cache redirection feature of the NetScaler appliance can help load balance the cache servers, but a single appliance or a couple of appliances might not efficiently handle the large volume of traffic.

You can solve the problem by deploying the NetScaler appliances in two tiers (layers), where the appliances in the upper tier load balance those in the lower tier and the appliances in the lower tier load balance the cache servers. This arrangement is called *n-tier cache redirection*.

For purposes such as auditing and security, an ISP has to track client details such as the IP address, information provided, and the time of the interaction. Therefore, client connections through a NetScaler appliance have to be fully transparent. However, if you configure transparent cache redirection, with the NetScaler appliances deployed in parallel, the IP address of the client has to be shared among all the appliances. Sharing of the client IP address creates a conflict that makes network devices, such as routers, cache servers, origin servers, and other NetScaler appliances, unable to determine the appliance, and therefore the client, to which the response should be sent.

How N-tier Cache Redirection Is Implemented

To solve the problem, NetScaler n-tier cache redirection splits the source port range among the appliances in the lower tier and includes the client IP address in the request sent to the cache servers. The upper-tier NetScaler appliances are configured to do sessionless load balancing in order to avoid unnecessary load on the appliances.

When the lower-tier NetScaler appliance communicates with a cache server, it uses a mapped IP address (MIP) to represent the source IP address. Therefore, the cache server can identify the NetScaler from which it received the request and send the response to the same NetScaler.

The lower-tier NetScaler appliance inserts the client IP address into the header of the request sent to the cache server. The client IP in the header helps the NetScaler to determine the client to which the packet should be forwarded when it receives the response from a cache server, or the origin server in case of a cache miss. The origin server determines the response to be sent according to the client IP inserted in the request header.

The origin server sends the response to an upper-tier NetScaler, including the source port number from which the origin server received the request. The entire source port range, 1024 to 65535, is distributed among the lower-tier NetScaler appliances. Each lower-tier appliance is exclusively assigned a group of addresses within the range. This allotment enables the upper-tier appliance to unambiguously identify the lower-tier NetScaler appliance that sent the request to the origin server. The upper-tier appliance can therefore forward the response to the correct lower-tier appliance.

The upper-tier NetScaler appliances are configured to do policy-based routing, and the routing policies are defined to determine the IP address of the destination NetScaler from the source port range.

Setup Necessary for Configuring N-Tier CRD

The following setup is necessary for the functioning of n-tier cache redirection:

For each upper-tier NetScaler appliance:

- Enable Layer 3 mode.
- Define policies for policy-based routes (PBRs) so that traffic is forwarded according to the range of the destination port.
- Configure a load balancing virtual server.
- Configure the virtual server to listen to all the traffic coming from the client. Set the Service Type/Protocol to be ANY and IP Address as asterisk (*).
- Enable sessionless load balancing with MAC-based redirection mode to avoid unnecessary load on the upper-tier NetScaler appliances.
- Make sure that the Use Proxy Port option is enabled.
- Create a service for each lower-tier NetScaler and bind all the services to the virtual server.

For each lower-tier NetScaler appliance,

- Configure the cache redirection port range on the NetScaler. Assign an exclusive range to each lower-tier NetScaler.
- Configure a load balancing virtual server and enable MAC-based redirection.
- Create a service for each cache server that is to be load balanced by this NetScaler. When creating the service, enable insertion of client IP in the header. Then, bind all the services to the load balancing virtual server.
- Configure a transparent mode cache redirection virtual server with the following settings:
  - Enable the Origin USIP option.
  - Add a source IP expression to include the client IP in the header.
  - Enable the Use Port Range option.

How N-Tier Cache Redirection Works During a Cache Hit

The following figure shows how cache redirection works when a client request is cacheable and the response is sent from a cache server.

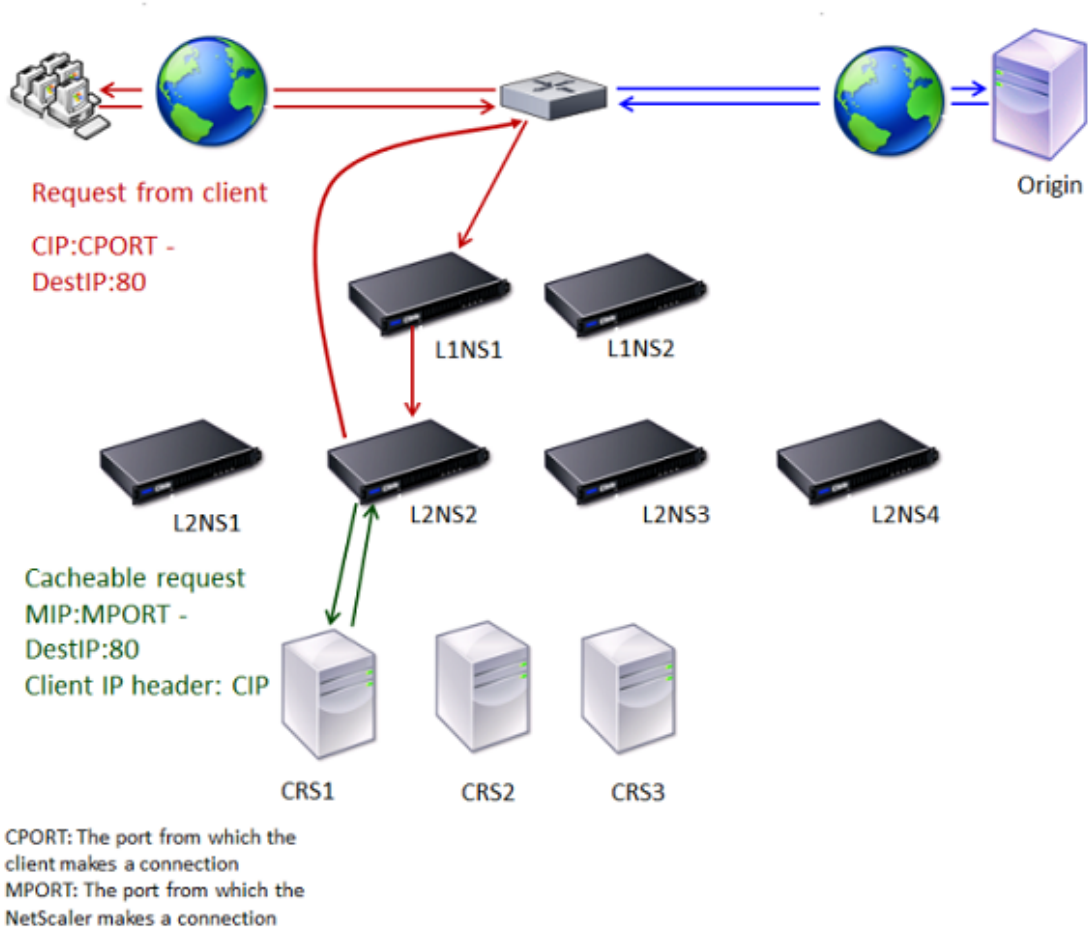


Figure 1. Cache Redirection in Case of a Cache Hit

Two NetScaler appliances, L1NS1 and L1NS2, are deployed in the upper tier, and four NetScaler appliances, L2NS1, L2NS2, L2NS3, and L2NS4, are deployed in the lower tier. Client A sends a request, which is forwarded by the router. Cache servers CRS1, CRS2, and CRS3 service the cache requests. Origin Server O services the uncached requests.

Traffic Flow

1. Client sends a request, and the router forwards it to L1NS1.
2. L1NS1 load balances the request to L2NS2.
3. L2NS2 load balances the request to the cache server CRS1, and the request is cacheable. L2NS2 includes the client IP in the request header.
4. CRS1 sends the response to L2NS2 because L2NS2 used its MIP as the source IP address when connecting to CRS1.
5. With the help of the client IP address in the request header, L2NS2 identifies the client from which the request came. L2NS2 directly sends the response to the router, avoiding unnecessary load on the NetScaler in the upper tier.
6. The router forwards the response to Client A.

How N-Tier Cache Redirection Works During a Cache Bypass

The following figure shows how cache redirection works when a client request is sent to an origin server for a response.

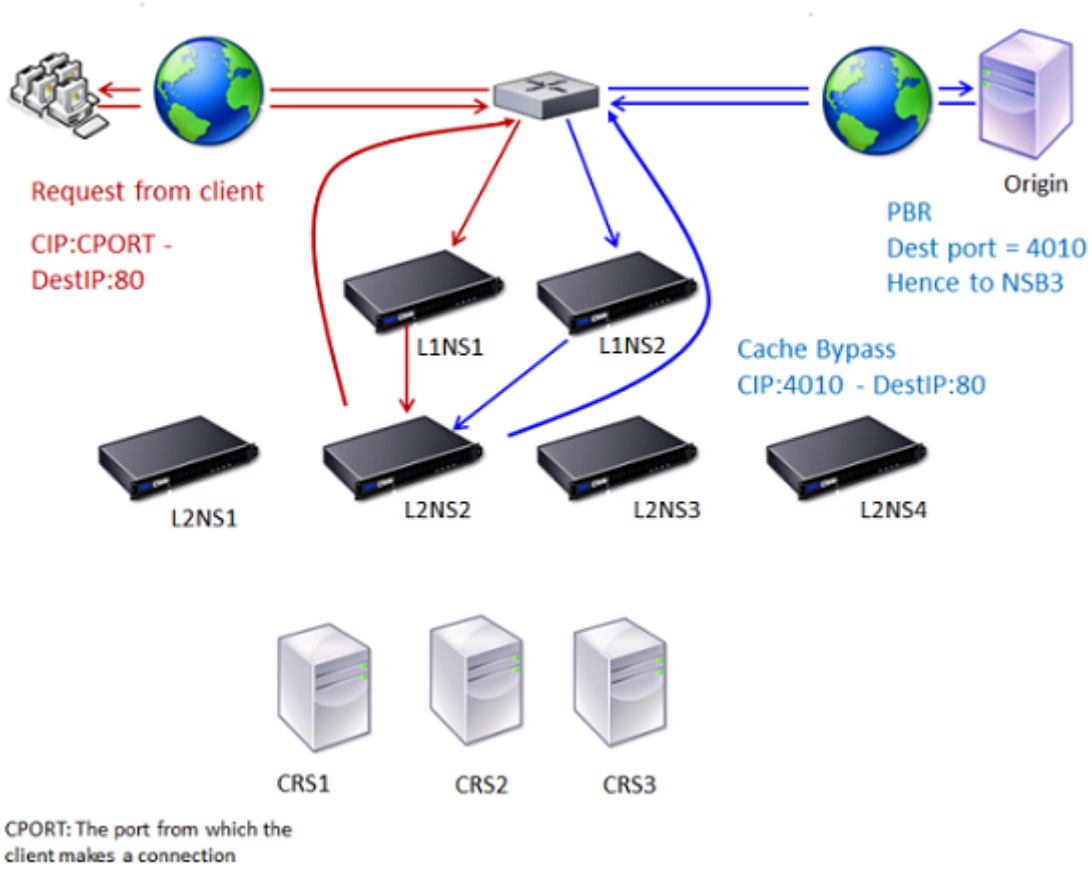


Figure 2. Cache Redirection in Case of a Cache Bypass

Two NetScaler appliances, L1NS1 and L1NS2, are deployed in the upper tier, and four NetScaler appliances, L2NS1, L2NS2, L2NS3, and L2NS4, are deployed in the lower tier. Client A sends a request, which is forwarded by the router. Cache servers CRS1, CRS2, and CRS3 service the cache requests. Origin Server O services the uncached requests.

Traffic Flow

1. Client sends a request, and the router forwards it to L1NS1.
2. L1NS1 load balances the request to L2NS2.
3. The request is uncacheable (cache bypass). Therefore, L2NS2 sends the request to the origin server through the router.
4. The origin server sends the response to an upper-tier NetScaler, L1NS2.
5. According to the PBR policies, L1NS2 forwards the traffic to the appropriate NetScaler in the lower tier, L2NS2.
6. L2NS2 uses the client IP address in the request header to identify the client from which the request came and sends the response directly to the router, avoiding unnecessary load on the NetScaler in the upper tier.
7. The router forwards the response to Client A.

How N-Tier Cache Redirection Works During a Cache Miss

The following figure shows how cache redirection works when a client request is not cached.

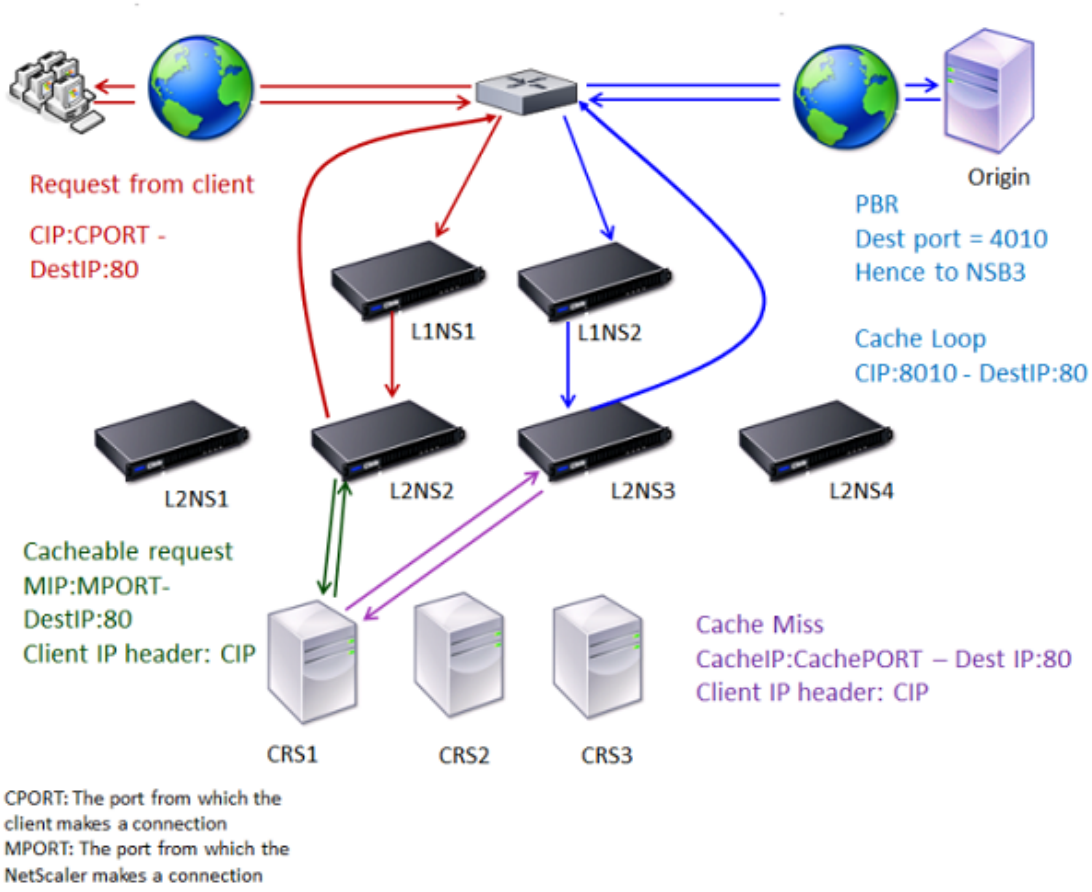


Figure 3. Cache Redirection in Case of a Cache Miss

Two NetScaler appliances, L1NS1 and L1NS2, are deployed in the upper tier, and four NetScaler appliances, L2NS1, L2NS2, L2NS3, and L2NS4, are deployed in the lower tier. Client A sends a request, which is forwarded by the router. Cache servers CRS1, CRS2, and CRS3 service the cache requests. Origin Server O services the uncached requests.

Traffic Flow

1. Client sends a request, and the router forwards it to L1NS1.
2. L1NS1 load balances the request to L2NS2.
3. L2NS2 load balances the request to the cache server CRS1 because the request is cacheable.
4. CRS1 does not have the response (cache miss). CRS1 forwards the request to the origin server through the NetScaler in the lower tier. L2NS3 intercepts the traffic.
5. L2NS3 takes the client IP from the header and forwards the request to the origin server. The source port included in the packet is the L2NS3 port from which the request is sent to the origin server.
6. The origin server sends the response to an upper-tier NetScaler, L1NS2.
7. According to the PBR policies, L1NS2 forwards the traffic to the appropriate NetScaler in the lower tier, L2NS3.
8. L2NS3 forwards the response to the router.
9. The router forwards the response to Client A.

Configuring the Upper-Tier NetScaler Appliances

Configure each of the upper-tier NetScaler appliances as follows.

To configure an upper-tier appliance for n-tier cache redirection by using the command line interface

At the command prompt, type the following commands:

- add service <name>@ <serviceIP> <serviceType> <port>

  Run this command for each service to be added.

- add lb vserver <name>@ ANY * <port> -persistenceType <persistenceMethod> -lbMethod <lbMethod> -m MAC -sessionless ENABLED -cltTimeout <client_Timeout_Value>

- bind lb vserver <name>@ <serviceName>

  Run this command for each service to be bound.

- enable ns mode l3

- add ns pbr <name> <action> -srcPort <sourcePortNumber> -destPort <startPortNumber-endPortNumber> -nexthop <serviceIpAddress> -protocol TCP

- apply ns pbrs

  Run this command after adding all the necessary PBRs.

Parameters for configuring a service

name

Name of the service. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serverName

Either the name of a previously created server object, or the IP address of the load-balanced server that hosts this service, in either IPv4 or IPv6 format. When you provide the IP address of the service, a server object is created with this IP address as its name. You can also create a server object manually, and then select the server name instead of an IP address from the drop-down menu that is associated with this field.

If the server is not reachable from the NetScaler or is not active, the service is designated as DOWN.

serviceType

The type of connections that the service will handle. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, DNS_TCP, ADNS_TCP, RADIUS, MYSQL, MSSQL, and RDPHTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, and SSL_DIAMETER. Default: HTTP.

port

Port on which the service listens. The port number must be a positive number not greater than 65534.

Parameters for creating a virtual server

name

Name of the virtual server. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( )

IPAddress

IP address of the virtual server. This IP address can be an IPv4 or IPv6 address, and is usually a public IP address. Clients send connection requests to this IP address.

serviceType

The type of services to which the virtual server distributes requests. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, and MSSQLHTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, and SSL_DIAMETER. Default: HTTP

port

Port on which the virtual server listens for client connections. The port number must be between 0-65535.

To configure an upper-tier appliance for n-tier cache redirection by using the configuration utility

1. Enable L3 mode:
    a. In the navigation pane, click System, and then click Settings.
    b. In the Settings group, click the Configure modes link.
    c. Select the Layer 3 Mode (IP Forwarding) check box.
    d. Click OK.
2. Configure policy-based routing (PBR):
    a. In the navigation pane, click Network, and then click PBRs.
    b. In the Policy-Based Routing (PBRs) pane, click Add.
    c. Type a name for the PBR.
    d. Select the action as Allow.
    e. In the Next Hop box, type the IP address of the service, which represents a lower-tier NetScaler.
    f. Select TCP from the Protocol drop-down list.
    g. Type the source port and the range of the destination port corresponding to the lower-tier NetScaler being added.
    h. Click Create.
    i. In the details pane, select the PBR and click Apply.
    j. Repeat Step (i) to Step (vii) for each lower-tier NetScaler.
3. Create a service for each lower-tier NetScaler:
    a. In the navigation pane, expand Load Balancing, and then click Services.
    b. In the details pane, click Add.
    c. Specify the name, protocol, IP address, and port. The protocol should be ANY.
    d. Click Create.
4. Configure a load balancing virtual server:
    a. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
    b. In the details pane, click Add.
    c. Specify the name, protocol, IP address, and port. The protocol should be ANY and the IP address should be *.

d. In the Services tab, select the services that represent the lower-tier NetScaler appliances.

e. In the Advanced tab, select the Redirection Mode as MAC Based and select the Sessionless check box.

f. Click Create.

Configuring the Lower-Tier NetScaler Appliances

Configure each of the lower-tier NetScaler appliances as follows.

To configure a lower-tier appliance for n-tier cache redirection by using the command line interface

At the command prompt, type the following commands:

- add service <name>@ <cacheServiceIP> <serviceType> <port> -cip ENABLED "ClientIP" –cachetype transparent

  Repeat for each cache server.

- add lb vserver <name>@ <serviceType> -m MAC

- bind lb vserver <name>@ <cacheServiceName>

  Repeat for each cache server.

- add cr vserver <name> <serviceType> * <port> -srcIPExpr "HTTP.REQ.HEADER(\"ClientIP\")" -originusip ON -cacheVserver <cachevServerName> –usePortRange ON

- set ns param-crPortRange <startPortNumber-endPortNumber>

Parameters for configuring a service

name

Name of the service. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serverName

Either the name of a previously created server object, or the IP address of the load-balanced server that hosts this service, in either IPv4 or IPv6 format. When you provide the IP address of the service, a server object is created with this IP address as its name. You can also create a server object manually, and then select the server name instead of an IP address from the drop-down menu that is associated with this field.

If the server is not reachable from the NetScaler or is not active, the service is designated as DOWN.

serviceType

The type of connections that the service will handle. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, DNS_TCP, ADNS_TCP, RADIUS, MYSQL, MSSQL, and RDPHTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, and SSL_DIAMETER. Default: HTTP.

port

Port on which the service listens. The port number must be a positive number not greater than 65534.

Parameters for creating a virtual server

name

Name of the virtual server. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( )

IPAddress

IP address of the virtual server. This IP address can be an IPv4 or IPv6 address, and is usually a public IP address. Clients send connection requests to this IP address.

serviceType

The type of services to which the virtual server distributes requests. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, and MSSQLHTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, and SSL_DIAMETER. Default: HTTP

port

Port on which the virtual server listens for client connections. The port number must be between 0-65535.

To configure a lower-tier appliance for n-tier cache redirection by using the configuration utility

1. Create a service for each cache server. To create a service:
    a. In the navigation pane, expand Load Balancing, and then click Services.
    b. In the details pane, click Add, and specify the name and protocol. Clear the Directly Addressable check box.
    c. In the Advanced tab, select the Override Global check box and the Client IP check box, and then in the Header box, type ClientIP.
    d. In the Cache Type box, select Transparent Cache.
    e. Click Create.
2. Configure a load balancing virtual server:
    a. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
    b. In the details pane, click Add and specify the name, protocol, IP address, and port. The IP address should be an asterisk (*).
    c. In the Services tab, select the services that represent the cache servers.
    d. In the Advanced tab, for Redirection Mode, select MAC Based.
    e. Click Create.
3. Configure a cache redirection virtual server:
    a. In the navigation pane, expand Cache Redirection, and then click Virtual Servers.
    b. In the details pane, click Add and specify the name, protocol, IP address, and port. The IP address should be *.
    c. For Cache Type, select Transparent.
    d. On the Advanced tab, in the Cache Server box, select the new load balancing virtual server and check the Origin USIP and Use Port Range check boxes. In the Source IP Expression box, type `HTTP.REQ.HEADER("ClientIP")`.
    e. Click Create.
4. Assign a source port range for the NetScaler:
    a. In the navigation pane, click System, and then click Settings.
    b. In the Settings group, click the Change global system settings link.
    c. In the Cache Redirection Port Range group, specify the port range for the NetScaler by typing a port number for Start Port and a port number for End Port.
    d. Click OK.

Content Switching

In today's complex Web sites, you may want to present different content to different users. For example, you may want to allow users from the IP range of a customer or partner to have access to a special Web portal. You may want to present content relevant to a specific geographical area to users from that area. You may want to present content in different languages to the speakers of those languages. You may want to present content tailored to specific devices, such as smartphones, to those who use the devices. The Citrix NetScaler content switching feature enables the NetScaler appliance to distribute client requests across multiple servers on the basis of specific content that you wish to present to those users.

To configure content switching, first create a basic content switching setup, and then customize it to meet your needs. This entails enabling the content switching feature, setting up load balancing for the server or servers that host each version of the content that is being switched, creating a content switching virtual server, creating policies to choose which requests are directed to which load balancing virtual server, and binding the policies to the content switching virtual server. You can then customize the setup to meet your needs by setting precedence for your policies, protecting your setup by configuring a backup virtual server, and improving the performance of your setup by redirecting requests to a cache.

How Content Switching Works

Content Switching enables the NetScaler appliance to direct requests sent to the same Web host to different servers with different content. For example, you can configure the appliance to direct requests for dynamic content (such as URLs with a suffix of .asp, .dll, or .exe) to one server and requests for static content to another server. You can configure the appliance to perform content switching based on TCP/IP headers and payload.

You can also use content switching to configure the appliance to redirect requests to different servers with different content on the basis of various client attributes. Some of those client attributes are:

- **Device Type.** The appliance examines the user agent or custom HTTP header in the client request for the type of device from which the request originated. Based on the device type, it directs the request to a specific Web server. For example, if the request came from a cell phone, the request is directed to a server that is capable of serving content that the user can view on his or her cell phone. A request from a computer is directed to a different server that is capable of serving content designed for a computer screen.

- **Language.** The appliance examines the Accept-Language HTTP header in the client request and determines the language used by the client's browser. The appliance then sends the request to a server that serves content in that language. For example, using content switching based on language, the appliance can send someone whose browser is configured to request content in French to a server with the French version of a newspaper. It can send someone else whose browser is configured to request content in English to a server with the English version.

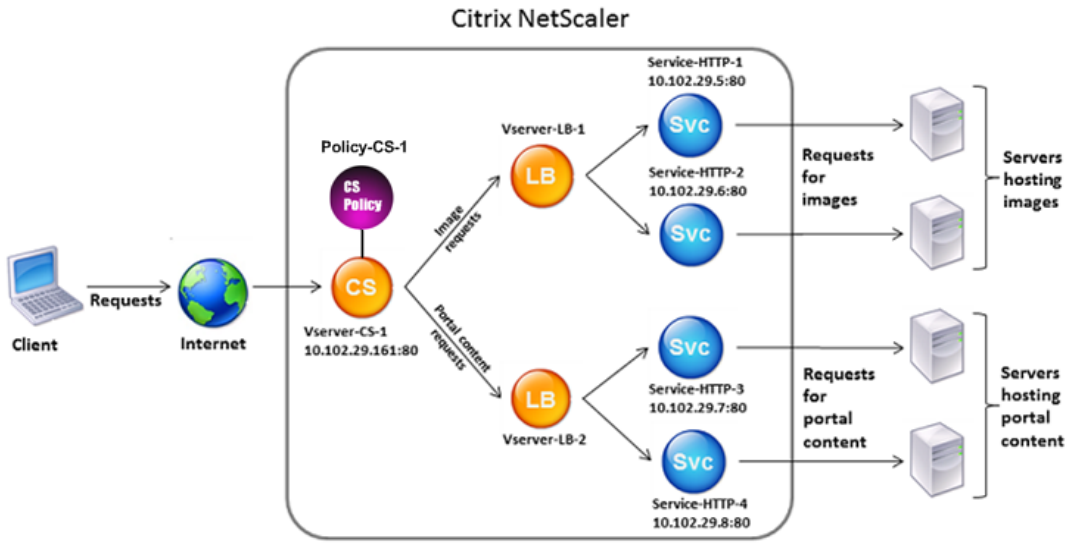
- **Cookie.** The appliance examines the HTTP request headers for a cookie that the server set previously. If it finds the cookie, it directs requests to the appropriate server, which hosts custom content. For example, if a cookie is found that indicates that the client is a member of a customer loyalty program, the request is directed to a faster server or one with special content. If it does not find a cookie, or if the cookie indicates that the user is not a member, the request is directed to a server for the general public.

- **HTTP Method.** The appliance examines the HTTP header for the method used, and sends the client request to the right server. For example, GET requests for images can be directed to an image server, while POST requests can be directed to a faster server that handles dynamic content.

- **Layer 3/4 Data.** The appliance examines requests for the source or destination IP, source or destination port, or any other information present in the TCP or UDP headers, and directs the client request to the right server. For example, requests from source IPs that belong to customers can be directed to a custom web portal on a faster server, or one with special content.

A typical content switching deployment consists of the entities described in the following diagram.

Figure 1. Content Switching Architecture



A content switching configuration consists of a content switching virtual server, a load balancing setup consisting of load balancing virtual servers and services, and content switching policies. To configure content switching, you must configure a content switching virtual server and associate it with policies and load balancing virtual servers. This process creates a *content group*—a group of all virtual servers and policies involved in a particular content switching configuration.

Content switching can be used with HTTP, HTTPS, TCP, and UDP connections. For HTTPS, you must enable SSL Offload.

When a request reaches the content switching virtual server, the virtual server applies the associated content switching policies to that request. The priority of the policy defines the order in which the policies bound to the content switching virtual server are evaluated. If you are using default syntax policies, when you bind a policy to the content switching virtual server, you must assign a priority to that policy. If you are using NetScaler classic policies, you can assign a priority to your policies, but are not required to do so. If you assign priorities, the policies are evaluated in the order that you set. If you do not, the NetScaler appliance evaluates your policies in the order in which they were created.

In addition to configuring policy priorities, you can manipulate the order of policy evaluation by using Goto expressions and policy bank invocations. For more details about default syntax policy configuration, see "Configuring Default Syntax Policies."

After it evaluates the policies, the content switching virtual server routes the request to the appropriate load balancing virtual server, which sends it to the appropriate service.

Content switching virtual servers can only send requests to other virtual servers. If you are using an external load balancer, you must create a load balancing virtual server for it and bind its virtual server as a service to the content switching virtual server.

Configuring Basic Content Switching

Before you configure content switching, you must understand how content switching is set up and how the services and virtual servers are connected.

To configure a basic, functional content switching setup, first enable the content switching feature. Then, create at least one content group. For each content group, create a content switching virtual server to accept requests to a group of web sites that use content switching. Also create a load balancing setup, which includes a group of load balancing virtual servers to which the content switching virtual server directs requests. To specify which requests to direct to which load balancing virtual server, create at least two content switching policies, one for each type of request that is to be redirected. When you have created the virtual servers and policies, bind the policies to the content switching virtual server. You can also bind a policy to multiple content switching virtual servers. When you bind a policy, you specify the load balancing virtual server to which requests that match the policy are to be directed.

In addition to binding individual policies to a content switching virtual server, you can bind policy labels. If you create additional content groups, you can bind a policy or policy label to more than one of the content switching virtual servers.

Note: After creating a content group, you can modify its content switching virtual serve to customize the configuration. For information on modifying the configuration of an existing content switching virtual server, see "Customizing the Basic Content Switching Configuration." For information on disabling and re-enabling entities, unbinding policies, and removing entities, see "Managing a Content Switching Setup."

Enabling Content Switching

To use the content switching feature, you must enable content switching. You can configure content switching entities even though the content switching feature is disabled. However, the entities will not work.

To enable content switching by using the command line interface

At the command prompt, type the following commands to enable content switching and verify the configuration:

- enable ns feature CS
- show ns feature

Example

```
> enable  feature ContentSwitch
 Done
> show feature

      Feature                 Acronym           Status
      -------                 -------           ------
 1)   Web Logging               WL                OFF
 2)   Surge Protection          SP                ON
 3)   Load Balancing            LB                ON
 4)   Content Switching          CS                ON
 .
 .
 .
 22)  Responder                 RESPONDER         ON
 23)  HTML Injection            HTMLInjection     ON
 24)  NetScaler Push            push              OFF
 Done
```

To enable content switching by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features, click Change basic features.
3. In the Configure Basic Features dialog box, select the Content Switching check box, and then click OK.
4. In the Enable/Disable Features(?) dialog box, click Yes.

Creating Content Switching Virtual Servers

You can add, modify, and remove content switching virtual servers. The state of a virtual server is DOWN when you create it, because the load balancing virtual server is not yet bound to it.

To create a virtual server by using the command line interface

At the command prompt, type:

add cs vserver <name> <protocol> <IPAddress> <port>

Example

add cs vserver Vserver-CS-1 HTTP 10.102.29.161 80

Parameters for configuring content switching

vServerName

Name of the content switching virtual server. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and blank space.

IPAddress

IP address of the virtual server. This IP address (VIP) is usually a public IP address to which the clients send connection requests.

port

Port on which the virtual server listens for client connections. The port number must be between 0-65535.

protocol

Protocol of the requests processed by the content switching virtual server. Choose one of the following service types:

- **HTTP.** For HTTP services.
- **TCP.** For non-RFC implementation of HTTP services.

- **UDP.** For DNS, ICMP, and other UDP-based services.
- **FTP.** For FTP services. This setting ensures that the NetScaler appliance takes care of the specifics of the FTP protocol.
- **SSL.** For HTTPS services. Select this type to encrypt HTTP traffic between the NetScaler appliance and the server.
- **SSL_TCP.** For secure TCP services.
- **RTSP.** For Real-Time Streaming Protocol services.
- **DNS.** For domain name servers.
- **SIP-UDP.** For SIP servers.
- **ANY.** For services that accept all traffic of any protocol type.
- **RADIUS.** For RADIUS authentication services.
- **RDP.** For remote desktop services.
- **MYSQL.** For MySQL database servers.
- **MSSQL.** For Microsoft SQL Servers.

To add a content switching virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Content Switching) dialog box, in the Name, IP Address, and Port text boxes, type the name, IP address, and port of the virtual server, (for example, Vserver-CS-1, 10.102.29.161, and 80).

   Note: If you need to enter an IPv6 address, select the IPv6 check box before you enter the address.
4. In the Protocol list, select the type of the virtual server (for example, HTTP).
5. Click Create, and then click Close.

Configuring a Load Balancing Setup for Content Switching

The content switching virtual server redirects all requests to a load balancing virtual server. You must create one load balancing virtual server for each version of the content that is being switched. This is true even when your setup has only one server for each version of the content, and you are therefore not doing any load balancing with those servers. You can also configure actual load balancing with multiple load-balanced servers that mirror each version of the content. In either scenario, the content switching virtual server needs to have a specific load balancing virtual server assigned to each version of the content that is being switched.

The load balancing virtual server then forwards the request to a service. If it has only one service bound to it, it selects that service. If it has multiple services bound to it, it uses its configured load balancing method to select a service for the request, and forwards that request to the service that it selected.

To configure a basic load balancing setup, you need to perform the following tasks:

- Create load balancing virtual servers
- Create services
- Bind services to the load balancing virtual server

For more information on load balancing, see "Load Balancing." For detailed instructions on setting up a basic load balancing configuration, see "Setting Up Basic Load Balancing."

Configuring a Content Switching Action

You specify the target load balancing virtual server for a content switching policy when binding the policy to the content switching virtual server. Consequently, you have to configure one policy for each load balancing virtual server to which to direct traffic.

However, if your content switching policy uses a default syntax rule, you can configure an action for the policy. In the action, you can specify the name of the target load balancing virtual server, or you can configure a request-based expression that, at run time, computes the name of the load balancing virtual server to which to send the request. The action expression must be specified in the default syntax.

The expression option can drastically reduce the size of your content switching configuration, because you need only one policy per content switching virtual server. Content switching policies that use an action can also be bound to multiple content switching virtual servers, because the target load balancing virtual server is no longer specified in the content switching policy. The ability to bind a single policy to multiple content switching virtual servers helps to further reduce the size of your content switching configuration.

After you create an action, you create a content switching policy and specify the action in the policy, so that the action is performed when that policy matches a request.

Note: You can also, for a content switching policy that uses a default syntax rule, specify the target load balancing virtual server when binding the policy to a content switching virtual server, instead of using a separate action. For domain-based policies, URL-based policies, and rule based policies that use classic expressions, an action is not available. So, for these types of policies, you specify the name of the target load balancing virtual server when binding the policy to a content switching virtual server. For more information, see "Binding Policies to a Content Switching Virtual Server."

Configuring an Action that Specifies the Name of the Target Load Balancing Virtual Server

If you choose to specify the name of the target load balancing virtual server in a content switching action, you need as many content switching policies as you have target load balancing virtual servers. Content switching decisions, in this case, are based on the rule in the content switching policy, and the action merely specifies the target load balancing virtual server. When a request matches the policy, the request is forwarded to the specified load balancing virtual server.

To create and verify a content switching action that specifies the name of the target load balancing virtual server, by using the command line interface

At the command prompt, type:

- add cs action <name> -targetLBVserver <string> [-comment <string>]
- show cs action <name>

Example

```
> add cs action mycsaction -targetLBVserver mylbvserver -comment "Forwards requests to mylbvserver."
 Done
> show cs action mycsaction
   Name: mycsaction
   Target LB Vserver: mylbvserver
   Hits: 0
   Undef Hits: 0
   Action Reference Count: 0
   Comment: "Forwards requests to mylbvserver."

 Done
>
```

Parameters for creating a content switching action that specifies the name of the target load balancing virtual server

name (Name)

Name for the content switching action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the content switching action is created.

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

targetLBVserver (Target LB Virtual Server)

Name of the load balancing virtual server to which to forward requests matching the rule in the content switching policy.

comment (Comment)

Any comments that you might want to associate with the content switching action.

To configure a content switching action that specifies the name of the target load balancing virtual server, by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Actions.
2. In the details pane, do one of the following:
   - To create a content switching action, click Add.
   - To modify a content switching action, select the content switching action, and then click Open.
3. In the Create Content Switching Action or Configure Content Switching Action dialog box, set the following parameters:
   - Name*
   - Target LB Virtual Server* (Under Target LB Virtual Server, click Name.)
   - Comment

   * A required parameter
4. Click Create.

Configuring an Action that Specifies an Expression for Selecting the Target at Run Time

If you choose to configure a request-based expression that can dynamically compute the name of the target load balancing virtual server, you need to configure only one content switching policy to select the appropriate virtual server. The rule for the policy can be a simple `TRUE` (the policy matches all requests) because, in this case, content switching decisions are based on the expression in the action. By configuring an expression in an action, you can drastically reduce the size of your content switching configuration.

If you choose to configure a request-based expression for computing the name of the target load balancing virtual server at run time, you must carefully consider how to name the load balancing virtual servers in the configuration. You must be able to derive their names by using the request-based policy expression in the action.

For example, if you are switching requests on the basis of the URL suffix (file extension of the requested resource), when naming the load balancing virtual servers, you can follow the convention of appending the URL suffix to a predetermined string, such as `mylb_`. For example, load balancing virtual servers for HTML pages and PDF files could be named `mylb_html` and `mylb_pdf`, respectively. In that case, the rule that you can use in the content switching action, to select the appropriate load balancing virtual server, is `"mylb_"+HTTP.REQ.URL.SUFFIX`. If the content switching virtual server receives a request for an HTML page, the expression returns `mylb_html`, and the request is switched to virtual server `mylb_html`.

To create a content switching action that specifies an expression, by using the command line interface

At the command line, type the following commands to create a content switching action that specifies an expression and verify the configuration:

- add cs action <name> -targetVserverExpr <expression>) [-comment <string>]
- show cs action <name>

Example

```
> add cs action mycsaction1 -targetvserverExpr '"mylb_" + HTTP.REQ.URL.SUFFIX'
 Done
> show cs action mycsaction1
    Name: mycsaction1
    Target Vserver Expression: "mylb_" + HTTP.REQ.URL.SUFFIX
    Target LB Vserver: No_Target
```

```
                ...
 Done
>
```

Parameters for creating a content switching action that specifies an expression

name (Name)

Name for the content switching action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the content switching action is created.

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

targetVserverExpr (Target LB Expression)

Expression in the default syntax, for computing the name of the load balancing virtual server at run time.

Comment (Comment)

Any comments that you might want to associate with the content switching action.

To configure a content switching action that specifies an expression by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Actions.
2. In the details pane, do one of the following:
   - To create a content switching action, click Add.
   - To modify a content switching action, select the content switching action, and then click Open.
3. In the Create Content Switching Action or Configure Content Switching Action dialog box, set the following parameters:
   - Name*
   - Target LB Expression* (Under Target LB Virtual Server, click Expression.)
   - Comment

   * A required parameter
4. Click Create.

Configuring Content Switching Policies

A content switching policy defines a type of request that is to be directed to a load balancing virtual server. These policies are applied in the order of the priorities assigned to them or (if you are using NetScaler classic policies and do not assign priorities when binding them) in the order in which the policies were created.

The policies can be:

- **Domain-based policies.** The NetScaler appliance compares the domain of an incoming URL with the domains specified in the policies. The appliance then returns the most appropriate content. Domain-based policies must be classic policies; default syntax policies are not supported for this type of content switching policy.
- **URL-based policies.** The appliance compares an incoming URL with the URLs specified in the policies. The appliance then returns the most appropriate URL-based content, which is usually the longest matching configured URL. URL-based policies must be classic policies; default syntax policies are not supported for this type of content switching policy.
- **Rule-based policies.** The appliance compares incoming data to expressions specified in the policies. You create rule-based policies by using either a classic expression or a default syntax expression. Both classic and default syntax policies are supported for rule-based content switching policies.

  Note: A rule based policy can be configured with an optional action. A policy with an action can be bound to multiple virtual servers or policy labels.

  If you set a priority when binding your policies to the content switching virtual server, the policies are evaluated in order of priority. If you do not set specific priorities when binding your policies, the policies are evaluated in the order in which they were created.

For information about NetScaler classic policies and expressions, see "Configuring Classic Policies and Expressions." For information about Default Syntax policies, see "Configuring Default Syntax Expressions."

To create a content switching policy by using the command line interface

At the command prompt, type one of the following commands:

- add cs policy <policyName> -domain <domain>
- add cs policy <policyName> -url <URLValue>
- add cs policy <policyName> -rule <RULEValue>
- add cs policy <policyName> -rule <RULEValue> -action <actionName>

Example

```
add cs policy Policy-CS-1 -url "/sports/*"

add cs policy Policy-CS-1 -domain "example.com"

add cs policy Policy-CS-1 -rule "CLIENT.IP.SRC.SUBNET(24).EQ(10.217.84.0)"

add cs policy Policy-CS-2 -rule "SYS.TIME.BETWEEN(GMT 2009 Nov,GMT 2009 Dec)"

add cs policy Policy-CS-3 -rule "http.req.method.eq(GET)" -action act1
```

Parameters for configuring content switching policies

policyName (Name)

Name for the content switching policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, “my policy” or ‘my policy’).

Cannot be changed after the policy is created.

domain (Domain)

The domain in the URL. The NetScaler appliance uses the domain to choose the correct content for each incoming request.

URLValue (URL)

An absolute or relative URL. The NetScaler appliance uses the URL to choose the correct content for each incoming request.

RULEValue (Expression)

A classic or default syntax policy expression that defines the appropriate content for each request.

action (Action)

Name of the content switching action to be used by the policy.

To create a content switching policy by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Policies.
2. In the details pane, click Add.
3. In the Create Content Switching Policy dialog box, in the Name text box, type the name of the policy (for example, Policy-CS-1).
4. Choose the type of policy that you want to create, and configure the policy.
   - To create a domain-based policy, in the Domain text box, type the domain (for example, example.com).
   - To create a URL-based policy, click URL, and in the Value text box, type an absolute or relative URL (for example, http://www.example.com/sports, or just /sports).
   - To create a rule-based policy, click Configure, and do the following:
     a. In the Create Expression dialog box, choose the expression syntax you want to use.
        - If you want to use default syntax, accept the default and proceed to the next step.
        - If you want to use classic syntax, click Switch to Classic Syntax.

        The Expression portion of the dialog box changes to match your choice. The default syntax Expression view has fewer elements than does the classic syntax Expression view. In the default syntax Expression view, instead of a preview window, a button provides access to an expression evaluator. The evaluator evaluates the expression you entered, to verify that it is valid, and displays an analysis of the expression's effect.
     b. Enter your policy expressions.
        - If you are using classic syntax and need further instructions, see Configuring Classic Policies and Expressions.
        - If you are using the default syntax and need further instructions, see Configuring Default Syntax Expressions.
5. Click Create, and then click Close. The policy you created appears in the Content Switching Policies pane.

Configuring Content Switching Policy Labels

A policy label is a user-defined bind point to which policies are bound. When a policy label is invoked, all the policies bound to it are evaluated in the order of the priority that you assigned to them. A policy label can include one or more policies, each of which can be assigned its own result. A match on one policy in the policy label can result in proceeding to the next policy, invoking a different policy label or appropriate resource, or an immediate end to policy evaluation and return of control to the policy that invoked the policy label. You can create policy labels for default syntax policies only.

For information about policy labels, see the "Creating Policy Labels."

A content switching policy label consists of a name, a label type, and a list of policies bound to the policy label. The policy label type specifies the protocol that was assigned to the policies bound to the label. It must match the service type of the content switching virtual server to which the policy that invokes the policy label is bound. For example, you can bind TCP Payload policies to a policy label of type TCP only. Binding TCP Payload policies to a policy label of type HTTP is not supported.

Each policy in a content switching policy label is associated with either a target (which is equivalent to the action that is associated with other types of policies, such as rewrite and responder policies) or a gotoPriorityExpression option and/or an invoke option. That is, for a given policy in a content switching policy label, you can specify a target, or you can set the gotoPriorityExpression option and/or the invoke option. Additionally, if multiple policies evaluate to true, only the target of the last policy that evaluates to true is considered.

You can use either the NetScaler command line or the configuration utility to configure content switching policy labels. In the NetScaler command-line interface (CLI), you first create a policy label by using the add cs policylabel command. Then, you bind policies to the policy label, one policy at a time, by using the bind cs policylabel command. In the NetScaler configuration utility, you perform both tasks in a single dialog box.

To create a content switching policy label by using the command line interface

At the command prompt, type:

add cs policylabel <labelName> <cspolicylabelTypetype>

Example

add cs policylabel testpollab http

Parameters for creating content switching policy labels

name (Name)

Name for the policy label. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, “my label” or ‘my label’). The label name must be unique within the list of policy labels for content switching. Cannot be changed after the policy label is created.

type (Label type)

Protocol supported by the policy label. All policies bound to the policy label must either match the specified protocol or be a subtype of that protocol. Available settings function as follows:

- **HTTP**—Supports policies that process HTTP traffic. Used to access unencrypted Web sites.
- **SSL**—Supports policies that process HTTPS/SSL encrypted traffic. Used to access encrypted Web sites.
- **TCP**—Supports policies that process any type of TCP traffic, including HTTP.
- **SSL_TCP**—Supports policies that process SSL-encrypted TCP traffic, including SSL.
- **UDP**—Supports policies that process any type of UDP-based traffic, including DNS.
- **DNS**—Supports policies that process DNS traffic.
- **ANY**—Supports all types of policies except HTTP, SSL, and TCP.
- **SIP_UDP**—Supports policies that process UDP based Session Initiation Protocol (SIP) traffic. SIP initiates, manages, and terminates multimedia communications sessions, and has emerged as the standard for Internet telephony (VoIP).
- **RTSP**—Supports policies that process Real Time Streaming Protocol (RTSP) traffic. RTSP provides delivery of multimedia and other streaming data, such as audio, video, and other types of streamed media.
- **RADIUS**—Supports policies that process Remote Authentication Dial In User Service (RADIUS) traffic. RADIUS supports combined authentication, authorization, and auditing services for network management.
- **RDP**—Supports policies that process remote desktop traffic.
- **MYSQL**—Supports policies that process MYSQL traffic.
- **MSSQL**—Supports policies that process Microsoft SQL traffic.

All policies bound to the policy label must either match the designated protocol or be a subtype of the designated protocol.

To bind a policy to a content switching policy label by using the command line interface

At the command prompt, type the following commands to bind a policy to a policy label and verify the configuration:

- bind cs policylabel <labelName> <policyName> <priority>[[-targetVserver <string>] | [-gotoPriorityExpression <expression>] | [-invoke <labeltype> <labelName>]]
- show cs policylabel <labelName>

Example

```
bind cs policylabel testpollab test_Pol 100 -targetVserver LBVIP
show cs policylabel testpollab
        Label Name: testpollab
        Label Type: HTTP
        Number of bound policies: 1
        Number of times invoked: 0
1)      Policy Name: test_Pol
        Priority: 100
        Target Virtual Server: LBVIP
```

Note: If a policy is configure with an action, the target virtual server (targetVserver), go to priority expression (gotoPriorityExpression), and invoke (invoke) parameters are not required. If a policy is not configure with an action, you need to configure at least one of the following parameters: targetVserver, gotoPriorityExpression, and invoke.

Parameters for binding a policy to a content switching policy label

labelName

Name of the policy label to which to bind a content switching policy.

policyName

Name of the content switching policy to bind to the content switching policy label.

priority

Unsigned integer that determines the priority of the policy relative to other policies in this policy label. Smaller the number, higher the priority.

targetVserver

Name of the virtual server to which to forward requests that match the policy.

gotoPriorityExpression

Expression or other value specifying the priority of the next policy to be evaluated if the current policy rule evaluates to TRUE. Alternatively, you can specify one of the following values:

- **NEXT**. Go to the policy with the next higher priority.
- **END**. End evaluation. (This is the default. Evaluation stops if the gotoPriorityExpression parameter is not set.)
- **USE_INVOCATION_RESULT**. Applicable if this entry invokes another policy label. If the final Goto in the invoked policy label has a value of END, evaluation stops. If the final Goto is anything other than END, the current policy label performs a NEXT.

invoke

Invoke other policy labels. After evaluating the policies in the invoked policy label, the appliance continues to evaluate policies that are bound to the current policy label (the selected bind point).

labelType

Type of policy label to be invoked.

To unbind a policy from a policy label by using the command line interface

At the command prompt, type the following commands to unbind a policy from a policy label and verify the configuration:

- unbind cs policylabel <labelName> <policyName>
- show cs policylabel <labelName>

Example

```
unbind cs policylabel testpollab test_Pol
show cs policylabel testpollab
      Label Name: testpollab
      Label Type: HTTP
      Number of bound policies: 0
      Number of times invoked: 0
```

Parameters for unbinding a policy from a content switching policy label

labelName

Name of the policy label from which to unbind a content switching policy.

policyName

Name of the content switching policy to unbind from the label.

To remove a policy label by using the command line interface

At the command prompt, type:

rm cs policylabel <labelName>

To manage a content switching policy label by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Policy Labels.
2. In the details pane, do one of the following:
   - To create a new policy label, click Add.
   - To modify an existing policy label, select the policy label, and then click Open.
3. In the Create Content Switching Policy Label dialog box, set the following parameters:
   - Name*
   - Label Type*

   * A required parameter
4. To add a policy to a list, click Insert Policy, and then click one of the policies in the drop-down list. If you click New Policy, create a new policy as described in "Creating Content Switching Policies."
5. For the policy that you added to the list, set the following parameters:
   - Priority* (The default value is 100. To modify the value, double-click in the Priority column.)
   - Target
   - Goto Expression
   - Invoke

   * A required parameter
6. To automatically renumber the policies, click Regenerate Priorities.
7. Click Create or OK.

Binding Policies to a Content Switching Virtual Server

After you create your content switching virtual server and policies, you bind each policy to the content switching virtual server. When binding the policy to the content switching virtual server, you specify the target load balancing virtual server.

Note: If your content switching policy uses a default syntax rule, you can configure a content switching action for the policy. If you configure an action, you must specify the target load balancing virtual server when you are configuring the action, not when you are binding the policy to the content switching virtual server. For more information about configuring a content switching action, see Configuring a Content Switching Action.

To bind a policy to a content switching virtual server and select a target load balancing virtual server by using the command line interface

At the command prompt, type:

bind cs vserver <name>[-lbvserver<string> -targetLBVServer<string> -policyname <string> -priority <positive_integer>] [-gotoPriorityExpression <expression>] [-type (REQUEST | RESPONSE)] [-invoke (<labelType> <labelName>)]

Example

bind cs vserver csw-vip2 -policyname csw-ape-policy2 -priority 14 -gotoPriorityExpression NEXT

bind cs vserver csw-vip3 -policyname rewrite-policy1 -priority 17 -gotoPriorityExpression 'q.header("a").count' -flowtype REQUEST -invoke policylabel label1

bind cs vserver Vserver-CS-1 Vserver-LB-1 -policyname Policy-CS-1 -priority 20

Note: The parameters, target load balancing virtual server (targetVserver), go to priority expression (gotoPriorityExpression), and invoke method (invoke) cannot be used if a policy has an action.

To bind a policy to a content switching virtual server and select a target load balancing virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, double-click the virtual server for which you want to bind the policy (for example, Vserver-CS-1).
3. In the Configure Virtual Server (Content Switching) dialog box, on the Policies tab, click Insert Policy. A list of existing policies appears in the Policy Name drop-down list, You can either select an existing policy or create a new policy:
   - Select an existing policy that you previously created to bind to the virtual server.
   - Select New Policy from the Policy Name drop-down list to create a new content switching policy. After you create a new policy, it is automatically bound to the virtual server.
4. Click OK.

Verifying the Configuration

To verify that your content switching configuration is correct, you need to view the content switching entities. To verify proper operation after your content switching configuration has been deployed, you can view the statistics that are generated as the servers are accessed.

Viewing the Properties of Content Switching Virtual Servers

You can view the properties of content switching virtual servers that you have configured on the NetScaler. You can use the information to verify whether the virtual server is correctly configured and, if necessary, to troubleshoot. In addition to details such as name, IP address, and port, you can view the various policies bound to a virtual server, and its traffic-management settings.

The content switching policies are displayed in the order of their priority. If more than one policy has the same priority, they are shown in the order in which they are bound to the virtual server.

Note: If you have configured the content switching virtual server to forward traffic to a load balancing virtual server, you can also view the content switching policies by viewing the properties of the load balancing virtual server.

To view the properties of content switching virtual servers by using the command line interface

To list basic properties of all content switching virtual servers in your configuration, or detailed properties of a specific content switching virtual server, at the command prompt, type one of the following commands:

- show cs vserver
- show cs vserver <name>

Example

1.

```
show cs vserver Vserver-CS-1
Vserver-CS-1 (10.102.29.161:80) - HTTP Type: CONTENT
State: UP
Last state change was at Thu Jun 30 10:48:59 2011
Time since last state change: 6 days, 20:03:00.760
Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED
Default: Content Precedence: RULE
Vserver IP and Port insertion: OFF
Case Sensitivity: ON
Push: DISABLED Push VServer:
```

Push Label Rule: none

...
1) Policy : __ESNS_PREBODY_POLICY Priority:0
2) Policy : __ESNS_POSTBODY_POLICY Priority:0

1) Compression Policy Name: __ESNS_CMP_POLICY Priority: 2147483647
GotoPriority Expression: END
Flowtype: REQUEST

1) Rewrite Policy Name: __ESNS_REWRITE_POLICY Priority: 2147483647
GotoPriority Expression: END
Flowtype: REQUEST

1) Cache Policy Name: dfbx Priority: 10
GotoPriority Expression: END
Flowtype: REQUEST

1) Responder Policy Name: __ESNS_RESPONDER_POLICY Priority: 2147483647
GotoPriority Expression: END

1) Policy: wiki Target: LBVIP2 Priority: 25 Hits: 0
2) Policy: plain Target: LBVIP1 Priority: 90 Hits: 0
3) Policy: DispOrderTest2 Target: KerbAuthLBVS Priority: 91 Hits: 0
4) Policy: test_Pol Target: LBVIP1 Priority: 92 Hits: 0
5) Policy: PolicyNameTesting Target: LBVIP1 Priority: 100 Hits: 0
Done
>

2.
show cs vserver
1) Vserver-CS-1 (10.102.29.161:80) - HTTP Type: CONTENT
State: UP
…
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED

2) apubendpt (10.111.111.1:80) - HTTP Type: CONTENT
State: UP
…
Client Idle Timeout: 180 sec
Down state flush: DISABLED
…

3) apubendpt1 (10.111.111.2:80) - HTTP Type: CONTENT
State: UP
…
Disable Primary Vserver On Down : DISABLED
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED
…

To view the properties of content switching virtual servers by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, click a virtual server to display its configuration details at the bottom of the screen.
3. To display the names of the policies that are bound to the content switching virtual server, double-click the virtual server and then click the Policies tab.

Viewing Content Switching Policies

You can view the properties of the content switching policies that you defined, such as the name, domain, and URL or expression, and use the information to find any mistakes in the configuration, or to troubleshoot if something is not working as it should.

To view the properties of content switching policies by using the command line interface

To list either basic properties of all content switching policies in your configuration or detailed properties of a specific content switching policy, at the command prompt, type one of the following commands:

- show cs policy
- show cs policy <PolicyName>

Example

show cs policy

show cs policy Policy-CS-1

To view the properties of content switching policies by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Policies.
2. In the details pane, double-click a policy to view the details.
3. To view the policy labels and virtual servers that this policy is bound to, on the Content Switching Policies pane, click Show Bindings.

Viewing a Content Switching Virtual Server Configuration by Using the Visualizer

The Content Switching Visualizer is a tool that you can use to view a content switching configuration in graphical format. You can use the visualizer to view the following configuration items:

- A summary of the load balancing virtual servers to which the content switching virtual server is bound.
- All services and service groups that are bound to the load balancing virtual server and all monitors that are bound to the services.
- The configuration details of any displayed element.
- Any policies bound to the content switching virtual server. These policies need not be content switching policies. Many types of policies, such as Rewrite policies, can be bound to a content switching virtual server.

After you configure the various elements in a content switching and load balancing setup, you can export the entire configuration to an application template file.

Note: The Visualizer requires a graphical interface, so it is available only through the configuration utility.

To view a content switching configuration by using the Visualizer in the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to view, and then click Visualizer.
3. In the Content Switching Visualizer window, you can adjust the viewable area as follows:
   - Click the Zoom In and Zoom Out icons to increase or decrease the viewable area.
   - Click the Save Image icon to save the graph as an image file.
   - In the Search in text field, begin typing the name of the item you are looking for. When you have typed enough characters to identify the item, its location is highlighted. To restrict the search, click the drop-down menu and select the type of element that you want to search for.
4. To view configuration details for entities that are bound to this virtual server, you can do the following:
   - To view policies that are bound to the virtual server, in the tool bar at the top of the dialog box select one or more feature-specific policy icons. If policy labels are configured, they appear in the main view area.
   - To view the configuration details for a bound service or service group, click the icon for the service, click the Related Tasks tab, and then click Show Member Services.
   - To view the configuration details for a monitor, click the icon for the monitor, click the Related Tasks tab, and then click View Monitor.
5. To view detailed statistics for any virtual server in the content switching configuration, click the virtual server for which you want to view statistics, then click the Related Tasks tab, and then click Statistics.
6. To view a comparative list of the parameters whose values either differ or are not defined across service containers for a load balancing virtual server, click the icon for a container, click the Related Tasks tab, and then click Service Attributes Diff.
7. To view monitor binding details for the services in a container, in the Service Attributes Diff dialog box, in the Group column for the container, click Details. This comparative list helps you determine which service container has the configuration you want to apply to all the service containers.
8. To view the number of requests received per second at a given point in time by the virtual servers in the configuration, and the number of hits per second at a given point in time for rewrite, responder, and cache policies, click Show Stats. The statistical information is displayed on the respective nodes in the Visualizer. This information is not updated in real time. It has to be refreshed manually. To refresh the information, click Refresh Stats.

   Note: This option is available only on NetScaler nCore builds.

9. To copy configuration details for an element to a document or spreadsheet, click the icon for that element, click Related Tasks, click Copy Properties, and then paste the information into a document.

10. To export the entire configuration that is displayed in the Visualizer to an application template file, click the icon for the content switching virtual server, click Related Tasks, and then click Create Template. When creating the application template, you can configure variables in some policy expressions and actions. For more information about creating the application template file and configuring variables for a template, see AppExpert.

Customizing the Basic Content Switching Configuration

After you configure a basic content switching setup, you might need to customize it to meet your requirements. If your web servers are UNIX-based and rely on case sensitive pathnames, you can configure case sensitivity for policy evaluation. You can also set precedence for evaluation of the content switching policies that you configured. If you want to configure content switching for a specific a virtual LAN, you can configure a content switching virtual server with a listen policy.

Configuring Case Sensitivity for Policy Evaluation

You can configure the content switching virtual server to treat URLs as case sensitive in URL-based policies. When case sensitivity is configured, the NetScaler appliance considers case when evaluating policies. For example, if case sensitivity is off, the URLs /a/1.htm and /A/1.HTM are treated as identical. If case sensitivity is on, those URLs are treated as separate and can be switched to different targets.

To configure case sensitivity by using the command line interface

At the command prompt, type:

set cs vserver <name> -caseSensitive (ON|OFF)

Example

set cs vserver Vserver-CS-1 -caseSensitive ON

Parameters for configuring case sensitivity

vServerName

The name of the content switching virtual server that you are configuring. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

caseSensitive

The URL lookup case option on the content switching vserver. If case sensitivity of a content switching virtual server is set to 'ON', the URLs /a/1.html and /A/1.HTML are treated differently and may have different targets (set by content switching policies).

If case sensitivity is set to 'OFF', the URLs /a/1.html and /A/1.HTML are treated the same, and will be switched to the same target.

Possible values: ON, OFF

Default value: ON

To configure case sensitivity by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure case sensitivity (for example, Vserver-CS-1), and then click Open.
3. In the Configure Virtual Server (Content Switching) dialog box, on the Advanced tab, select Case Sensitivity check box, and then click OK.

Setting the Precedence for Policy Evaluation

Precedence refers to the order in which policies that are bound to a virtual server are evaluated. You do not normally have to configure precedence: the default precedence works correctly in many cases. If you want to make sure that one policy or set of policies is applied first, however, and another policy or set of policies is applied only if the first set does not match a request, you can configure either URL-based precedence or rule-based precedence.

Precedence with URL-Based Policies

If there are multiple matching URLs for the incoming request, the precedence (priority) for URL-based policies is:

1. Domain and exact URL
2. Domain, prefix, and suffix
3. Domain and suffix
4. Domain and prefix
5. Domain only
6. Exact URL
7. Prefix and suffix
8. Suffix only
9. Prefix only
10. Default

If you configure precedence based on URL, the request URL is compared to the configured URLs. If none of the configured URLs match the request URL, then rule-based policies are checked. If the request URL does not match any rule-based policies, or if the content group selected for the request is down, then the request is processed as follows:

- If you configure a default group for the content switching virtual server, then the request is forwarded to the default group.
- If the configured default group is down or if no default group is configured, then an “HTTP 404 Not Found” error message is sent to the client.

Note: You should configure URL-based precedence if the content type (for example, images) is the same for all clients. However, if different types of content must be served

based on client attributes (such as Accept-Language), you must use rule-based precedence.

Precedence with Rule-Based Policies

If you configure precedence based on rules, which is the default setting, the request is tested on the basis of the rule-based policies you have configured. If the request does not match any rule-based policies, or if the content group selected for the incoming request is down, the request is processed in the following manner:

- If a default group is configured for the content switching virtual server, the request is forwarded to the default group.
- If the configured default group is down or if no default group is configured, an “HTTP 404 Not Found” error message is sent to the client.

To configure precedence by using the command line interface

At the command prompt, type:

set cs vserver <name> -precedence (RULE | URL)

Example

set cs vserver Vserver-CS-1 -precedence RULE

Parameters for configuring precedence

vServerName

The name of the content switching virtual server that you are configuring. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

precedence

The type of precedence to use for both RULE-based and URL-based policies on the content switching virtual server. With the precedence set to RULE, incoming requests are evaluated against the rule-based content switching policies. If none of the rules match, the URL in the request is evaluated against the URL-based content switching policies. Possible values: RULE, URL. Default: RULE.

To configure precedence by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure precedence, (for example, Vserver-CS-1), and then click Open.
3. In the Configure Virtual Server (Content Switching) dialog box, on the Advanced tab, under Precedence, click Rule or URL, and then click OK.

Configuring per-VLAN Wildcarded Virtual Servers

If you want to configure content switching for traffic on a specific virtual local area network (VLAN), you can create a wildcarded virtual server with a listen policy that restricts it to processing traffic only on the specified VLAN.

To configure a wildcarded virtual server that listens to a specific VLAN by using the command line interface

At the command prompt, type:

add cs vserver <name> <serviceType> IPAddress * Port * -listenpolicy <expression> [-listenpriority <positive_integer>]

Example

```
add cs vserver Vserver-CS-vlan1 ANY * *
    -listenpolicy "CLIENT.VLAN.ID.EQ(2)"  -listenpriority 10
```

Parameters for configuring per-VLAN wildcarded virtual servers

name

Name of the virtual server. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

IPAddress

IP address of the virtual server. For wildcarded virtual servers bound to VLANs, this is always *.

type

Behavior of the service. Select one of the following service types: HTTP, SSL, TCP, FTP, RTSP, SSL_TCP, UDP, DNS, SIP_UDP, ANY, RADIUS, RDP, MYSQL, MSSQL.

port

Port on which the virtual server listens for client connections. The port number must be in the range 0-65535. For wildcarded virtual servers bound to VLANs, the setting is

normally *.

listenpriority

The priority assigned to the listen policy. This can be any positive integer. Priority is evaluated in reverse order; the lower the number, the higher the priority assigned to the listen policy.

rule

The policy rule to use to identify the VLAN that you want this virtual server to listen to. This rule is:

CLIENT.VLAN.ID.EQ(<integer>)

For <integer>, substitute the ID number assigned to the VLAN.

To configure a wildcarded virtual server that listens to a specific VLAN by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, do one of the following:
   - To create a new virtual server, click Add.
   - To modify an existing virtual server, select the virtual server, and then click Open.
3. In the Create Virtual Server or Configure Virtual Server dialog box, on the Services tab, type or select values for the following parameters:
   - Name*—name
   - Protocol*—type
   - IP address*—IPAddress
   - Port—port

   * A required parameter
4. In the Advanced tab, expand Listen Policy, and then type or select values for the following parameters:
   - Listen Priority*—priority
   - Listen Policy Rule*—rule

   * A required parameter
5. Click Create or OK, depending on whether you are creating a new virtual server or modifying an existing virtual server.
6. Click Close. The virtual server that you created now appears in the Virtual Servers page.
7. To remove a virtual server, in the Virtual Servers pane select the virtual server, and then click Remove.

After you have created this virtual server, you bind it to one or more services as described in Binding Services to the Virtual Server.

Configuring the Microsoft SQL Server Version Setting

You can specify the version of Microsoft® SQL Server® for a content switching virtual server that is of type MSSQL. The version setting is recommended if you expect some clients to not be running the same version as your Microsoft SQL Server product. The version setting provides compatibility between the client-side and server-side connections by ensuring that all communication conforms to the server's version.

To set the Microsoft SQL Server version parameter by using the command line interface

At the command prompt, type the following commands to set the Microsoft SQL Server version parameter for a content switching virtual server and verify the configuration:

- set cs vserver <name> -mssqlServerVersion <mssqlServerVersion>
- show cs vserver <name>

Example

```
> set cs vserver myMSSQLcsvip -mssqlServerVersion 2008R2
 Done
> show cs vserver myMSSQLcsvip
    myMSSQLcsvip (192.0.2.13:1433) - MSSQL  Type: CONTENT
    State: UP
    . . .
    . . .
    MSsql Server Version: 2008R2
    . . .
    . . .
 Done
>
```

Parameters for configuring the MS SQL Server version setting

name

The name of the virtual server for which you want to configure the MS SQL Server version setting.

mssqlServerVersion

The version of MS SQL Server that you are using. Following are the possible values:

- `70`, for Microsoft SQL Server 7.0
- `2000`, for Microsoft SQL Server 2000
- `2000SP1`, for Microsoft SQL Server 2000 Service Pack 1 (SP1)
- `2005`, for Microsoft SQL Server 2005
- `2008`, for Microsoft SQL Server 2008
- `2008R2`, for Microsoft SQL Server 2008 R2

To set the Microsoft SQL Server version parameter by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure the setting, and then click Open.
3. In the Configure Virtual Server dialog box, do the following:
   a. In the advanced tab, click MsSql.
   b. In the Server Version list, select the version of your Microsoft SQL Server product.
   c. Click Create or OK, and then click Close.

Protecting the Content Switching Setup against Failure

Content switching may fail when the content switching virtual server goes DOWN or fails to handle excessive traffic, or for other reasons. To reduce the chances of failure, you can take the following measures to protect the content switching setup against failure:

- Configure a backup content switching virtual server.
- Configure spillover for preventing the overloading of the primary and diverting excess traffic to the backup virtual server.
- Specify a redirect URL, the URL to which the content is switched if both the primary and backup content switching virtual servers are DOWN.
- Enable the State Update option for marking a content switching virtual server as DOWN when the load balancing virtual server is DOWN.
- Flush the surge queues when the queues become too long.

Configuring a Redirection URL

You can configure a redirect URL to communicate the status of the NetScaler appliance in the event that a content switching virtual server of type HTTP or HTTPS is DOWN or DISABLED. This URL can be local or remote.

Redirect URLs can be absolute URLs or relative URLs. If the configured redirect URL contains an absolute URL, the HTTP redirect is sent to the configured location, regardless of the URL specified in the incoming HTTP request. If the configured redirect URL contains only the domain name (relative URL), the HTTP redirect is sent to a location after appending the incoming URL to the domain configured in the redirect URL.

Note: If a content switching virtual server is configured with both a backup virtual server and a redirect URL, the backup virtual server takes precedence over the redirect URL. A redirect URL is used when the primary and backup virtual servers are down.

When redirection is configured and the content switching virtual server is unavailable, the appliance issues an HTTP 302 redirect to the user's browser.

To configure a redirect URL for when the content switching virtual server is unavailable by using the command line interface

At the command prompt, type:

set cs vserver <name> -redirectURL <URLValue>

Example

set cs vserver Vserver-CS-1 -redirectURL http://www.newdomain.com/mysite/maintenance

Parameters for configuring a redirect URL

vServerName

The name of the content switching virtual server that you are configuring. This alphanumeric string is required and cannot be changed after the virtual server is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

URLValue

URL to which traffic is redirected if the content switching virtual server becomes unavailable. This value must not exceed 127 characters. The domain specified in the URL

must not match the domain specified in the domain name argument of a content switching policy. If the same domain is specified in both arguments, the request is redirected continuously to the same unavailable virtual server in the NetScaler, and the user cannot get the requested content.

To configure a redirect URL for when the content switching virtual server is unavailable by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure a redirect URL (for example, Vserver-CS-1), and then click Open.
3. In the Configure Virtual Server (Content Switching) dialog box, on the Advanced tab, in the Redirect URL text box, type the redirect URL (for example, http://www.newdomain.com/mysite/maintenance).
4. Click OK.

Configuring a Backup Virtual Server

If the primary content switching virtual server is marked DOWN or DISABLED, the NetScaler appliance can direct requests to a backup content switching virtual server. It can also send a notification message to the client regarding the site outage or maintenance. The backup content switching virtual server is a proxy and is transparent to the client.

When configuring the backup virtual server, you can specify the configuration parameter Disable Primary When Down to ensure that, when the primary virtual server comes back up, it remains the secondary until you manually force it to take over as the primary. This is useful if you want to ensure that any updates to the database on the server for the backup are preserved, enabling you to synchronize the databases before restoring the primary virtual server.

You can configure a backup content switching virtual server when you create a content switching virtual server or when you change the optional parameters of an existing content switching virtual server. You can also configure a backup content switching virtual server for an existing backup content switching virtual server, thus creating cascaded backup content switching virtual servers. The maximum depth of cascaded backup content switching virtual servers is 10. The appliance searches for a backup content switching virtual server that is up and accesses that content switching virtual server to deliver the content.

Note: If a content switching virtual server is configured with both a backup content switching virtual server and a redirect URL, the backup content switching virtual server takes precedence over the redirect URL. The redirect is used when the primary and backup virtual servers are down.

To set up a backup content switching virtual server by using the command line interface

At the command prompt, type:

set cs vserver <name> -backupVserver <string> -disablePrimaryOnDown (ON|OFF)

Example

set cs vserver Vserver-CS-1 -backupVserver Vserver-CS-2 -disablePrimaryOnDown ON

Parameters for configuring a backup virtual server

primaryVServer

The name of the primary virtual server for which you are configuring a backup. This alphanumeric string is required and cannot be changed after the virtual server is

created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

backupVServer

The name of the backup virtual server that you are configuring. This alphanumeric string is required and cannot be changed after the virtual server is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

You can create a virtual server and specify the name, IP address, port, and type as described in Creating Content Switching Virtual Servers. You can use the name of the content switching virtual server as a backup content switching virtual server.

disablePrimaryOnDown

Configures the appliance to leave the former primary virtual server as secondary until you manually set it to take over as the primary. Possible Values: ON, OFF. Default: OFF.

To set up a backup content switching virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to set up a backup content switching virtual server (for example, Vserver-CS-1), and then click Open.
3. In the Configure Virtual Server (Content Switching) dialog box, click the Advanced tab.
4. In the Backup Virtual Server list, select the backup virtual server (for example, Vserver-CS-2).
5. If you want to configure the backup server to remain as the primary server after the primary virtual server is brought back up, select the Disable Primary When Down check box.
6. Click OK.

Diverting Excess Traffic to a Backup Virtual Server

The spillover option diverts new connections arriving at a content switching virtual server to a backup content switching virtual server when the number of connections to the content switching virtual server exceeds the configured threshold value. The threshold value is dynamically calculated, or you can set the value. The number of established connections (in case of TCP) at the virtual server is compared with the threshold value. When the number of connections reaches the threshold, new connections are diverted to the backup content switching virtual server.

If the backup content switching virtual servers reach the configured threshold and are unable to take the load, the primary content switching virtual server diverts all requests to the redirect URL. If a redirect URL is not configured on the primary content switching virtual server, subsequent requests are dropped.

To configure a content switching virtual server to divert new connections to a backup virtual server by using the command line interface

At the command prompt, type:

set cs vserver <name> -soMethod <methodType> -soThreshold <thresholdValue> -soPersistence <persistenceValue> -soPersistenceTimeout <timeoutValue>

Example

set cs vserver Vserver-CS-1 -soMethod Connection -soThreshold 1000 -soPersistence enabled -soPersistenceTi

Parameters for configuring spillover

vServerName

The name of the content switching virtual server for which you are configuring spillover. This alphanumeric string is required and cannot be changed after the virtual server is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

soMethod

Type of spillover used to divert traffic to the backup content switching virtual server when the virtual server reaches the spillover threshold. The valid options for this

parameter are: CONNECTION, BANDWIDTH, and NONE. For more information about how each of these methods work, see Load Balancing.

soThreshold

For the CONNECTION spillover type, the Threshold value is the maximum number of connections a virtual server can handle before spillover. For the BANDWIDTH spillover type, the Threshold value is the amount of incoming and outgoing traffic (in kilobits per second) that a virtual server can handle before spillover occurs. The minimum value is 1, and the maximum value is 4294967294.

soPersistence

The spillover persistence state. If you enable spillover persistence, the NetScaler maintains sourceIP-based persistence over primary virtual server and backup content switching virtual servers. The valid options for this parameter are: ENABLED and DISABLED. The default value is DISABLED.

soPersistenceTimeout

This value sets the timeout for spillover persistence. The default value is 2 minutes. The minimum value is 2 minutes, and the maximum value is 1440 minutes.

To set a content switching virtual server to divert new connections to a backup virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure spillover (for example, Vserver-CS-1), and then click Open.
3. In the Configure Virtual Server (Content Switching) dialog box, on the Advanced tab, under Spillover, in the Method list, select the type of spillover, and in Threshold text box, type the threshold value (for example, Connection and 1000).
4. Select the Persistence check box and, in Persistence Time-out (min) text box, type the timeout value (for example, 2).
5. Click OK.

Configuring the State Update Option

The content switching feature enables the distribution of client requests across multiple servers on the basis of the specific content presented to the users. For efficient content switching, the content switching virtual server distributes the traffic to the load balancing virtual servers according to the content type, and the load balancing virtual servers distribute the traffic to the physical servers according to the specified load balancing method.

For smooth traffic management, it is important for the content switching virtual server to know the status of the load balancing virtual servers. The state update option helps to mark the content switching virtual server DOWN if the load balancing virtual server bound to it is marked DOWN. A load balancing virtual server is marked DOWN if all the physical servers bound to it are marked DOWN.

When State Update is disabled:

The status of the content switching virtual server is marked as UP. It remains UP even if there is no bound load balancing virtual server that is UP.

When State Update is enabled:

When you add a new content switching virtual server, initially, its status is shown as DOWN. When you bind a load balancing virtual server whose status is UP, the status of the content switching virtual server becomes UP.

If more than one load balancing virtual server is bound and if one of them is specified as the default, the status of the content switching virtual server reflects the status of the default load balancing virtual server.

If more than one load balancing virtual server is bound without any of them being specified as the default, the status of the content switching virtual server is marked UP only if all the bound load balancing virtual servers are UP.

To configure the state update option by using the command line interface

At the command prompt, type:

add cs vserver <name> <protocol> <ipAddress> <port> -stateUpdate ENABLED

Example

add cs vserver csw_vserver HTTP 10.18.250.154 80 -stateupdate ENABLED -cltTimeout 180

Parameters for configuring state update option

vServerName

Name of the content switching virtual server. This alphanumeric string is required and cannot be changed after the content switching virtual server is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and blank space.

ipAddress

IP address of the virtual server. This IP address (VIP) is usually a public IP address to which the clients send connection requests.

port

Port on which the virtual server listens for client connections. The port number must be between 0-65535.

protocol

Protocol of the requests processed by the content switching virtual server. Possible values: HTTP, TCP, UDP, FTP, SSL, SSL_TCP, RTSP, DNS, SIP-UDP, ANY.

stateUpdate

Status of the content switching virtual server according to the status of the bound load balancing virtual server. Possible values: ENABLED, DISABLED. DEFAULT: DISABLED.

To configure the state update option by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, do one of the following:
   - To add a virtual server, click Add.
   - To modify a virtual server, select the server, and click Open.
3. In the Create Virtual Server (Content Switching) dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring content switching" as shown:
   - Name-vServerName
   - IP Address-ipAddress

     Note: If you need to enter an IPv6 address, select the IPv6 check box before you enter the address.
   - Port-port
   - Protocol-protocol
4. On the Advanced tab, select the State Update check box.
5. Click Create.
6. Select the new virtual server, click Open, and verify the settings.

Flushing the Surge Queue

When a physical server receives a surge of requests, it becomes slow to respond to the clients that are currently connected to it, which leaves users dissatisfied and disgruntled. Often, the overload also causes clients to receive error pages. To avoid such overloads, the NetScaler appliance provides features such as surge protection, which controls the rate at which new connections to a service can be established.

The appliance does connection multiplexing between clients and physical servers. When it receives a client request to access a service on a server, the appliance looks for an already established connection to the server that is free. If it finds a free connection, it uses that connection to establish a virtual link between the client and the server. If it does not find an existing free connection, the appliance establishes a new connection with the server, and establishes a virtual link between client and the server. However, if the appliance cannot establish a new connection with the server, it sends the client request to a surge queue. If all the physical servers bound to the load balancing or content switching virtual server reach the upper limit on client connections (max client value, surge protection threshold or maximum capacity of the service), the appliance cannot establish a connection with any server. The surge protection feature uses the surge queue to regulate the speed at which connections are opened with the physical servers. The appliance maintains a different surge queue for each service bound to the virtual server.

The length of a surge queue increases whenever a request comes for which the appliance cannot establish a connection, and the length decreases whenever a request in the queue gets sent to the server or a request gets timed out and is removed from the queue.

If the surge queue for a service or service group becomes too long, you may want to flush it. You can flush the surge queue of a specific service or service group, or of all the services and service groups bound to a load balancing virtual server. Flushing a surge queue does not affect the existing connections. Only the requests present in the surge queue get deleted. For those requests, the client has to make a fresh request.

You can also flush the surge queue of a content switching virtual server. If a content switching virtual server forwards some requests to a particular load balancing virtual server, and the load balancing virtual server also receives some other requests, when you flush the surge queue of the content switching virtual server, only the requests received from this content switching virtual server are flushed; the other requests in the surge queue of the load balancing virtual server are not flushed.

Note: You cannot flush the surge queues of cache redirection, authentication, VPN or GSLB virtual servers or GSLB services.

Note: Do not use the Surge Protection feature if Use Source IP (USIP) is enabled.

To flush a surge queue by using the command line interface

The flush ns surgeQ command works in the following manner:

- You can specify the name of a service, service group, or virtual server whose surge queue has to be flushed.
- If you specify a name while executing the command, surge queue of the specified entity will be flushed. If more than one entity has the same name, the appliance flushes surge queues of all those entities.
- If you specify the name of a service group, and a server name and port while executing the command, the appliance flushes the surge queue of only the specified service group member.
- You cannot directly specify a service group member (<serverName> and <port>) without specifying the name of the service group (<name>) and you cannot specify <port> without a <serverName>. Specify the <serverName> and <port> if you want to flush the surge queue for a specific service group member.
- If you execute the command without specifying any names, the appliance flushes the surge queues of all the entities present on the appliance.
- If a service group member is identified with a server name, you must specify the server name in this command; you cannot specify its IP address.

At the command prompt, type:

flush ns surgeQ [-name <name>] [-serverName <serverName> <port>]

Examples

1.
flush ns surgeQ –name SVC1ANZGB –serverName 10.10.10.1 80
The above command flushes the surge queue of the service or virtual server that is named SVC1ANZGB and h
2.
flush ns surgeQ
The above command flushes all the surge queues on the appliance.

Parameters for flushing a surge queue

name

Name of a virtual server, service or service group

serverName

Name of a service group member

To flush a surge queue by using the configuration utility

1. In the navigation pane, expand Load Balancing.
2. To select an entity, do one of the following:
   - To flush the surge queue of a virtual server, click Virtual Servers, and then select the virtual server.
   - To flush the surge queue of a service, click Services, and then select the service.
   - To flush the surge queue of all the members in a service group, click Service Groups, and then select the service group.
   - To flush the surge queue of a specific member in a service group, click Service Groups, and in the action pane, click Manage Members. In the Manage Members of a Service Group dialog box, select the service group member.

   Note: You can select multiple entities in any window.

   Note: To flush the surge queue of a content switching virtual server, in Steps 1 and 2, expand Content Switching, and then select a virtual server.
3. In the action pane, click Flush Surge Queue.
4. Click OK.

   Note: On the appliance, if there are other entities with the same name as you selected, you are alerted that the surge queues of those entities would also be flushed. Take an appropriate action.

Managing a Content Switching Setup

After a content switching setup is configured, it may require periodic changes. When operating systems or software are updated, or hardware wears out and is replaced, you may need to take down your setup. Load on your setup may increase, requiring additional resources. You may also modify the configuration to improve performance.

These tasks may require unbinding policies from the content switching virtual server, or disabling or removing content switching virtual servers. After you have made changes to your setup, you may need to re-enable servers and rebind policies. You might also want to rename your virtual servers.

Unbinding Policies from the Content Switching Virtual Server

When you unbind a content switching policy from its virtual server, the virtual server no longer includes that policy when determining where to direct requests.

To unbind a policy from a content switching virtual server by using the command line interface

At the command prompt, type:

unbind cs vserver <name> -policyname <string>

Example

unbind cs vserver Vserver-CS-1 -policyname Policy-CS-1

Parameters for unbinding content switching policies

vServerName

The name of the content switching virtual server from which you are unbinding the policy. This alphanumeric string is required and cannot be changed after the virtual server is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

policyName

The name of the policy that you are unbinding.

To unbind a policy from a content switching virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server form which you want to unbind the policy (for example, Vserver-CS-1), and click Open.
3. In the Configure Virtual Server (Content Switching) dialog box, on the Policies tab, in the Active column, clear the check box next to the policy that you want to unbind from the virtual server (for example, Policy-CS-1).
4. Click OK.

Removing Content Switching Virtual Servers

You normally remove a content switching virtual server only when you no longer require the virtual server. When you remove a content switching virtual server, the NetScaler appliance first unbinds all policies from the content switching virtual server, and then removes it.

To remove a content switching virtual server by using the command line interface

At the command prompt, type:

rm cs vserver <name>@

Example

rm cs vserver Vserver-CS-1

To remove a content switching virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to remove (for example, Vserver-CS-1), and then click Remove.
3. In the Remove dialog box, click Yes.

Disabling and Re-Enabling Content Switching Virtual Servers

Content switching virtual servers are enabled by default when you create them. You can disable a content switching virtual server for maintenance. If you disable the content switching virtual server, the state of the content switching virtual server changes to Out of Service. While out of service, the content switching virtual server does not respond to requests.

To disable or re-enable a virtual server by using the command line interface

At the command prompt, type one of the following commands:

- disable cs vserver <name>@
- enable cs vserver <name>@

Example

disable cs vserver Vserver-CS-1

enable cs vserver Vserver-CS-1

To disable or re-enable a virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to disable (for example, Vserver-CS-1).
3. Disable or re-enable the virtual server by clicking Disable or Enable, and then clicking Yes to confirm your choice.

Renaming Content Switching Virtual Servers

You can rename a content switching virtual server without unbinding it. The new name is propagated automatically to all affected parts of the NetScaler configuration.

To rename a virtual server by using the command line interface

At the command prompt, type:

rename cs vserver <name>@ <newName>@

Example

rename cs vserver Vserver-CS-1 Vserver-CS-2

To rename a virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to rename (for example, Vserver-CS-1).
3. Click Rename.
4. In the Name text box, type a new name for the virtual server.
5. Click OK to save your changes.

Managing Content Switching Policies

You can modify an existing policy by configuring rules or changing the URL of the policy, or you can remove a policy. You can create different policies based on the URL. URL-based policies can be of different types, as described in the following table.

Table 1. Examples of URL-Based Policies

Type of URL-Based Policy	Specifies
Domain and Exact URL	Requests must match the configured domain name and configured URL (an exact prefix match if only the prefix is configured; or an exact match of the prefix and suffix if both the prefix and suffix are configured). **Example:** **add cs policy Policy-CS-1 -url /sports/tennis/index.html -domain "www.domainxyz.com"**
Domain and Wild Card URL	Requests must match the exact domain name and a partial prefix of the configured URL. **Example:** **add cs policy Policy-CS-1 -url /*.jsp -domain "www.domainxyz.com"**
Domain Only	Requests need match only the configured domain name. **Example:** **add cs policy Policy-CS-1 -domain "www.domainxyz.com"**

The Exact URL	The incoming URL must exactly match the URL specified by the policy. If only a URL prefix rule is configured, there must be an exact prefix match with the incoming URL. If a URL prefix and suffix-based rule is configured, there should be an exact match of the prefix and suffix with the incoming URL. **Example:** **add cs policy Policy-CS-1 -url /sports/tennis/index.html**
Prefix Only (Wild Card URL)	All the incoming URLs must start with the configured prefix. **Example:** **add cs policy Policy-CS-1 -url /sports*** sports/*" matches all URLs under /sports "/sports*" matches all URLs whose prefix match "/sports" starting from the beginning of a URL
Suffix Only (Wild Card URL)	All incoming URLs must end with the configured URL suffix. **Example:** **add cs policy Policy-CS-1 -url /*.jsp** "/*.jsp" matches all URLs whose file extension is "jsp"
Prefix and Suffix (Wild Card URL)	All incoming URLs must start with the configured prefix and end with the configured suffix. **Example:** **add cs policy Policy-CS-1 -url /sports/*.jsp**

Note: You can configure rule-based content switching using classical policy expressions or advanced policy expressions. For more information about configuring policy expressions, see "Policy Configuration and Reference."

To modify, remove, or rename a policy by using the command line interface

At the command prompt, type one of the following commands:

- set cs policy <policyName> [-domain <domainValue>] [-rule <ruleValue>] [-url <URLValue>]
- rm cs policy <policyName>

Example

set cs policy Policy-CS-1 -domain "www.domainxyz.com"

set cs policy Policy-CS-1 -rule "CLIENT.IP.SRC.SUBNET(22).EQ(10.100.148.0)"

set cs policy Policy-CS-2 -rule "SYS.TIME.BETWEEN(GMT 2010 Jun,GMT 2010 Jul)"

set cs policy Policy-CS-1 -url /sports/*

rm cs policy Policy-CS-1

Parameters for configuring content switching policies

policyName

newPolicyName

New name for the content switching policy.

domain

The domain name. The alphanumeric string can range from 3 to 63 characters, and can consist of any characters that are allowed in a domain name.

rule

A NetScaler advanced policy expression that defines which requests to forward to a particular content switching virtual server.

url

A URL or partial URL that enables the NetScaler appliance to choose requests to forward to a particular content switching server.

To modify, remove, or rename a policy by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Policies.
2. In the details pane, select the policy that you want to modify (for example, Policy-CS-1).
3. Modify, remove, or rename the policy.
   - To modify the policy, click Open and then make the changes that you want. For example, you can type a new domain name in the Domain text box. Then, click Yes to confirm your changes.
   - To remove the policy, click Remove, and then click Yes to confirm your choice.
   - To rename the policy, click Rename, and specify the new name in the Name text field in the Rename CSW Policy dialog box, and then click OK.
4. In the Configure Content Switching Policies dialog box, in the Domain text box, type the domain name (for example, www.domainxyz.com).
5. Click OK.

Modifying a Content Switching Configuration by Using the Visualizer

You can use the Visualizer to modify a load balancing virtual server to which the content switching virtual server is bound. You can also modify a service or group of similar services, or a monitor. For more information, see "The Load Balancing Visualizer."

Managing Client Connections

To ensure efficient management of client connections, you can configure the content switching virtual servers on the NetScaler appliance to use the following features:

- Redirecting client requests to a cache
- Enabling delayed cleanup of virtual server connections
- Rewriting ports and protocols for redirection
- Inserting the IP address and port of a virtual server in the request header
- Setting a time-out value for idle client connections
- Configuring the ICMP Response. You can configure the NetScaler to send ICMP responses to PING requests according to your settings. On the IP address corresponding to the virtual server, set the ICMP RESPONSE to VSVR_CNTRLD, and on the virtual server, set the ICMP VSERVER RESPONSE.

  The following settings can be made on a virtual server:

  - When you set ICMP VSERVER RESPONSE to PASSIVE on all virtual servers, NetScaler always responds.
  - When you set ICMP VSERVER RESPONSE to ACTIVE on all virtual servers, NetScaler responds even if one virtual server is UP.
  - When you set ICMP VSERVER RESPONSE to ACTIVE on some and PASSIVE on others, NetScaler responds even if one virtual server set to ACTIVE is UP.

Identifying Connections with the 4-tuple and Layer 2 Connection Parameters

You can now set the L2Conn option for a content switching virtual server. With the L2Conn option set, connections to the content switching virtual server are identified by the combination of the 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>) and Layer 2 connection parameters. The Layer 2 connection parameters are the MAC address, VLAN ID, and channel ID.

To set the L2Conn option for a content switching virtual server by using the command line interface

At the command line, type the following commands to configure the L2Conn parameter for a content switching virtual server and verify the configuration:

- set cs vserver <name> -l2Conn (**ON** | **OFF**)
- show cs vserver <name>

Example

```
> set cs vserver mycsvserver -l2Conn ON
Done
> show cs vserver mycsvserver
    mycsvserver (192.0.2.56:80) - HTTP   Type: CONTENT
    State: UP
       . . .
       . . .
    L2Conn: ON Case Sensitivity: ON
       . . .
       . . .
Done
>
```

Parameters for identifying connections with the 4-tuple and layer 2 connection parameters

name (Name)

The name of the content switching virtual server.

l2Conn

Identify connections to the virtual server with the 4-tuple and the Layer 2 connection parameters (MAC address, VLAN ID, and channel ID). Possible values: ON, OFF.

To set the L2Conn option for a content switching virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, click the content switching virtual server for which you want to set the L2Conn option, and then click Open.
3. In the Configure Virtual Server (Content Switching) dialog box, on the Advanced tab, select L2 Connection.
4. Click OK.

Redirecting Client Requests to a Cache

The NetScaler cache redirection feature redirects HTTP requests to a cache. You can significantly reduce the burden of responding to HTTP requests and improve your Web site performance through proper implementation of the cache redirection feature.

A cache stores frequently requested HTTP content. When you configure cache redirection on a virtual server, the NetScaler appliance sends cacheable HTTP requests to the cache and non-cacheable HTTP requests to the origin Web server. For more information on cache redirection, see "Cache Redirection."

To configure cache redirection on a virtual server by using the command line interface

At the command prompt, type:

set cs vserver <name> -cacheable <Value>

Example

set cs vserver Vserver-CS-1 -cacheable yes

Parameters for configuring cache redirection

vServerName

The name of the virtual server that you are configuring.

cacheable

Route virtual server requests to the cache redirection virtual server before sending them to the configured servers. Possible values: YES, NO. Default: NO.

To configure cache redirection on a virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure cache redirection (for example, Vserver-CS-1), and then click Open.
3. In the Configure Virtual Server (Content Switching) dialog box, on the Advanced tab, select the Cache Redirection check box.
4. Click OK.

Enabling Delayed Cleanup of Virtual Server Connections

Under certain conditions, you can configure the down state flush setting to terminate existing connections when a service or a virtual server is marked DOWN. Terminating existing connections frees resources and in certain cases speeds recovery of overloaded load balancing setups.

To configure the down state flush setting on a virtual server by using the command line interface

At the command prompt, type:

set cs vserver <name> -downStateFlush <Value>

Example

set cs vserver Vserver-CS-1 -downStateFlush enabled

Parameters for configuring down state flush

vServerName

The name of the virtual server that you are configuring.

downStateFlush

Perform delayed cleanup of connections on the virtual server. Possible values: ENABLED, DISABLED. Default: ENABLED.

To configure the down state flush setting on a virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure down state flush (for example, Vserver-CS-1), and click Open.
3. In the Configure Virtual Server (Content Switching) dialog box, click the Advanced tab.
4. Select the Down state flush check box, and then click OK.

Rewriting Ports and Protocols for Redirection

Virtual servers and the services that are bound to them may use different ports. When a service responds to an HTTP connection with a redirect, you may need to configure the NetScaler appliance to modify the port and the protocol to ensure that the redirection goes through successfully. You do this by enabling and configuring the redirectPortRewrite setting.

To configure HTTP redirection on a virtual server by using the command line interface

At the command prompt, type:

set cs vserver <name> -redirectPortRewrite <Value>

Example

set cs vserver Vserver-CS-1 -redirectPortRewrite enabled

Parameters for redirect port rewrite

vServerName

The name of the virtual server that you are configuring.

redirectPortRewrite

State of port rewrite while performing HTTP redirect. Possible values: ENABLED and DISABLED. Default: DISABLED.

To configure HTTP redirection on a virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure HTTP redirection (for example, Vserver-CS-1), and then click Open.
3. In the Configure Virtual Server (Content Switching) dialog box, click the Advanced tab.
4. Select the Redirect Port Rewrite check box, and then click OK.

Inserting the IP Address and Port of a Virtual Server in the Request Header

If you have multiple virtual servers that communicate with different applications on the same service, you must configure the NetScaler appliance to add the IP address and port number of the appropriate virtual server to the HTTP requests that are sent to that service. This setting allows applications running on the service to identify the virtual server that sent the request.

If the primary virtual server is down and the backup virtual server is up, the configuration settings of the backup virtual server are added to the client requests. If you want the same header tag to be added, regardless of whether the requests are from the primary virtual server or backup virtual server, you must configure the required header tag on both virtual servers.

Note: This option is not supported for wildcarded virtual servers or dummy virtual servers.

To insert the IP address and port of the virtual server in the client requests by using the command line interface

At the command prompt, type:

set cs vserver <name> -insertVserverIPPort <vServerIPPORT>

Example

set cs vserver Vserver-CS-1 -insertVserverIPPort 10.201.25.136:80

Parameters for virtual server IP port insertion

vServerName

The name of the virtual server that you are configuring.

insertVserverIPPort

Virtual IP address and port header insertion option for the virtual server.

VIPADDR-Header contains the virtual server IP address and port number without any translation.

If VIPADDR is not specified, the header is inserted with the name specified in the default header tag vip-header and the virtual server IP and port are inserted in the request with the default header tag vipHeader.

If VIPADDR is specified, the header is inserted with the user-specified name in vipHeader. The virtual server IP and port are inserted in the request with the user-specified header tag vipHeader.

OFF- The virtual IP and port header insertion option is disabled. The virtual server and port number are not inserted.

V6TOV4MAPPING - If the virtual server uses an IPv6 address and the server uses IPv4, this setting maps the virtual server address and port to the IPv4 address.

Possible values: OFF, VIPADDR, and V6TOV4MAPPING. Default: OFF.

To insert the IP address and port of the virtual server in the client requests by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure virtual server port insertion (for example, Vserver-CS-1), and then click Open.
3. In the Configure Virtual Server (Content Switching) dialog box, click the Advanced tab.
4. In the Vserver IP Port Insertion list, select the VIPADDR or V6TOV4MAPPING, and then type the port header in a text box next to Vserver IP Port Insertion box.
5. Click OK.

Setting a Time-out Value for Idle Client Connections

You can configure a virtual server to terminate any idle client connections after a configured time-out period elapses. When you configure this setting, the NetScaler appliance waits for the time you specify and, if the client is idle after that time, it closes the client connection.

To set a time-out value for idle client connections by using the command line interface

At the command prompt, type:

set cs vserver <name> -cltTimeout <Value>

Example

set cs vserver Vserver-CS-1 -cltTimeout 100

Parameters for setting the client time-out value

vServerName

The name of the virtual server that you are configuring.

cltTimeout

Idle time (in seconds) after which the client connection is terminated. The default values are:

- 180 seconds for HTTP/SSL-based services.
- 9000 seconds for other TCP-based services.
- 180 seconds for DNS-based services.
- 180 seconds for other UDP-based services.

Maximum value: 31536000.

To set a time-out value for idle client connections by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to set a time-out value (for example, Vserver-CS-1), and then click Open.
3. In the Configure Virtual Server (Content Switching) dialog box, click the Advanced tab.
4. In the Client Time-out (secs) text box, type the time-out value (for example, 100).
5. Click OK.

DataStream

The NetScaler DataStream feature provides an intelligent mechanism for request switching at the database layer by distributing requests based on the SQL query being sent.

When deployed in front of database servers, a NetScaler ensures optimal distribution of traffic from the application servers and Web servers. Administrators can segment traffic according to information in the SQL query and on the basis of database names, usernames, character sets, and packet size.

You can either configure load balancing to switch requests based on load balancing algorithms or elaborate the switching criteria by configuring content switching to make a decision based on an SQL query parameters. You can further configure monitors to track the state of database servers.

Note: NetScaler DataStream is supported only for MySQL and MS SQL databases. For information about the supported protocol version, character sets, special queries, and transactions, see DataStream Reference.

How NetScaler DataStream Works

In DataStream, the NetScaler is placed in-line between the application and/or Web servers and the database servers. On the NetScaler appliance, the database servers are represented by services.

A typical DataStream deployment consists of the entities described in the following diagram.

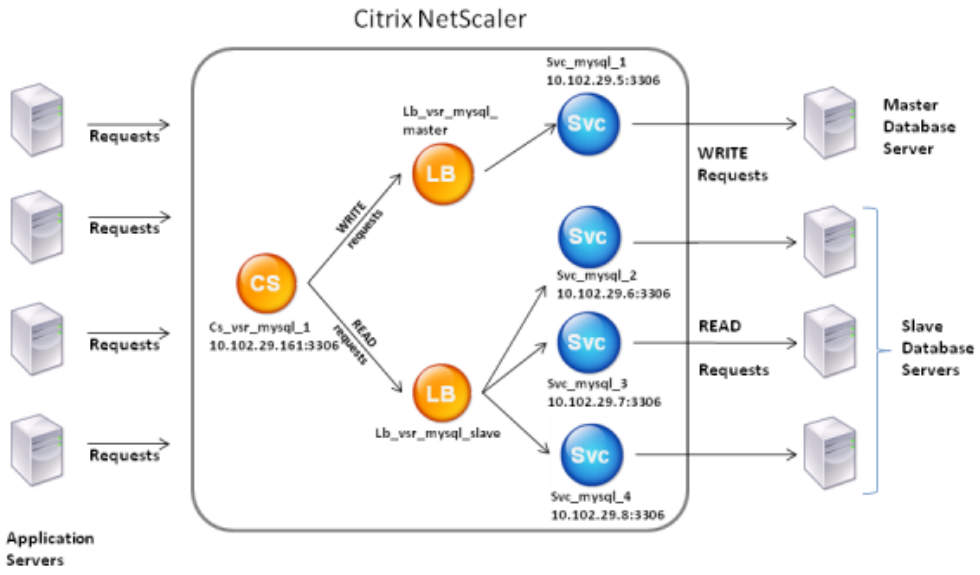


Figure 1. *DataStream Entity Model*

As shown in this figure, a DataStream configuration can consist of an optional content switching virtual server (CS), a load balancing setup consisting of load balancing virtual servers (LB1 and LB2) and services (Svc1, Svc2, Svc3, and Svc4), and content switching policies (optional).

The clients (application or Web servers) send requests to the IP address of a content switching virtual server (CS) configured on the NetScaler appliance. The NetScaler, then, authenticates the clients using the database user credentials configured on the NetScaler appliance. The content switching virtual server (CS) applies the associated content switching policies to the requests. After evaluating the policies, the content switching virtual server (CS) routes the requests to the appropriate load balancing virtual server (LB1 or LB2), which, then, distributes the requests to the appropriate database servers (represented by services on the NetScaler) based on the load balancing algorithm. The NetScaler uses the same database user credentials to authenticate the connection with the

database server.

If a content switching virtual server is *not* configured on the NetScaler, the clients (application or Web servers) send their requests to the IP address of a load balancing virtual server configured on the NetScaler appliance. The NetScaler authenticates the client by using the database user credentials configured on the NetScaler appliance, and then uses the same credentials to authenticate the connection with the database server. The load balancing virtual server distributes the requests to the database servers according to the load balancing algorithm. The most effective load balancing algorithm for database switching is the least connection method.

DataStream uses connection multiplexing to enable multiple client-side requests to be made over the same server-side connection. The following connection properties are considered:

- User name
- Database name
- Packet size
- Character set

Configuring Database Users

In databases, a connection is always stateful, which means that as soon as a connection is established, it must be authenticated.

You need to configure your database user name and password on the NetScaler ADC. For example, if you have a user John configured on the database, you need to configure the user John on the ADC too. When you add the database user names and passwords on the ADC, these are added to the nsconfig file.

Note: Names are case sensitive.

The ADC uses these user credentials to authenticate the clients, and then authenticate the server connections with the database servers.

To add a database user by using the command line interface

At the command prompt, type

add db user <username> - password <password>

Example

```
> add db user nsdbuser -password dd260427edf
```

Parameters for creating a database user

username

The database user name. This is a mandatory argument. The maximum length of the user name is 127 characters.

password

The password used to log on to the database. The maximum length of the password is 127 characters.

To add a database user by using the configuration utility

1. In the navigation pane, expand System, and then click Database Users.
2. In the details pane, click Add.
3. In the Create Database User dialog box, specify values for the following parameters.
   - User Name
   - Password
   - Confirm Password
4. Click Create, and then click Close. The user you created appears in the Database Users pane.

If you have changed the password of the database user on the database server, you must reset the password of the corresponding user configured on the NetScaler.

To reset the password of a database user by using the command line interface

At the command prompt, type

set db user <username> -password <password>

Example

```
> set db user nsdbuser -password dd260538abs
```

To reset the password of database users by using the configuration utility

1. In the navigation pane, expand System, and then click Database Users.
2. In the details pane, select the database user for which you want to reset the password, and then click Open.
3. In the Configure Database User dialog box, modify the values for the following parameters.
   - Password
   - Confirm Password
4. Click OK.

If a database user no longer exists on the database server, you can remove the user from the NetScaler. However, if the user continues to exist on the database server and you remove the user from the NetScaler, any request from the client with this user name does not get authenticated, and therefore, does not get routed to the database server.

To remove a database user by using the command line interface

At the command prompt, type

rm db user <username>

Example

```
> rm db user nsdbuser
```

To remove a database user by using the configuration utility

1. In the navigation pane, expand System, and then click Database Users.
2. In the details pane, select the database user that you want to remove, and then click Open.
3. In the Proceed message box, click Yes.

Configuring a Database Profile

A database profile is a named collection of parameters that is configured once but applied to multiple virtual servers that require those particular parameter settings. After creating a database profile, you bind it to load balancing or content switching virtual servers. You can create as many profiles as you need.

To create a database profile by using the command line interface

At the command line, type the following commands to create a database profile and verify the configuration:

- add db dbProfile <name> [-interpretQuery (YES | NO)] [-stickiness (YES | NO)] [-kcdAccount <string>]
- show db dbProfile

Example

```
> add dbProfile myDBProfile -interpretQuery YES -stickiness YES -kcdAccount mykcdaccnt
 Done
> show dbProfile myDBProfile
   Name: myDBProfile
   Interpret Query: YES
   Stickyness: YES
   KCD Account: mykcdaccnt
   Reference count: 0

 Done
>
```

Parameters for creating a database profile

name (Name)

Name for the database profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the database profile is created.

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

interpretQuery (Interpret Query)

Perform deep inspection of queries, and base load balancing decisions on the contents of queries.

stickiness (Stickiness)

Examine the query and determine whether it is associated with an earlier query. If it is, forward the query through the server connection that was used for the previous query.

kcdAccount (KCD Account)

Name of the Kerberos Constrained Delegation (KCD) account to use for authenticating users connecting to the virtual server.

To create a database profile by using the configuration utility

1. Navigate to System > Profiles.
2. In the details pane, on the Database Profiles tab, do one of the following:
   - To create a database profile, click Add.
   - To modify a database profile, click the profile, and then click Open.
3. In the Create Database Profile or Configure Database Profile dialog box, set the following parameters:
   - Name*
   - KCD Account
   - Interpret Query
   - Stickiness

   * Required parameter
4. Click Create or OK, and then click Close.

To bind a database profile to a load balancing or content switching virtual server by using the command line interface

At the command line, type:

set (lb | cs) vserver <name> -dbProfileName <string>

Parameters for binding a database profile to a load balancing or content switching virtual server

name

Name of the load balancing or content switching virtual server.

dbProfileName

Name of the database profile to bind to the virtual server.

To bind a database profile to a load balancing or content switching virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing or Content Switching, depending on the type of virtual server to which you want to bind the database profile.
2. Click Virtual Servers.
3. In the details pane, select the virtual server, and then click Open.
4. In the Configure Virtual Server (Load Balancing) or Configure Virtual Server (Content Switching) dialog box, on the Profiles tab, in the Database Profile list, select the database profile.
5. Click OK.

Configuring Load Balancing for DataStream

Before configuring a load balancing setup, you must enable the load balancing feature. Then, begin by creating at least one service for each database server in the load balancing group. With the services configured, you are ready to create a load balancing virtual server and bind the services to the virtual server.

For instructions about configuring load balancing, see Load Balancing.

Parameter values specific to DataStream

Protocol

Use the MYSQL protocol type for MySQL databases and MSSQL protocol type for MS SQL databases while configuring virtual servers and services. The MySQL and TDS protocols are used by the clients to communicate with the respective database servers by using SQL queries. For information about the MySQL protocol, see http://dev.mysql.com/doc/internals/en/client-server-protocol.html. For information about the TDS protocol, see http://msdn.microsoft.com/en-us/library/dd304523(v=prot.13).aspx.

Port

Port on which the virtual server listens for client connections. Use port 3306 for MySQL database servers.

Method

It is recommended that you use the Least Connection method for better load balancing and lower server load. However, other methods, such as Round Robin, Least Response Time, Source IP Hash, Source IP Destination IP Hash, Least Bandwidth, Least Packets, and Source IP Source Port Hash, are also supported.

Note: URL Hash method is not supported for DataStream.

MS SQL Server Version

If you are using Microsoft SQL Server, and you expect some clients to not be running the same version as your Microsoft SQL Server product, set the Server Version parameter for the load balancing virtual server. The version setting provides compatibility between the client-side and server-side connections by ensuring that all communication conforms to the server's version. For more information about setting the Server Version parameter, see Configuring the Microsoft SQL Server Version Setting.

Configuring Content Switching for DataStream

You can segment traffic according to information in the SQL query, on the basis of database names, user names, character sets, and packet size.

You can configure content switching policies with default syntax expressions to switch content based on connection properties, such as user name and database name, command parameters, and the SQL query to select the server.

The default syntax expressions evaluate traffic associated with MYSQL and MS SQL database servers. You can use request-based expressions in default syntax policies to make request switching decisions at the content switching virtual server bind point and response-based expressions (expressions that begin with MYSQL.RES) to evaluate server responses to user-configured health monitors.

Note: For information about default syntax expressions, see Default Syntax Expressions: DataStream.

Parameter values specific to DataStream

Protocol

Use the MYSQL protocol type for MySQL databases and MSSQL protocol type for MS SQL databases while configuring virtual servers and services. The MySQL and TDS protocols are used by the clients to communicate with the respective database servers by using SQL queries. For information about the MySQL protocol, see http://dev.mysql.com/doc/internals/en/client-server-protocol.html. For information about the TDS protocol, see http://msdn.microsoft.com/en-us/library/dd304523(v=prot.13).aspx.

Port

Port on which the virtual server listens for client connections. Use port 3306 for MySQL database servers.

MS SQL Server Version

If you are using Microsoft SQL Server, and you expect some clients to not be running the same version as your Microsoft SQL Server product, set the Server Version parameter for the content switching virtual server. The version setting provides compatibility between the client-side and server-side connections by ensuring that all communication conforms to the server's version. For more information about setting the Server Version parameter, see Configuring the Microsoft SQL Server Version Setting.

For instructions about configuring content switching, see "Content Switching".

Configuring Monitors for DataStream

To track the state of each load balanced database server in real time, you need to bind a monitor to each service. The monitor is configured to test the service by sending periodic probes to the service. (This is sometimes referred to as performing a health check.) If the monitor receives a timely response to its probes, it marks the service as UP. If it does not receive a timely response to the designated number of probes, it marks the service as DOWN.

For DataStream, you need to use the built-in monitors, MYSQL-ECV and MSSQL-ECV. This monitor provides the ability to send an SQL request and parse the response for a string.

Before configuring monitors for DataStream, you must add database user credentials to your NetScaler. For information about configuring monitors, see Monitors.

When you create a monitor, a TCP connection is established with the database server, and the connection is authenticated by using the user name provided while creating the monitor. You can then run an SQL query to the database server and evaluate the server response to check whether it matches the configured rule.

Parameters specific to DataStream

type

Type of monitor. Use the MYSQL-ECV monitor type for MySQL databases and MSSQL-ECV monitor type for MS SQL databases.

sqlQuery

SQL query for the MYSQL-ECV and MSSQL-ECV monitors. After the connection to the database server is authenticated, you can run this query to the server.

evalRule

Rule evaluated to determine the state of the monitor. A rule consists of default syntax expressions.

database

Name of the database that needs to be probed. During authentication, this database name is used to connect to the database.

userName

User name to connect to the database. This is looked up in the database user list to extract the database.

Examples

In the following example, the value of the error message is evaluated to determine the state of the server.

```
add lb monitor lb_mon1 MYSQL_ECV -sqlQuery "select * from
table2;" -evalrule "mysql.res.error.message.contains(\"Invalid
User\")"-database "NS" -userName "user1"
```

In the following example, the number of rows in the response is evaluated to determine the state of the server.

```
add lb monitor lb_mon4 MYSQL_ECV -sqlQuery "select * from
table4;" -evalrule "mysql.res.atleast_rows_count(7)" -database "NS" -userName "user2"
```

In the following example, the value of a particular column is evaluated to determine the state of the server.

```
add lb monitor lb_mon3 MYSQL_ECV
-sqlQuery "select * from ABC;" -evalrule "mysql.res.row(1).double_elem(2) == 345.12"
-database "NS" -userName "user3"
```

DataStream Use Cases

The following topics describe how you can configure DataStream for various scenarios.

- Configuring DataStream for a Master/Slave Database Architecture
- Configuring the Token Method of Load Balancing for DataStream

Configuring DataStream for a Master/Slave Database Architecture

A commonly used deployment scenario is the master/slave database architecture where the master database replicates all information to the slave databases.

For master/slave database architecture, you may want all WRITE requests to be sent to the master database and all READ requests to the slave databases.

The following figure shows the entities and the values of the parameters you need to configure on the appliance.

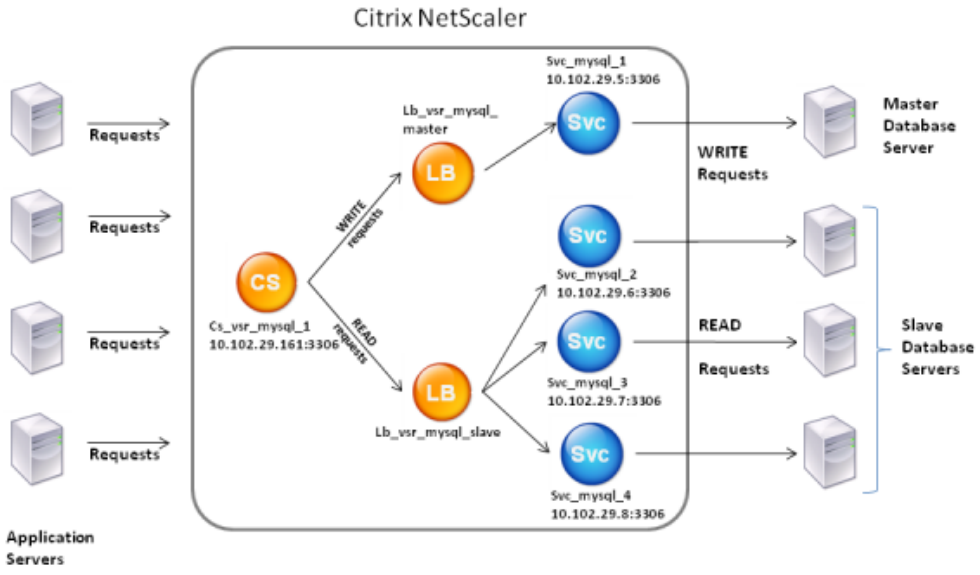


Figure 1. *DataStream Entity Model for Master/Slave Database Setup*

In this example scenario, a service (Svc_mysql_1) is created to represent the master database and is bound to a load balancing virtual server (Lb_vsr_mysql_master). Three more services (Svc_mysql_2, Svc_mysql_3, and Svc_mysql_4) are created to represent the three slave databases, and they are bound to another load balancing virtual server (Lb_vsr_mysql_slave).

A content switching virtual server (Cs_vsr_mysql_1) is configured with associated policies to send all WRITE requests to the load balancing virtual server, Lb_vsr_mysql_master, and all READ requests to the load balancing virtual server, Lb_vsr_mysql_slave.

When a request reaches the content switching virtual server, the virtual server applies the associated content switching policies to that request. After evaluating the policies, the content switching virtual server routes the request to the appropriate load balancing virtual server, which sends it to the appropriate service.

The following table lists the names and values of the entities and the policy configured on the NetScaler.

Table 1. *Entity and Policy Names and Values*

Entity Type	Name	IP Address	Protocol	Port	Expression
Services	Svc_mysql_1	10.102.29.5	MYSQL	3306	NA
	Svc_mysql_2	10.102.29.6	MYSQL	3306	NA
	Svc_mysql_3	10.102.29.7	MYSQL	3306	NA
	Svc_mysql_4	10.102.29.8	MYSQL	3306	NA
Load balancing virtual servers	Lb_vsr_mysql_master	10.102.29.201	MYSQL	3306	NA
	Lb_vsr_mysql_slave	10.102.29.202	MYSQL	3306	NA
Content switching virtual server	Cs_vsr_mysql_1	10.102.29.161	MYSQL	3306	NA
Content switching policy	Cs_select	NA	NA	NA	"MYSQL.REQ.QUERY.COMMAND.contains(\"selec

To configure DataStream for a master/slave database setup by using the command line interface

At the command prompt, type

- add service Svc_mysql_1 10.102.29.5 mysql 3306
- add service Svc_mysql_2 10.102.29.6 mysql 3306
- add service Svc_mysql_3 10.102.29.7 mysql 3306
- add service Svc_mysql_4 10.102.29.8 mysql 3306
- add lb vserver Lb_vsr_mysql_master mysql 10.102.29.201 3306
- add lb vserver Lb_vsr_mysql_slave mysql 10.102.29.202 3306
- bind lb vserver Lb_vsr_mysql_master svc_mysql_1
- bind lb vserver Lb_vsr_mysql_slave svc_mysql_2

- bind lb vserver Lb_vsr_mysql_slave svc_mysql_3
- bind lb vserver Lb_vsr_mysql_slave svc_mysql_4
- add cs vserver Cs_vsr_mysql_1 mysql 10.102.29.161 3306
- add cs policy Cs_select –rule "MYSQL.REQ.QUERY.COMMAND.contains(\"select\")"
- bind cs vserver Cs_vsr_mysql_1 Lb_vsr_mysql_master
- bind cs vserver Cs_vsr_mysql_1 Lb_vsr_mysql_slave –policy Cs_select –priority 10

To configure DataStream for a master/slave database setup by using the configuration utility

Add four services, one to represent the master database server and three to represent the slave database servers.

To add a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, specify values for the following parameters as listed in the table "Entity and Policy Names and Values".
   - Service Name
   - IP Address
   - Protocol
   - Port
4. Click Create, and then click Close. The service you created appears in the Services pane.

Add two load balancing virtual servers.

To create a load balancing virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Load Balancing) dialog box, specify values for the following parameters as listed in the table "Entity and Policy Names and Values".
   - Name
   - IP Address
   - Protocol
   - Port
4. Click Create, and then click Close.

Bind the service Svc_mysql_1 to the load balancing virtual server Lb_vsr_mysql_master, and bind the three services (Svc_mysql_2, Svc_mysql_3, and Svc_mysql_4) to the load balancing virtual server Lb_vsr_mysql_slave.

To bind a service to a load balancing virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server to which you want to bind the service (for example, Lb_vsr_mysql_master).
3. Click Open.
4. In the Configure Virtual Server (Load Balancing) dialog box, on the Services tab, select the Active check box next to the service that you want to bind to the virtual server (for example, Svc_mysql_1).
5. Click OK.

Create a content switching virtual server.

To add a content switching virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Content Switching) dialog box, specify values for the following parameters as listed in the table "Entity and Policy Names and Values."
   - Name
   - IP Address
   - Protocol
   - Port
4. Click Create, and then click Close.

Create a content switching policy to evaluate all READ requests.

To create a content switching policy by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Policies.
2. In the details pane, click Add.
3. In the Create Content Switching Policy dialog box, in the Name text box, type the name of the policy (for example, Cs_select).
4. Choose the type of policy that you want to create, and configure the policy. To create a rule-based policy, click **Configure**, and do the following:
   - In the Create Expression dialog box, choose the expression syntax you want to use and enter your policy expressions as listed in the table "Entity and Policy Names and Values."
5. Click Create, and then click Close.

Bind the content switching policy to the content switching virtual server. You should also select a load balancing virtual server as the target for the policy so that, after the content switching virtual server evaluates the policy, it routes requests that match the policy to the load balancing virtual server to forward them to the appropriate database server.

To bind the policy to the content switching virtual server and select a load balancing virtual server target by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Policies.
2. In the details pane, double-click the virtual server to which you want to bind the policy (for example, Cs_vsr_mysql_1).
3. In the Configure Virtual Server (Content Switching) dialog box, on the Policies tab, click Insert Policy, and in the Policy Name column, select the policy that you want to bind to the virtual server (for example, Cs_select).
4. In the Target column next to the policy, select the load balancing virtual server that you want to assign as the target for the policy (for example, Lb_vsr_mysql_slave).
5. Click OK.

Set the load balancing virtual server, Lb_vsr_mysql_master, as the default virtual server for the content switching virtual server by binding the content switching virtual server to this load balancing virtual server. This ensures that the content switching virtual server routes requests that do not match the Cs_select policy to the load balancing virtual server to forward them to the appropriate database server.

To bind the content switching virtual server to a load balancing virtual server by using the configuration utility

1. In the navigation pane, expand Content Switching, and then click Policies.
2. In the details pane, double-click the virtual server to which you want to bind the policy (for example, Cs_vsr_mysql_1).
3. In the Configure Virtual Server (Content Switching) dialog box, on the Policies tab, click Insert Policy, and in the Policy Name column, select (Default).
4. In the Target column next to the policy, select the load balancing virtual server that you want to assign as the target for the policy (for example, Lb_vsr_mysql_master).
5. Click OK.

Configuring the Token Method of Load Balancing for DataStream

You can configure the token method of load balancing for DataStream to base the selection of database servers on the value of the token extracted from the client (application or web server) requests. These tokens are defined by using SQL expressions. For subsequent requests with the same token, the NetScaler sends the requests to the same database server that handled the initial request. Requests with the same token are sent to the same database server until the maximum connection limit is reached or the session entry has aged out.

You can use the following sample SQL expressions to define tokens:

MySQL	MS SQL
MYSQL.REQ.QUERY.TEXT	MSSQL.REQ.QUERY.TEXT
MYSQL.REQ.QUERY.TEXT(n)	MSSQL. REQ.QUERY.TEXT(n)
MYSQL.REQ.QUERY.COMMAND	MSSQL.REQ.QUERY.COMMAND
MYSQL.CLIENT.USER	MSSQL.CLIENT.USER
MYSQL.CLIENT.DATABASE	MSSQL.CLIENT.DATABASE
MYSQL.CLIENT.CAPABILITIES	

The following example shows how the NetScaler DataStream feature works when you configure the token method of load balancing.

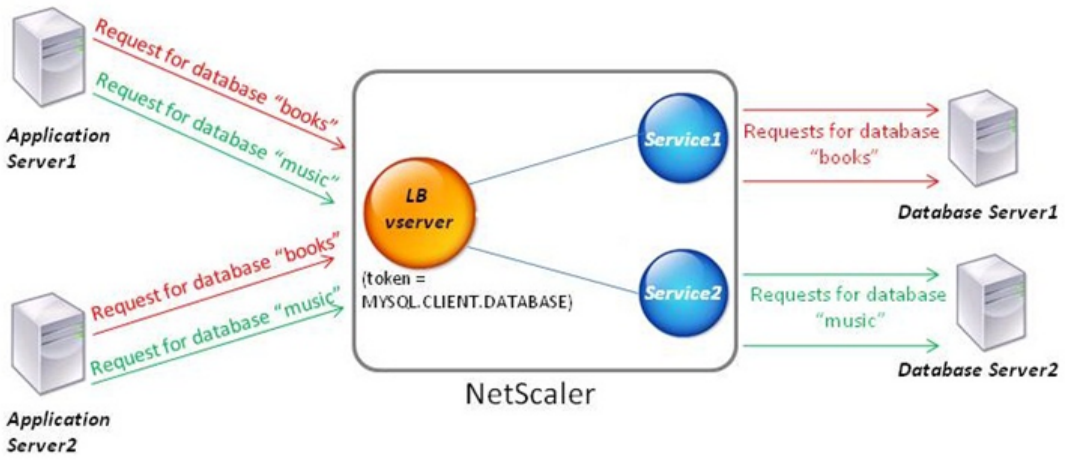


Figure 1. How DataStream Works with the Token Method of Load Balancing

In this example, the token is the name of the database. A request with token `books` is sent to `Database Server1` and a request with token `music` is sent to `Database Server2`. All subsequent requests with token `books` are sent to `Database Server1` and requests with token `music` are sent to `Database Server2`. This configuration provides pseudo

persistence with the database servers.

To configure this example by using the command line interface

At the command prompt, type:

- add service Service1 192.0.2.9 MYSQL 3306
- add service Service2 192.0.2.11 MYSQL 3306
- add lb vserver token_lb_vserver MYSQL 192.0.2.15 3306 -lbmethod token -rule MYSQL.CLIENT.DATABASE
- bind lb vserver token_lb_vserver Service1
- bind lb vserver token_lb_vserver Service2

To configure this example by using the configuration utility

1. Add two services to represent the two database servers.
    a. In the navigation pane, expand Load Balancing, and then click Services.
    b. In the details pane, click Add.
    c. In the Create Service dialog box, set the following parameters.
        - Service Name
        - IP Address
        - Protocol
        - Port
    d. Click Create, and then click Close.
2. Add one load balancing virtual server and set the token load balancing method.
    a. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
    b. In the details pane, click Add.
    c. In the Create Virtual Server (Load Balancing) dialog box, specify values for the following parameters.
        - Name
        - IP Address
        - Protocol
        - Port
    d. On the Method and Persistence tab, under LB Method, in the Method drop list, select Token.
    e. In the Rule box, type `MYSQL.CLIENT.DATABASE`.
    f. Click Create, and then click Close.

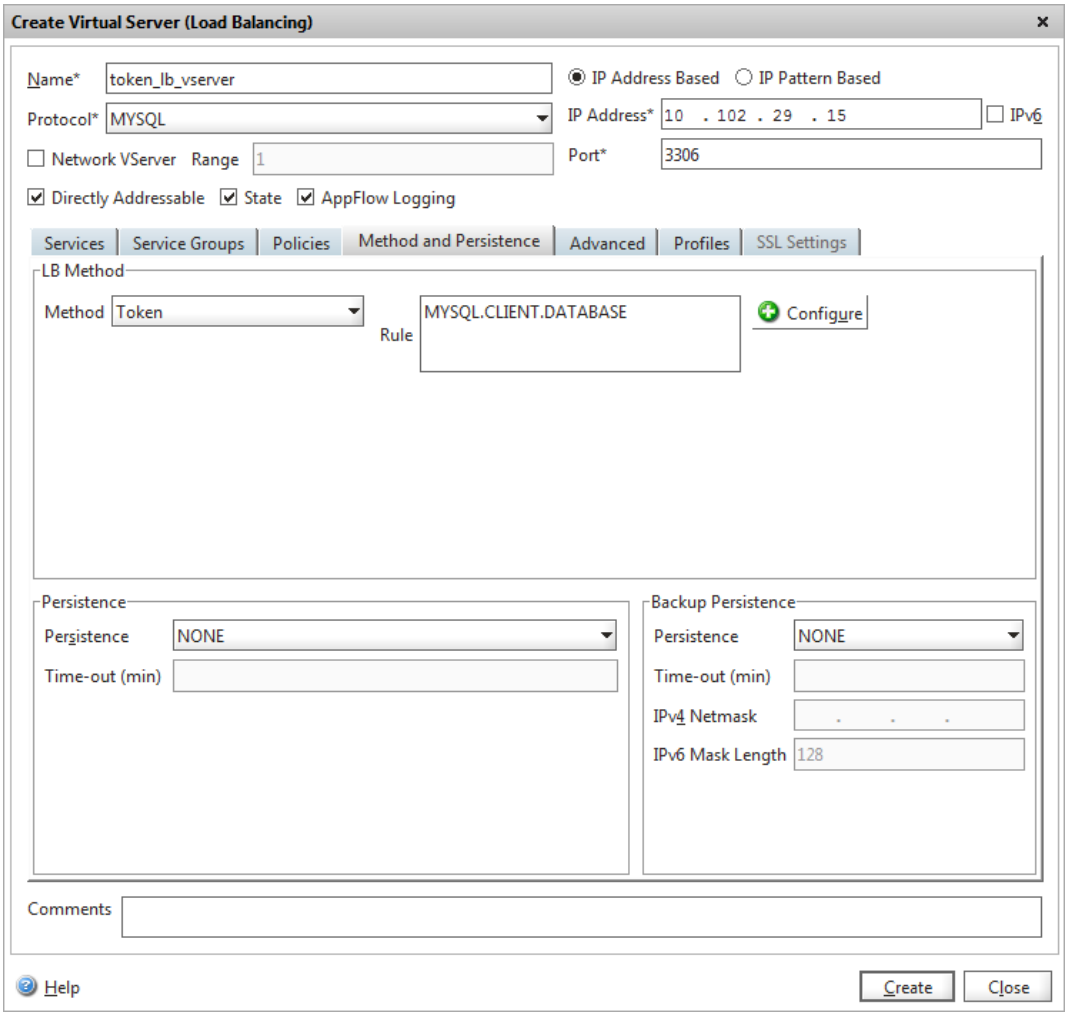


Figure 2. Configuring a Load Balancing Virtual Server by Using the Configuration Utility

3. Bind the two services to the load balancing virtual server.

   a. In the navigation pane, expand Load Balancing, and then click Virtual Servers.

   b. In the details pane, select the virtual server to which you want to bind the service (for example, token_lb_vserver).

   c. Click Open.

   d. In the Configure Virtual Server (Load Balancing) dialog box, on the Services tab, select the Active check box next to the service that you want to bind to the virtual server (for example, Service1).

   e. Click OK.

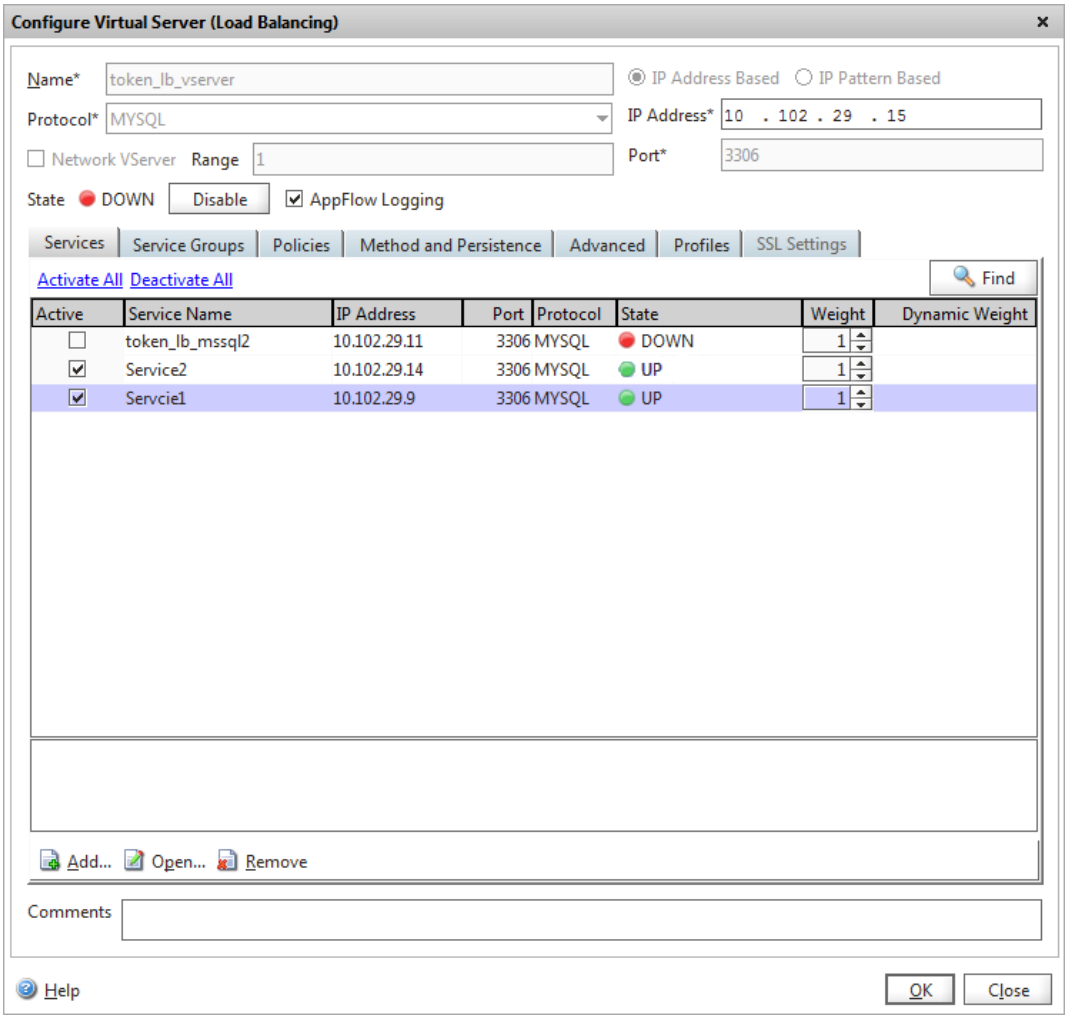


Figure 3. Binding Services to a Virtual Server by Using the Configuration Utility

DataStream Reference

This reference describes the MySQL and TDS protocols, the database versions, the authentication methods, and the character sets supported by the DataStream feature. It also describes how NetScaler handles transaction requests and special queries that modify the state of a connection.

You can also configure the NetScaler appliance to generate audit log messages for the DataStream feature.

Supported Database Versions, Protocols, and Authentication Methods

	MySQL Database	MS SQL Database
Database Versions	MySQL database versions 4.1, 5.0, 5.1, 5.4, 5.5, and 5.6.	MS SQL database versions 2000, 2000SP1, 2005, 2008, and 2008R2.
Protocols	MySQL protocol version 10. For information about the MySQL protocol, see http://dev.mysql.com/doc/internals/en/client-server-protocol.html	TDS protocol version 7.1 and higher. For information about the TDS protocol, see http://msdn.microsoft.com/en-us/library/dd304523(v=prot.13).aspx
Authentication Methods	MySQL native authentication is supported.	SQL server authentication is supported. Currently Windows authentication is not supported.

Character Sets

The DataStream feature supports only the UTF-8 charset.

The character set used by the client while sending a request may be different from the character set used in the database server responses. Although the charset parameter is set during the connection establishment, it can be changed at any time by sending an SQL query. The character set is associated with a connection, and therefore, requests on connections with one character set cannot be multiplexed onto a connection with a different character set.

NetScaler parses the queries sent by the client and the responses sent by the database server.

The character set associated with a connection can be changed after the initial handshake by using the following two queries:

- SET NAMES <charset> COLLATION <collation>
- SET CHARACTER SET <charset>

Transactions

In MySQL, transactions are identified by using the connection parameter AUTOCOMMIT or the BEGIN:COMMIT queries. The AUTOCOMMIT parameter can be set during the initial handshake, or after the connection is established by using the query SET AUTOCOMMIT.

NetScaler explicitly parses each and every query to determine the beginning and end of a transaction.

In MySQL protocol, the response contains two flags to indicate whether the connection is a transaction, the TRANSACTION and AUTOCOMMIT flags.

If the connection is a transaction, the TRANSACTION flag is set. Or, if the AutoCommit mode is OFF, the AUTOCOMMIT flag is not set. NetScaler parses the response, and if either the TRANSACTION flag is set or the AUTOCOMMIT flag is not set, it does not do connection multiplexing. When these conditions are no longer true, the NetScaler begins connection multiplexing.

Special Queries

There are special queries, such as SET and PREPARE, that modify the state of the connection and may break request switching, and therefore, these need to be handled differently.

On receiving a request with special queries, NetScaler sends an OK response to the client and additionally, stores the request in the connection.

When a non-special query, such as INSERT and SELECT, is received along with a stored query, the NetScaler first, looks for the server-side connection on which the stored query has already been sent to the database server. If no such connections exist, NetScaler creates a new connection, and sends the stored query first, and then, sends the request with the non-special query.

In case of SET, USE db, and INIT_DB special queries, the appliance modifies a field in the server side connection corresponding to the special query. This results in better reuse of the server side connection.

Only 16 queries are stored in each connection.

The following is a list of the special queries for which NetScaler has a modified behavior.

SET query

The SET SQL queries define variables that are associated with the connection. These queries are also used to define global variables, but as of now, NetScaler is unable to differentiate between local and global variables. For this query, the NetScaler uses the 'store and forward' mechanism described earlier .

USE <db> query

Using this query, the user can change the database associated with a connection. In this case, NetScaler parses the <db> value sent and modifies a field in the server side connection to reflect the new database to be used.

INIT_DB command

Using this query, the user can change the database associated with a connection. In this case, NetScaler parses the <init_db> value sent and modifies a field in the server side connection to reflect the new database to be used.

COM_PREPARE

NetScaler stops request switching on receiving this command.

PREPARE query

This query is used to create prepared statements that are associated with a connection. For this query, the NetScaler uses the 'store and forward' mechanism described earlier in this section.

Audit Log Message Support

You can now configure the NetScaler appliance to generate audit log messages for the DataStream feature. Audit log messages are generated when client-side and server-side connections are established, closed, or dropped. The categories of messages that you can log and view are ERROR and INFO. Error messages for client-side connections begin with "CS" and error messages for server-side connections begin with "SS." Additional information is provided where necessary. For example, log messages for closed connections (CS_CONN_CLOSED) include only the connection ID. However, log messages for established connections (CS_CONN_ESTD) include information such as the user name, database name, and the client IP address in addition to the connection ID.

Domain Name System

You can configure the Citrix NetScaler appliance to function as an authoritative domain name server (ADNS server) for a domain. You can add the DNS resource records that belong to the domain for which the appliance is authoritative and configure resource record parameters. You can also configure the NetScaler appliance as a proxy DNS server that load balances a farm of DNS name servers that are either within your network or outside your network. You can configure the appliance as an end resolver and forwarder. You can configure DNS suffixes that enable name resolution when fully qualified domain names are not configured. The appliance also supports the DNS ANY query that retrieves all the records that belong to a domain.

You can configure the NetScaler appliance to concurrently function as an authoritative DNS server for one domain and a DNS proxy server for another domain. When you configure the NetScaler as the authoritative DNS server or DNS proxy server for a zone, you can enable the appliance to use the Transmission Control Protocol (TCP) for response sizes that exceed the size limit specified for the User Datagram Protocol (UDP).

How DNS Works on the NetScaler

You can configure the NetScaler appliance to function as an ADNS server, DNS proxy server, end resolver, and forwarder. You can add DNS resource records on the NetScaler, including service (SRV) records, IPv6 (AAAA) records, address (A) records, mail exchange (MX) records, canonical name (CNAME) records, pointer (PTR) records, start of authority (SOA) records, and text (TXT) records. Also, you can configure the NetScaler to load balance external DNS name servers.

The NetScaler can be configured as the authority for a domain. To do this, you add valid SOA and NS records for the domain.

An ADNS server is a DNS server that contains complete information about a zone.

To configure the NetScaler as an ADNS server for a zone, you must add an ADNS service, and then configure the zone. To do so, you add valid SOA and NS records for the domain. When a client sends a DNS request, the NetScaler appliance searches the configured resource records for the domain name. You can configure the ADNS service to be used with the NetScaler Global Server Load Balancing (GSLB) feature.

You can delegate a subdomain, by adding NS records for the subdomain to the zone of the parent domain. You can then make the NetScaler authoritative for the subdomain, by adding a "glue record" for each of the subdomain name servers. If GSLB is configured, the NetScaler makes a GSLB load balancing decision based on its configuration and replies with the IP address of the selected virtual server. The following figure shows the entities in an ADNS GSLB setup and a DNS proxy setup.

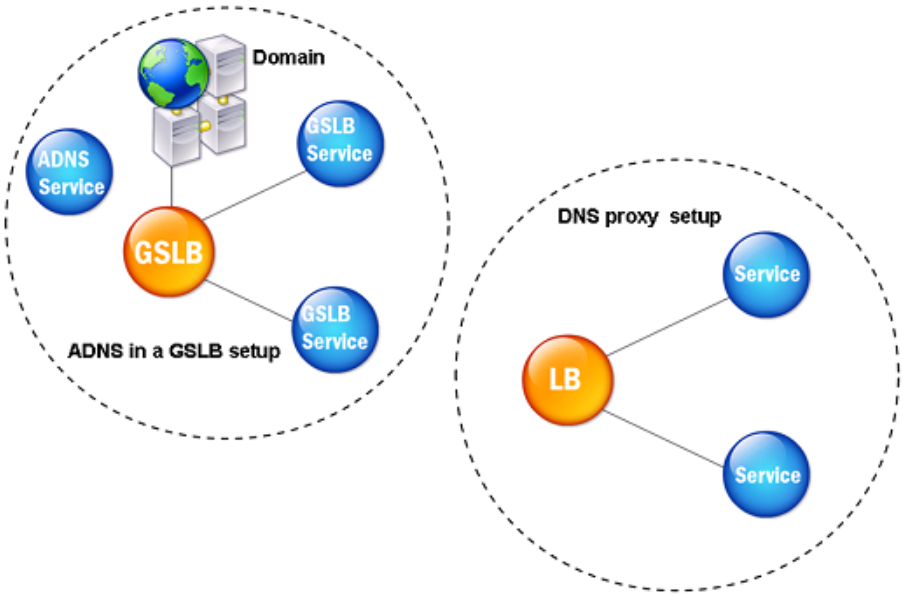


Figure 1. DNS Proxy Entity Model

The NetScaler appliance can function as a DNS proxy. Caching of DNS records, which is an important function of a DNS proxy, is enabled by default on the NetScaler appliance. This enables the NetScaler to provide quick responses for repeated translations. You must also create a load balancing DNS virtual server, and DNS services, and then bind these services to the virtual server.

The NetScaler provides two options, minimum time to live (TTL) and maximum TTL for configuring the lifetime of the cached data. The cached data times out as specified by your settings for these two options. The NetScaler checks the TTL of the DNS record coming from the server. If the TTL is less than the configured minimum TTL, it is replaced with the configured minimum TTL. If the TTL is greater than the configured maximum TTL, it is replaced with the configured maximum TTL.

The NetScaler also allows caching of negative responses for a domain. A negative response indicates that information about a requested domain does not exist, or that the server cannot provide an answer for the query. The storage of this information is called *negative caching*. Negative caching helps speed up responses to queries on a domain, and can optionally provide the record type.

A negative response can be one of the following:

- NXDOMAIN error message - If a negative response is present in the local cache, the NetScaler returns an error message (NXDOMAIN). If the response is not in the local cache, the query is forwarded to the server, and the server returns an NXDOMAIN error to the NetScaler. The NetScaler caches the response locally, then returns the error message to the client.

- NODATA error message - The NetScaler sends a NODATA error message, if the domain name in query is valid but records of the given type are not available.

The NetScaler supports recursive resolution of DNS requests. In recursive resolution, the resolver (DNS client) sends a recursive query to a name server for a domain name. If the queried name server is authoritative for the domain, it responds with the requested domain name. Otherwise, the NetScaler queries the name servers recursively until the requested domain name is found.

Before you can apply the recursive query option, you must first enable it. You can also set the number of times the DNS resolver must send a resolution request (DNS retries) if a DNS lookup fails.

You can configure the NetScaler as a DNS forwarder. A forwarder passes DNS requests to external name servers. The NetScaler allows you to add external name servers and provides name resolution for domains outside the network. The NetScaler also allows you to set the name lookup priority to DNS or Windows Internet Name Service (WINS).

Round Robin DNS

When a client sends a DNS request to find the DNS resource record, it receives a list of IP addresses resolving to the name in the DNS request. The client then uses one of the IP addresses in the list, generally, the first record or IP address. Hence, a single server is used for the total TTL of the cache and is overloaded when a large number of requests arrive.

When the NetScaler receives a DNS request, it responds by changing the order of the list of DNS resource records in a round robin method. This feature is called *round robin DNS*. Round robin distributes the traffic equally between data centers. The NetScaler performs this function automatically. You do not have to configure this behavior.

Functional Overview

If the NetScaler is configured as an ADNS server, it returns the DNS records in the order in which the records are configured. If the NetScaler is configured as a DNS proxy, it returns the DNS records in the order in which it receives the records from the server. The order of the records present in the cache matches the order in which records are received from the server.

The NetScaler then changes the order in which records are sent in the DNS response in a round robin method. The first response contains the first record in sequence, the second response contains the second record in sequence, the third response contains the third record in sequence, and the order continues in the same sequence. Thus, clients requesting the same name can connect to different IP addresses.

Round Robin DNS Example

As an example of round robin DNS, consider DNS records that have been added as follows:

```
add dns addRec ns1 1.1.1.1
add dns addRec ns1 1.1.1.2
add dns addRec ns1 1.1.1.3
add dns addRec ns1 1.1.1.4
```

The domain, abc.com is linked to an NS record as follows:

```
add dns nsrec abc.com. ns1
```

When the NetScaler receives a query for the A record of ns1, the Address records are served in a round robin method as follows. In the first DNS response, 1.1.1.1 is served as the first record:

```
ns1.            1H IN A      1.1.1.1
```

```
ns1.        1H IN A     1.1.1.2
ns1.        1H IN A     1.1.1.3
ns1.        1H IN A     1.1.1.4
```

In the second DNS response, the second IP address, 1.1.1.2 is served as the first record:

```
ns1.        1H IN A     1.1.1.2
ns1.        1H IN A     1.1.1.3
ns1.        1H IN A     1.1.1.4
ns1.        1H IN A     1.1.1.1
```

In the third DNS response, the third IP address, 1.1.1.2 is served as the first record:

```
ns1.        1H IN A     1.1.1.3
ns1.        1H IN A     1.1.1.4
ns1.        1H IN A     1.1.1.1
ns1.        1H IN A     1.1.1.2
```

Configuring DNS Resource Records

You configure resource records on the Citrix® NetScaler® appliance when you configure the appliance as an ADNS server for a zone. You can also configure resource records on the appliance if the resource records belong to a zone for which the appliance is a DNS proxy server. On the appliance, you can configure the following record types:

- Service records
- AAAA records
- Address records
- Mail Exchange records
- Name Server records
- Canonical records
- Pointer records
- NAPTR records
- Start of Authority records
- Text records

The following table lists the record types and the number of records (per record type) that you can configure for a domain on the NetScaler.

Table 1. Record Type and Number Configurable

Record Type	Number of Records
Address (A)	25
IPv6 (AAAA)	5
Mail exchange (MX)	12
Name server (NS)	16
Service (SRV)	8
Pointer (PTR)	20
Canonical name (CNAME)	1
Start of Authority (SOA)	1
Text (TXT)	20
Naming Authority Pointer (NAPTR)	20

Creating SRV Records for a Service

The SRV record provides information about the services available on the NetScaler appliance. An SRV record contains the following information: name of the service and the protocol, domain name, TTL, DNS class, priority of the target, weight of records with the same priority, port of the service, and host name of the service. The NetScaler chooses the SRV record that has the lowest priority setting first. If a service has multiple SRV records with the same priority, clients use the weight field to determine which host to use.

To add an SRV record by using the command line interface

At the command prompt, type the following commands to add an SRV record and verify the configuration:

- add dns srvRec <domain> <target> -priority <positive_integer> -weight <positive_integer> -port <positive_integer> [-TTL <secs>]
- sh dns srvRec <domain>

Example

```
> add dns srvRec _http._tcp.example.com nameserver1.com -priority 1 -weight 1 -port 80
 Done
> show dns srvRec _http._tcp.example.com
1)      Domain Name : _http._tcp.example.com
        Target Host : nameserver1.com
        Priority : 1    Weight : 1
        Port : 80       TTL : 3600 secs
 Done
>
```

To modify or remove an SRV record by using the command line interface

- To modify an SRV record, type the set dns srvRec command, the name of the domain for which the SRV record is configured, the name of the target host that hosts the associated service, and the parameters to be changed, with their new values.
- To remove an SRV record, type the rm dns srvRec command, the name of the domain for which the SRV record is configured, and the name of the target host that hosts the associated service.

Parameters for configuring an SRV record

domain

The domain name that is offering the services. The domain name includes the service offered and the transport layer protocol (for example, `_ftp._tcp.abc.com`). This is a mandatory argument. Maximum length: 255.

target

The host for the specified service. This is a mandatory argument. Maximum length: 255.

priority

The priority that is assigned to the target host. The lower the priority value, the higher the priority. Clients always attempt to use the SRV record that has the lowest priority value. This is a mandatory argument. Minimum value: 0. Maximum value: 65535.

weight

Weight for the target host. If two records have the same priority, the NetScaler selects the server based on the value of this parameter. This is a mandatory argument. Minimum value: 0. Maximum value: 65535.

port

The port name on which the target host is listening for client requests. This is a mandatory argument. Minimum value: 0. Maximum value: 65535.

TTL

The time to live, measured in seconds. Minimum value: 0. Maximum value: 2147483647. Default: 3600.

To configure an SRV record by using the configuration utility

1. In the navigation pane, expand DNS, expand Records, and then click SRV Records.
2. In the details pane, do one of the following:
   - To create a new SRV record, click Add.
   - To modify an existing SRV record, select the SRV record, and then click Open.
3. In the Create SRV Record or Configure SRV Record dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring an SRV record” as shown:
   - Domain Name*—domain (cannot be changed for an existing SRV record)
   - Target*—target (cannot be changed for an existing SRV record)
   - Priority*—priority
   - Weight*—weight
   - Port*—port
   - TTL—TTL

   * A required parameter
4. Click Create or OK.

Creating AAAA Records for a Domain Name

An AAAA resource record stores a single IPv6 address.

To add an AAAA record by using the command line interface

At the command prompt, type the following commands to add an AAAA record and verify the configuration:

- add dns aaaaRec <hostName> <IPv6Address> ... [-TTL <secs>]
- show dns aaaaRec <hostName>

Example

```
> add dns aaaaRec www.example.com 2001:0db8:0000:0000:0000:0000:1428:57ab
 Done
> show dns aaaaRec www.example.com
1)      Host Name : www.example.com
       Record Type : ADNS            TTL : 5 secs
       IPV6 Address : 2001:db8::1428:57ab
 Done
>
```

To remove an AAAA record and all of the IPv6 addresses associated with the domain name, type the rm dns aaaaRec command and the domain name for which the AAAA record is configured. To remove only a subset of the IPv6 addresses associated with the domain name in an AAAA record, type the rm dns aaaaRec command, the domain name for which the AAAA record is configured, and the IPv6 addresses that you want to remove.

Parameters for configuring an AAAA record

hostName

The domain name for which the Address record is added. This is a mandatory argument. Maximum length: 255.

IPv6Address

The IPv6 address of the domain name.

TTL

The time to live, measured in seconds. Minimum value: 0. Maximum value: 2147483647. Default: 3600.

To add an AAAA record by using the configuration utility

1. In the navigation pane, expand DNS, expand Records, and then click AAAA Records.
2. In the details pane, click Add.
3. In the Create AAAA Record dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring an AAAA record” as shown:
   - Host Name*—hostName
   - IPv6 Address*—IPv6Address
   - TTL-TTL

   * A required parameter
4. Click Add. The IPv6 address appears in the IP box.
5. Click Create, and then click Close.

Creating Address Records for a Domain Name

Address (A) records are DNS records that map a domain name to an IPv4 address.

You cannot delete Address records for a host participating in global server load balancing (GSLB). However, the NetScaler deletes Address records added for GSLB domains when you unbind the domain from a GSLB virtual server. Only user-configured records can be deleted manually. You cannot delete a record for a host referenced by records such as NS, MX, or CNAME.

To add an Address record by using the command line interface

At the command prompt, type the following commands to add an Address record and verify the configuration:

- add dns addRec <hostName> <IPAddress> [-TTL <secs>]
- show dns addRec <hostName>

Example

```
> add dns addRec ns.example.com 192.0.2.0
 Done
> show dns addRec ns.example.com
1)      Host Name : ns.example.com
       Record Type : ADNS                  TTL : 5 secs
       IP Address : 192.0.2.0
 Done
>
```

To remove an Address record and all of the IP addresses associated with the domain name, type the rm dns addRec command and the domain name for which the Address record is configured. To remove only a subset of the IP addresses associated with the domain name in an Address record, type the rm dns addRec command, the domain name for which the Address record is configured, and the IP addresses that you want to remove.

Parameters for configuring an Address record

hostName

The domain name for which the Address record is being added. This is a mandatory argument. Maximum length: 255.

IPAddress

The IP address of the domain name.

TTL

The time to live, measured in seconds. Minimum value: 0. Maximum value: 2147483647. Default: 3600.

To add an Address record by using the configuration utility

1. In the navigation pane, expand DNS, expand Records, and then click Address Records.
2. In the details pane, click Add.
3. In the Create Address Record dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring Address records” as shown:
   - Host Name*—hostName
   - IP Address*—IPAddress
   - TTL—TTL

   * A required parameter
4. Click Add. The IP address appears in the IP Address box.
5. Click Create, and then click Close.

Creating MX Records for a Mail Exchange Server

Mail Exchange (MX) records are used to direct email messages across the Internet. An MX record contains an MX preference that specifies the MX server to be used. The MX preference values range from 0 through 65536. An MX record contains a unique MX preference number. You can set the MX preference and the TTL values for an MX record.

When an email message is sent through the Internet, a mail transfer agent sends a DNS query requesting the MX record for the domain name. This query returns a list of host names of mail exchange servers for the domain, along with a preference number. If there are no MX records, the request is made for the Address record of that domain. A single domain can have multiple mail exchange servers.

To add an MX record by using the command line interface

At the command prompt, type the following commands to add an MX record and verify the configuration:

- add dns mxRec <domain> -mx <string> -pref <positive_integer> [-TTL <secs>]
- show dns mxRec <domain>

Example

```
> add dns mxRec example.com -mx mail.example.com -pref 1
 Done
> show dns mxRec example.com
1)      Domain : example.com    MX Name : mail.example.com
        Preference :   1        TTL : 5 secs
 Done
>
```

To modify or remove an MX record by using the command line interface

- To modify an MX record, type the set dns mxRec command, the name of the domain for which the MX record is configured, the name of the MX record, and the parameters to be changed, with their new values.
- To set the TTL parameter to its default value, type the unset dns mxRec command, the name of the domain for which the MX record is configured, the name of the MX record, and `-TTL` without any TTL value. You can use the unset dns mxRec command to unset only the TTL parameter.
- To remove an MX record, type the rm dns mxRec command, the name of the domain for which the MX record is configured, and the name of the MX record.

Parameters for configuring an MX record

domain

The domain for which the MX record is added. This is a mandatory argument. Maximum length: 255.

mx

The MX record name. This is a mandatory argument. Maximum length: 255.

pref

The route priority number. This is a mandatory argument. Minimum value: 0. Maximum value: 65535.

Note: A domain name can have multiple mail routes, with a priority number assigned to each. The mail route with the lowest number identifies the server responsible for the domain. Other listed mail servers are used as backups.

TTL

The time to live, in seconds. Minimum value: 0. Maximum value: 2147483647. Default: 3600.

To add an MX record by using the configuration utility

1. In the navigation pane, expand DNS, expand Records, and then click Mail Exchange Records.

2. In the details pane, do one of the following:

   - To create a new MX record, click Add.

   - To modify an existing MX record, select the MX record, and then click Open.

3. In the Create Mail Exchange Record or Configure Mail Exchange Record dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring an MX record” as shown:

   - Domain Name*—domain (cannot be changed for an existing MX record)

   - Mail Exchange*—mx (cannot be changed for an existing MX record)

   - Preference No.*—pref

   - TTL—TTL

   * A required parameter

4. Click Create or OK.

Creating NS Records for an Authoritative Server

Name Server (NS) records specify the authoritative server for a domain. You can configure a maximum of 16 NS records. You can use an NS record to delegate the control of a subdomain to a DNS server.

To create an NS record by using the command line interface

At the command prompt, type the following commands to create an NS record and verify the configuration:

- add dns nsRec <domain> <nameServer> [-TTL <secs>]
- show dns nsRec <domain>

Example

```
> add dns nsRec example.com nameserver1.example.com
 Done
> show dns nsRec example.com
1)      Domain : example.com    NameServer : nameserver1.example.com
       TTL : 5 sec
 Done
>
```

To remove an NS record, type the rm dns nsRec command, the name of the domain to which the NS record belongs, and the name of the name server.

Parameters for configuring an NS record

domain

The domain name for which the name server record is being added.

nameServer

The name server for the domain.

TTL

The time to live, measured in seconds. Minimum value: 0. Maximum value: 2147483647. Default: 3600.

To create an NS record by using the configuration utility

1. In the navigation pane, expand DNS, expand Records, and then click Name Server Records.

2. In the details pane, click Add.

3. In the Create Name Server Record dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring an NS record” as shown:

   - Domain Name*—domain

   - Name Server*—nameServer

   - TTL—TTL

   * A required parameter

4. Click Create, and then click Close.

Creating CNAME Records for a Subdomain

A canonical name record (CNAME record) is an alias for a DNS name. These records are useful when multiple services query the DNS server. The host that has an address (A) record cannot have a CNAME record.

To add a CNAME record by using the command line interface

At the command prompt, type the following commands to create a CNAME record and verify the configuration:

- add dns cnameRec <aliasName> <canonicalName> [-TTL <secs>]
- show dns cnameRec <aliasName>

Example

```
> add dns cnameRec www.example.com www.examplenw.com
 Done
> show dns cnameRec www.example.com
        Alias Name      Canonical Name  TTL
1)      www.example.com         www.examplenw.com       5 secs
 Done
>
```

To remove a CNAME record for a given domain, type the rm dns cnameRec command and the alias of the domain name.

Parameters for configuring a CNAME record

aliasName

Domain name for the defined alias. Maximum length: 256.

canonicalName

Alias name for the specified domain. Maximum length: 256.

TTL

The time to live, measured in seconds. Minimum value: 0. Maximum value: 2147483647. Default: 3600.

To add a CNAME record by using the configuration utility

1. In the navigation pane, expand DNS, expand Records, and then click Canonical Records.
2. In the details pane, click Add.
3. In the Create Canonical Name Record dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a CNAME record” as shown:
   - Alias Name*—aliasName
   - Canonical Name*—canonicalName
   - TTL—TTL

   * A required parameter
4. Click Create, and then click Close.

Caching CNAME Record

NetScaler ADC when deployed in a proxy mode does not always send the query for an address record to the back-end server. This happens when for a answer to a query for an address record, a partial CNAME chain is present in the cache. There are few conditions in which the ADC caches the partial CNAME record and serves the query from the cache. Following are the conditions:

- NetScaler should be deployed in a proxy mode
- The response from the back-end server should have a CNAME chain, for which the record type of last entry in the answer section must be a CNAME and the question type not a CNAME
- The response from the back-end server cannot be a No-data or NX-Domain
- The response from the back-end server has to be a authoritative response

Creating NAPTR Records for Telecommunications Domain

NAPTR (Naming Address Pointer) is one of the most commonly used DNS record in telecommunications domain. NAPTR records map the Internet telephony address space to the Internet address space. They therefore enable a mobile device to send a request to the correct server. The combination of NAPTR records with Service Records (SRV) allows the chaining of multiple records to form complex rewrite rules that produce new domain labels or uniform resource identifiers (URIs). The DNS code for NAPTR is 35.

NetScaler ADCs support NAPTR in two modes: ADNS mode and proxy mode. In proxy mode, the ADC caches the response from the servers and uses the cached records to server future queries. A maximum of 20 NAPTR records can be added for a particular domain in NetScaler. NetScaler caches the reply to a DNS NAPTR record query. Any subsequent requests for the NAPTR record is served from the cache.

To create a NAPTR record by using command line interface

At the command prompt, type the following commands to add a NAPTR record and verify the configuration:

add dns naptrRec <order> <preference>[flags<string>][services<string>](regexp<expressions>|-replacement<string>)[-TTL<secs>]

To remove a NAPTR record by using command line interface

rm dns naptrRec<domain> (<order> <preference> [-flags <string>] [-services <string>] (-regexp <expression> | -replacement <string>)) | -recordId <positive_integer>@)

To configure a NAPTR record using configuration utility

1. In the navigation pane, expand DNS, expand Records, and then click NAPTR Records.
2. In the Create NAPTR Record dialog box, set the following parameters:
   - Domain—Name of the domain for the NAPTR record. Maximum length: 255 characters.
   - Order—Integer specifying the order in which the NAPTR records must be processed in order to accurately represent the ordered list of rules. The ordering is from lowest to highest. Maximum value: 65535.
   - Preference— Integer specifying the preference of this NAPTR among NAPTR records. Maximum value: 65535.
   - Flags— Flags for this NAPTR record. Maximum length: 255 characters.
   - Regular Expression—Regular expression that specifies the substitution expression for this NAPTR. Maximum length: 255 characters.
   - Replacement—The replacement domain name for this NAPTR record. Maximum length: 255 characters.
   - TTL— Time to Live (TTL), in seconds, for the record.
3. Click Create, and then click Close.

Creating PTR Records for IPv4 and IPv6 Address

A pointer (PTR) record translates an IP address to its domain name. IPv4 PTR records are represented by the octets of an IP address in reverse order with the string "in-addr.arpa." appended at the end. For example, the PTR record for the IP address 1.2.3.4 is 4.3.2.1.in-addr.arpa.

IPv6 addresses are reverse mapped under the domain IP6.ARPA. IPv6 reverse-maps use a sequence of nibbles separated by dots with the suffix ".IP6.ARPA" as defined in RFC 3596. For example, the reverse lookup domain name corresponding to the address, 4321:0:1:2:3:4:567:89ab would be b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.ARPA.

To add a PTR record by using the command line interface

At the command prompt, type the following commands to add a PTR record and verify the configuration:

- add dns ptrRec <reverseDomain> <domain> [-TTL <secs>]
- show dns ptrRec <reverseDomain>

Example

```
> add dns ptrRec 0.2.0.192.in-addr.arpa example.com
 Done
> show dns ptrRec 0.2.0.192.in-addr.arpa
1)      Reverse Domain Name : 0.2.0.192.in-addr.arpa
        Domain Name : example.com               TTL : 3600 secs
 Done
>
```

To remove a PTR record, type the rm dns ptrRec command and the reverse domain name associated with the PTR record

Parameters for configuring a PTR record

reverseDomain

Reversed representation of the domain name that the PTR record must point to. Possible suffix values are in-addr.arpa. for IPv4 addresses and ip6.arpa. for IPv6 addresses. This is

a mandatory argument. Maximum length: 75.

domain

The domain name for which reverse mapping is being done. This is a mandatory argument. Maximum length: 255.

TTL

The time to live, measured in seconds. Minimum value: 0. Maximum value: 2147483647. Default: 3600.

To add a PTR record by using the configuration utility

1. In the navigation pane, expand DNS, expand Records, and then click PTR Records.
2. In the details pane, click Add.
3. In the Create PTR Record dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a PTR record” as shown:
   - Choose suffix*—(Select .in-addr.arpa. to specify a PTR record for an IPv4 address or .ip6.arpa. to specify a PTR record for an IPv6 address. The string that you select is appended to the reversed IP address to form the reverse domain name.)
   - IP Address*—(The IP address of the domain name. The Reverse Domain Name box displays the reverse domain name that is generated when you are entering the IP address. After you enter the IP address, verify that the reverse domain name is correct.)
   - Domain*—domain
   - TTL—TTL

   * A required parameter
4. Click Add.

   The domain name appears in the Domain list. Add as many domain names as you want to the Domain list.
5. Click Create, and then click Close.

Creating SOA Records for Authoritative Information

A Start of Authority (SOA) record is created only at the zone apex and contains information about the zone. The record includes, among other parameters, the primary name server, contact information (e-mail), and default (minimum) time-to-live (TTL) values for records.

To create an SOA record by using the command line interface

At the command prompt, type the following commands to add an SOA record and verify the configuration:

- add dns soaRec <domain> -originServer <originServerName> -contact <contactName>
- sh dns soaRec <do main>

Example

```
> add dns soaRec example.com -originServer nameserver1.example.com -contact admin.example.com
 Done
> show dns soaRec example.com
1)      Domain Name : example.com
        Origin Server : nameserver1.example.com
        Contact : admin.example.com
        Serial No. : 100        Refresh : 3600 secs     Retry : 3 secs
        Expire : 3600 secs      Minimum : 5 secs        TTL : 3600 secs
 Done
>
```

To modify or remove an SOA record by using the command line interface

- To modify an SOA record, type the set dns soaRec command, the name of the domain for which the record is configured, and the parameters to be changed, with their new values.
- To remove an SOA record, type the rm dns soaRec command and the name of the domain for which the record is configured.

Parameters for configuring an SOA record

domain

Domain name for which the SOA record is added.

originServer

Name of the origin server for the given domain.

contact

Contact person for this ADNS server. This is typically an e-mail address in which the at sign (@) is replaced by a period (.).

To configure an SOA record by using the configuration utility

1. In the navigation pane, expand DNS, expand Records, and then click SOA Records.
2. In the details pane, do one of the following:
   - To create an SOA record, click Add.
   - To configure an existing SOA record, select the SOA record, and then click Open.
3. In the Create SOA Record or Configure SOA Record dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring an SOA record” as shown:
   - Domain Name*—domain
   - Origin Server*—originServer
   - Contact*—contact

   * A required parameter
4. Click Create, and then click Close.

Creating TXT Records for Holding Descriptive Text

Domain hosts store TXT records for informative purposes. A TXT record's RDATA component, which consists of one or more character strings of variable length, can store practically any information that a recipient might need to know about the domain, including information about the service provider, contact person, email addresses, and associated details. SPF (Sender Policy Framework) protection has been the most prominent use case for the TXT record.

All configuration types (authoritative DNS, DNS proxy, end resolver, and forwarder configurations) on the NetScaler appliance support TXT records. You can add a maximum of 20 TXT resource records to a domain. Each resource record is stored with a unique, internally generated record ID. You can view the ID of a record and use it to delete the record. However, you cannot modify a TXT resource record.

To create a TXT resource record by using the command line interface

At the command prompt, type the following commands to create a TXT resource record and verify the configuration:

- add dns txtRec <domain> <string> ... [-TTL <secs>]
- show dns txtRec [<domain> | -type <type>]

Example

```
> add dns txtRec www.example.com "Contact: Mark" "Email: mark@example.com" -TTL 36000
 Done
> show dns txtRec www.example.com
1)  Domain : www.example.com    Record id: 13783      TTL : 36000 secs Record Type : ADNS
       "Contact: Mark"
       "Email: mark@example.com"
 Done
```

To remove a TXT resource record by using the command line interface

At the command prompt, type the following commands to remove a TXT resource record and verify the configuration:

- rm dns txtRec <domain> (<string> ... | -recordId <positive_integer>)
- show dns txtRec [<domain> | -type <type>]

Example

You can use the show dns txtRec command first to view the record ID of the TXT resource record that you want to remove, as shown:

```
> show dns txtRec www.example.com
1)  Domain : www.example.com    Record id: 36865      TTL : 36000 secs Record Type : ADNS
       "Contact: Evan"
       "Email: evan@example.com"
2)  Domain : www.example.com    Record id: 14373      TTL : 36000 secs Record Type : ADNS
       "Contact: Mark"
       "Email: mark1@example.com"
 Done
```

The simpler method of deleting a TXT record is to use the record ID. If you want to provide the strings, enter them in the order in which they are stored in the record. In the following example, the TXT record is deleted by using its record ID.

```
>rm dns txtRec www.example.com -recordID 36865
 Done
> show dns txtRec www.example.com
1)  Domain : www.example.com    Record id: 14373      TTL : 36000 secs Record Type : ADNS
       "Contact: Mark"
       "Email: mark1@example.com"
 Done
```

Parameters for configuring a TXT resource record

domain (Domain)

The name of the domain for which you want to create a TXT resource record. Maximum length: 255 characters.

string (Text)

The information that you want stored in the TXT resource record. Enclose the string in single or double quotation marks. You can add up to six strings in each TXT resource record. Each string can contain a maximum of 255 characters. If the string that you want to add contains more than 255 characters, evaluate whether breaking down the string into two or more smaller strings, subject to the limit of six strings per resource record, works for you.

TTL

The record's time to live, in seconds. Minimum value: 0. Maximum value: 2147483647. Default: 3600.

To configure a TXT record by using the configuration utility

1. In the navigation pane, expand DNS, expand Records, and then click TXT Records.
2. In the Create TXT Record dialog box, set the following parameters:
   - Domain
   - Text

     (Enter the string in Text, and then click Add. Repeat until you have added the strings you want. If you want to remove a string that you have added, click the cross next to the string.)
   - TTL (seconds)
3. Click Create.
4. In the details pane, verify that the details displayed for the TXT record are correct.

Viewing DNS Statistics

You can view the DNS statistics generated by the Citrix® NetScaler® appliance. The DNS statistics include runtime, configuration, and error statistics.

To view DNS records statistics by using the command line interface

At the command prompt, type:

stat dns

Example

```
> stat dns
DNS Statistics

Runtime Statistics
Dns queries                    21
NS queries                      8
SOA queries                    18
.
.
.
Configuration Statistics
AAAA records                   17
A records                      36
MX records                      9
.
.
.
Error Statistics
Nonexistent domain             17
No AAAA records                 0
No A records                   13
.
.
.
Done
>
```

To view DNS records statistics by using the configuration utility

1. Navigate to Traffic Management > DNS.
2. In the navigation pane, click DNS.
3. In the details pane, click Statistics.

Configuring a DNS Zone

A DNS zone entity on the Citrix® NetScaler® appliance facilitates the ownership of a domain on the appliance. A zone on the appliance also enables you to implement DNS Security Extensions (DNSSEC) for the zone. DNSSEC sign operations are performed on all the resource records in a DNS zone. Therefore, if you want to sign a zone, or if you want to offload DNSSEC operations for a zone, you must first create the zone on the NetScaler appliance.

You must create a DNS zone on the appliance in the following scenarios:

- The NetScaler appliance owns all the records in a zone, that is, the appliance is operating as the authoritative DNS server for the zone. The zone must be created with the proxyMode parameter set to NO.
- The NetScaler appliance owns only a subset of the records in a zone, and all the other resource records in the zone are hosted on a set of back-end name servers for which the appliance is configured as a DNS proxy server. A typical configuration where the NetScaler appliance owns only a subset of the resource records in the zone is a global server load balancing (GSLB) configuration. Only the GSLB domain names are owned by the NetScaler appliance, while all the other records are owned by the back-end name servers. The zone must be created with the proxyMode parameter set to YES.

If the NetScaler appliance does not host any of the resource records in a zone, you need not create a zone on the appliance.

Note: If the NetScaler is operating as the authoritative DNS server for a zone, you must create Start of Authority (SOA) and name server (NS) records for the zone before you create the zone. If the NetScaler is operating as the DNS proxy server for a zone, SOA and NS records must not be created on the NetScaler appliance. For more information about creating SOA and NS records, see Configuring DNS Resource Records.

When you create a zone, all existing domain names and resource records that end with the name of the zone are automatically treated as a part of the zone. Additionally, any new resource records created with a suffix that matches the name of the zone are implicitly included in the zone.

To create a DNS zone on the NetScaler appliance by using the command line interface

At the command prompt, type the following command to add a DNS zone to the NetScaler appliance and verify the configuration:

- add dns zone <zoneName> -proxyMode (YES | NO)
- show dns zone [<zoneName> | -type <type>]

Example

```
> add dns zone example.com -proxyMode Yes
 Done
> show dns zone example.com
        Zone Name : example.com
        Proxy Mode : YES
Done
>
```

To modify or remove a DNS zone by using the command line interface

- To modify a DNS zone, type the set dns zone command, the name of the DNS zone, and the parameters to be changed, with their new values.
- To remove a DNS zone, type the rm dns zone command and the name of the dns zone.

Parameters for configuring a DNS zone

zoneName

The name of the zone being added. This is a mandatory argument. Maximum length: 255

proxyMode

Specifies whether the zone is deployed in proxy mode. This is a mandatory argument. Possible values: YES, NO. Default value: ENABLED

To configure a DNS zone by using the configuration utility

1. In the navigation pane, expand DNS, and then click Zones.
2. In the details pane, do one of the following:
   - To create a DNS zone, click Add.
   - To modify an existing DNS zone, select the zone, and then click Open.
3. In the Create DNS Zone or Configure DNS Zone dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a DNS zone,” as shown:
   - DNS Zone*—zoneName (cannot be changed for an existing DNS zone)
   - Proxy Mode—proxyMode

   * A required parameter
4. Click Create or OK.
5. In the details pane, click the name of the zone you just configured and verify that the settings displayed at the bottom of the screen are correct.

Configuring the NetScaler as an ADNS Server

You can configure the Citrix® NetScaler® appliance to function as an authoritative domain name server (ADNS) for a domain. As an ADNS server for a domain, the NetScaler resolves DNS requests for all types of DNS records that belong to the domain. To configure the NetScaler to function as an ADNS server for a domain, you must create an ADNS service and configure NS and Address records for the domain on the NetScaler. Normally, the ADNS service uses the Mapped IP address (MIP). However, you can configure the ADNS service with any NetScaler-owned IP address. The following topology diagram shows a sample configuration and the flow of requests and responses.

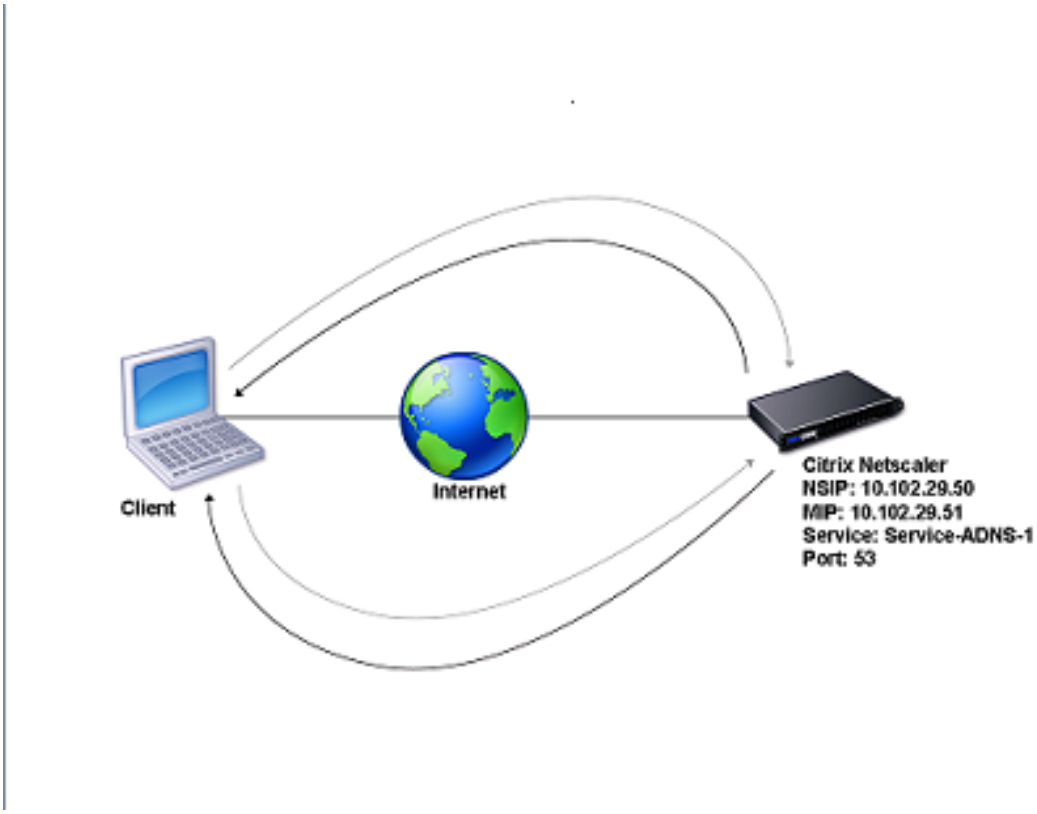


Figure 1. NetScaler as an ADNS

The following table shows the parameters that are configured for the ADNS service illustrated in the preceding topology diagram.

Table 1. Example of ADNS Service Configuration

Entity type	Name	IP address	Type	Port
ADNS Service	Service-ADNS-1	10.102.29.51	ADNS	53

To configure an ADNS setup, you must configure the ADNS service. For instructions on configuring the ADNS service, see "Load Balancing".

During DNS resolution, the ADNS server directs the DNS proxy or local DNS server to query the NetScaler for the IP address of the domain. Because the NetScaler is authoritative for the domain, it sends the IP address to the DNS proxy or local DNS server. The following diagram describes the placement and role of the ADNS server in a GSLB configuration.

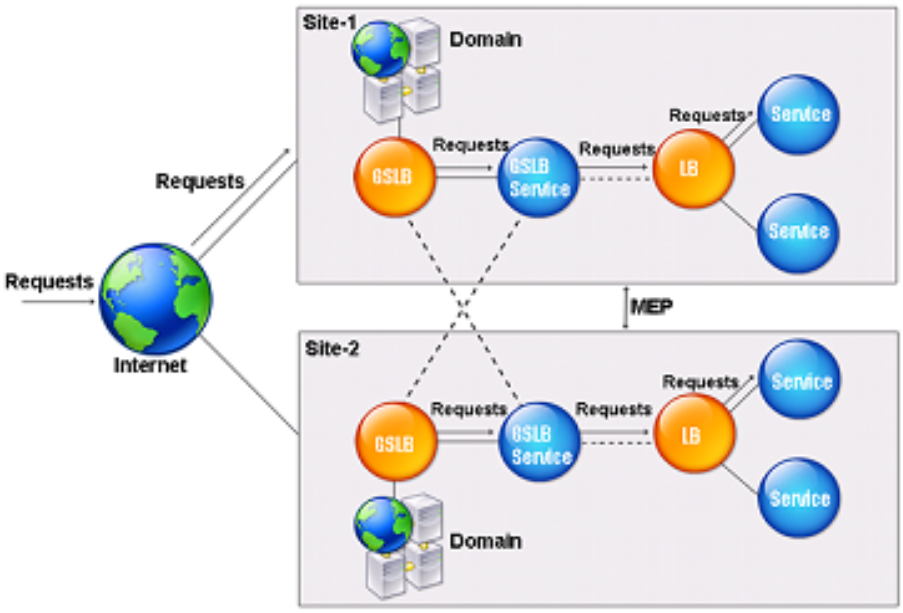


Figure 2. GSLB Entity Model

Note: In ADNS mode, if you remove SOA and ADNS records, the following do not function for the domain hosted by the NetScaler: ANY query (for more information about the ANY query, see DNS ANY Query), and negative responses, such as NODATA and NXDOMAIN.

Creating an ADNS Service

An ADNS service is used for global service load balancing. For more information about creating a GSLB setup, see "Global Server Load Balancing". You can add, modify, enable, disable, and remove an ADNS service. For instructions on creating an ADNS service, see Configuring Services.

Note: You can configure the ADNS service to use MIP, SNIP, or any new IP address.

When you create an ADNS service, the NetScaler responds to DNS queries on the configured ADNS service IP and port.

You can verify the configuration by viewing the properties of the ADNS service You can view properties such as name, state, IP address, port, protocol, and maximum client connections.

Configuring the ADNS Setup to Use TCP

By default, some clients use the User Datagram Protocol (UDP) for DNS, which specifies a limit of 512 bytes for the payload length of UDP packets. To handle payloads that exceed 512 bytes in size, the client must use the Transmission Control Protocol (TCP). To enable DNS communications over TCP, you must configure the NetScaler appliance to use the TCP protocol for DNS. The NetScaler then sets the truncation bit in the DNS response packets. The truncation bit specifies that the response is too large for UDP and that the client must send the request over a TCP connection. The client then uses the TCP protocol on port 53 and opens a new connection to the NetScaler. The NetScaler listens on port 53 with the IP address of the ADNS service to accept the new TCP connections from the client.

To configure the NetScaler to use the TCP protocol, you must configure an ADNS_TCP service. For instructions on creating an ADNS_TCP service, see "Load Balancing".

Important: To configure the NetScaler to use UDP for DNS and use TCP only when the payload length of UDP exceeds 512 bytes, you need to configure the ADNS and ADNS_TCP services. The IP address of the ADNS_TCP service must be same as the IP address of the ADNS service.

Adding DNS Resource Records

After you create an ADNS service, you can add DNS records. For instructions on adding DNS records, see Configuring DNS Resource Records.

Removing ADNS Services

For instructions on removing services, see Load Balancing.

Configuring Domain Delegation

Domain delegation is the process of assigning responsibility for a part of the domain space to another name server. Therefore, during domain delegation, the responsibility for responding to the query is delegated to another DNS server. Delegation uses NS records.

In the following example, sub1.abc.com is the subdomain for abc.com. The procedure describes the steps to delegate the subdomain to the name server ns2.sub1.abc.com and add an Address record for ns2.sub1.abc.com.

To configure domain delegation, you need to perform the following tasks, which are described in the sections that follow:

1. Create an SOA record for a domain.
2. Create an NS record to add a name server for the domain.
3. Create an Address record for the name server.
4. Create an NS record to delegate the subdomain.
5. Create a glue record for the name server.

Creating an SOA Record

For instructions on configuring SOA records, see Creating SOA Records for Authoritative Information.

Creating an NS Record for a Name Server

For instructions on configuring an NS record, see Creating NS Records for an Authoritative Server. In the Name Server drop-down list, select the primary authoritative name server, for example, ns1.abc.com.

Creating an Address Record

For instructions on configuring Address records, see Creating Address Records for a Domain Name. In the Host Name and IP address text boxes, type the domain name for the DNS Address record and the IP address, for example, ns1.abc.com and 10.102.11.135, respectively.

Creating an NS Record for Domain Delegation

For instructions on configuring NS records, see Creating NS Records for an Authoritative Server. In the Name Server drop-down list, select the primary authoritative name server, for example, ns2.sub1.abc.com.

Creating a Glue Record

NS records are usually defined immediately after the SOA record (but this is not a restriction.) A domain must have at least two NS records. If an NS record is defined within a domain, it must have a matching Address record. This Address record is referred to as a glue record. Glue records speed up DNS queries.

For instructions on adding glue records for a subdomain, see the procedure for adding an Address (A) record, Configuring DNS Resource Records.

For instructions on configuring Address records, see Creating Address Records for a Domain Name. In Host Name and IP address text boxes, type the domain name for the DNS Address record and the IP address, for example, ns2.sub1.abc.com and 10.102.12.135, respectively.

Configuring the NetScaler as a DNS Proxy Server

As a DNS proxy server, the Citrix® NetScaler® appliance can function as a proxy for either a single DNS server or a group of DNS servers. The flow of requests and responses is illustrated in the following sample topology diagram.

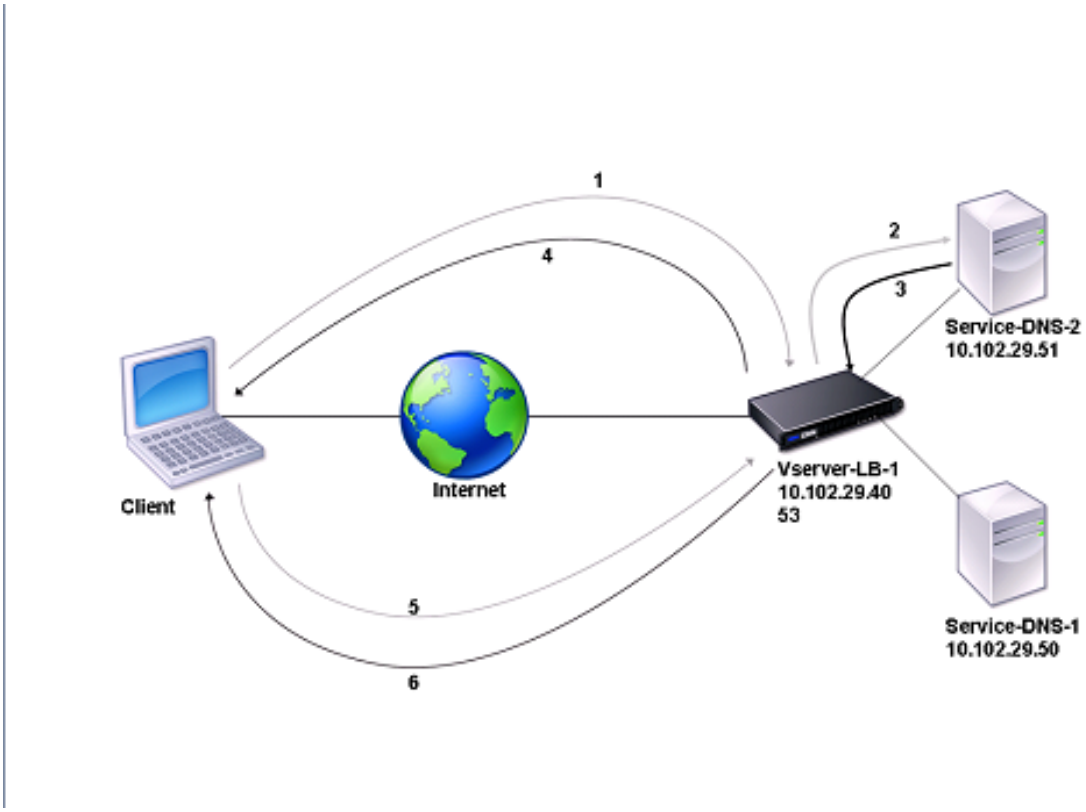


Figure 1. NetScaler as DNS proxy

By default, the NetScaler appliance caches responses from DNS name servers. When the appliance receives a DNS query, it checks for the queried domain in its cache. If the address for the queried domain is present in its cache, the NetScaler returns the corresponding address to the client. Otherwise, it forwards the query to a DNS name server that checks for the availability of the address and returns it to the NetScaler. The NetScaler then returns the address to the client.

For requests for a domain that has been cached earlier, the NetScaler serves the Address record of the domain from the cache without querying the configured DNS server.

The NetScaler discards a record stored in its cache when the time-to-live (TTL) value of the record reaches the configured value. A client that requests an expired record has to wait until the NetScaler retrieves the record from the server and updates its cache. To avoid this delay, the NetScaler proactively updates the cache by retrieving the record from the server

before the record expires.

The following table lists sample names and the values of the entities that need to be configured on the NetScaler.

Table 1. Example of DNS Proxy Entity Configuration

Entity type	Name	IP address	Type	Port
LB virtual server	Vserver-DNS-1	10.102.29.40	DNS	53
Services	Service-DNS-1	10.102.29.50	DNS	53
	Service-DNS-2	10.102.29.51	DNS	53

The following diagram shows the entities of a DNS Proxy and the values of the parameters to be configured on the NetScaler.

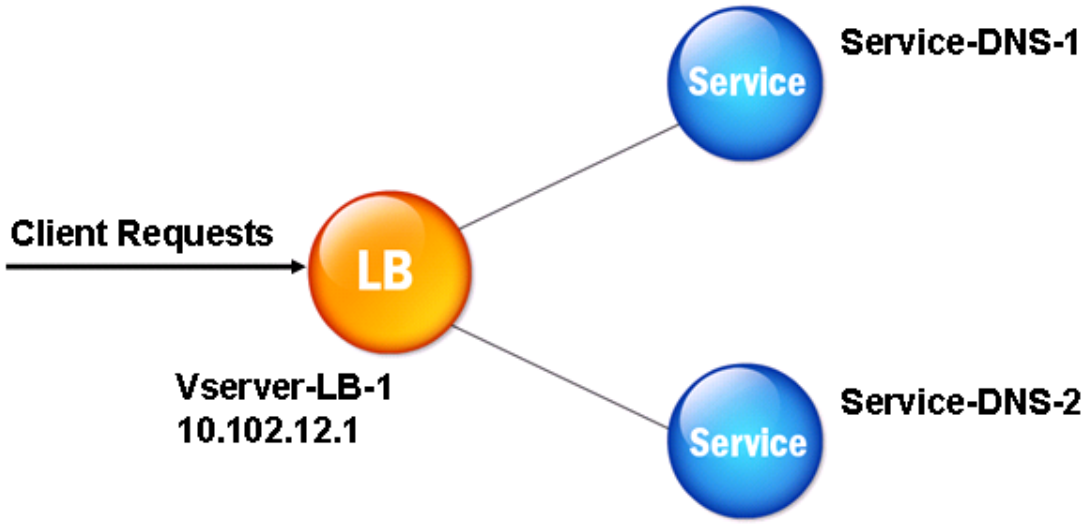


Figure 2. DNS Proxy Entity Model

Note: To configure DNS proxy, you need to know how to configure load balancing services and virtual servers. For information about configuring load balancing services and virtual servers, see "Load Balancing", and then configure DNS proxy setup.

Creating a Load Balancing Virtual Server

To configure a DNS Proxy on the NetScaler ADC, configure a load balancing virtual server of type DNS. To configure a DNS virtual server to load balance a set of DNS servers that support recursive queries, you must set the Recursion Available option. With this option, the RA bit is set to ON in the DNS replies from the DNS virtual server.

For instructions on creating a load balancing virtual server, see "Load Balancing".

Creating DNS Services

After creating a load balancing virtual server of type DNS, you must create DNS services. You can add, modify, enable, disable, and remove a DNS service. For instructions on creating a DNS service, see "Load Balancing".

Binding a Load Balancing Virtual Server to DNS Services

To complete the DNS Proxy configuration, you must bind the DNS services to the load balancing virtual server. For instructions on binding a service to a load balancing virtual server, see Load Balancing"".

Configuring the DNS Proxy Setup to Use TCP

Some clients use the User Datagram Protocol (UDP) for DNS communications. However, UDP specifies a maximum packet size of 512 bytes. When payload lengths exceed 512 bytes, the client must use the Transmission Control Protocol (TCP). When a client sends the Citrix® NetScaler® appliance a DNS query, the appliance forwards the query to one of the name servers. If the response is too large for a UDP packet, the name server sets the truncation bit in its response to the NetScaler. The truncation bit indicates that the response is too large for UDP and that the client must send the query over a TCP connection. The NetScaler relays the response to the client with the truncation bit intact and waits for the client to initiate a TCP connection with the IP address of the DNS load balancing virtual server, on port 53. The client sends the request over a TCP connection. The NetScaler appliance then forwards the request to the name server and relays the response to the client.

To configure the NetScaler to use the TCP protocol for DNS, you must configure a load balancing virtual server and services, both of type DNS_TCP. You can configure monitors of type DNS_TCP to check the state of the services. For instructions on creating DNS_TCP virtual servers, services, and monitors, see "Load Balancing."

For updating the records proactively, the NetScaler uses a TCP connection to the server to retrieve the records.

Important: To configure the NetScaler to use UDP for DNS and use TCP only when the payload length of UDP exceeds 512 bytes, you need to configure DNS and DNS_TCP services. The IP address of the DNS_TCP service must be same as that of the DNS service.

Enabling Caching of DNS Records

To complete the process of configuring a DNS proxy on the NetScaler, you must enable caching of DNS records. You must also specify minimum and maximum time-to-live (TTL) values for the records that are cached. The TTL values are measured in seconds.

To enable caching of DNS records by using the command line interface

At the command prompt, type the following commands to enable caching of DNS records and verify the configuration:

- set dns parameter -cacheRecords Yes
- show dns parameter

Example

```
> set dns parameter -cacheRecords YES
 Done
> show dns parameter
            .
            .
            .
       Cache Records : YES
            .
            .
            .
 Done
>
```

To enable caching of DNS records by using the configuration utility

1. In the navigation pane, click DNS.
2. In the details pane, under Settings, click Change DNS settings.
3. In the Configure DNS Parameters dialog box, select the Enable records caching check box, and then click OK.

Configuring Time-to-Live Values for DNS Entries

The TTL is the same for all DNS records with the same domain name and record type. If the TTL value is changed for one of the records, the new value is reflected in all records of the same domain name and type. The default TTL value is 3600 seconds. The minimum is 0, and the maximum is 2147483647. If a DNS entry has a TTL value less than the minimum or greater than the maximum, it is saved as the minimum or maximum TTL value, respectively.

To specify the minimum and/or maximum TTL by using the command line interface

At the NetScaler command prompt, type the following commands to specify the minimum and maximum TTL and verify the configuration:

- set dns parameter [-minTTL <secs>] [-maxTTL <secs>]
- show dns parameter

Example

```
> set dns parameter -minTTL 1200 -maxTTL 1800
 Done
> show dns parameter
       DNS parameters:
       DNS retries: 5
       Minimum TTL: 1200            Maximum TTL: 1800
          .
          .
          .
 Done
>
```

To specify the minimum and/or maximum TTL by using the configuration utility

1. In the navigation pane, click DNS.
2. In the details pane, under Settings, click Change DNS settings.
3. In the Configure DNS Parameters dialog box, in TTL, in the Minimum and Maximum text boxes, type the minimum and maximum time to live (in seconds), respectively, and then click OK.

Note: When the TTL expires, the record is deleted from the cache. The NetScaler proactively contacts the servers and obtains the DNS record just before the DNS record expires.

Flushing DNS Records

You can delete all DNS records present in the cache. For example, you might want to flush DNS records when a server is restarted after modifications are made.

To delete all proxy records by using the command line interface

At the NetScaler command prompt, type:

flush dns proxyRecords

To delete all proxy records by using the configuration utility

1. In the navigation pane, expand DNS, expand Records, and then click Address Records.
2. In the details pane, click Flush Proxy Records.

Adding DNS Resource Records

You can add DNS records to a domain for which the Citrix® NetScaler® appliance is configured as a DNS proxy server. For information about adding DNS records, see Configuring DNS Resource Records.

Removing a Load Balancing DNS Virtual Server

For information about removing a load balancing virtual server, see Load Balancing.

Limiting the Number of Concurrent DNS Requests on a Client Connection

You can limit the number of concurrent DNS requests on a single client connection, which is identified by the <clientip:port>-<vserver ip:port> tuple. Concurrent DNS requests are those requests that the NetScaler appliance has forwarded to the name servers and for which the appliance is awaiting responses. Limiting the number of concurrent requests on a client connection enables you to protect the name servers when a hostile client attempts a Distributed Denial of Service (DDoS) attack by sending a flood of DNS requests. When the limit for a client connection is reached, subsequent DNS requests on the connection are dropped till the outstanding request count goes below the limit. This limit does not apply to the requests that the NetScaler appliance serves out of its cache.

The default value for this parameter is 255. This default value is sufficient in most scenarios. If the name servers serve a large number of concurrent DNS requests under normal operating conditions, you can specify either a large value or a value of zero (0). A value of 0 disables this feature and specifies that there is no limit to the number of DNS requests that are allowed on a single client connection. This is a global parameter and applies to all the DNS virtual servers that are configured on the NetScaler appliance.

To specify the maximum number of concurrent DNS requests allowed on a single client connection by using the command line interface

At the command prompt, type the following commands to specify the maximum number of concurrent DNS requests allowed on a single client connection and verify the configuration:

- set dns parameter -maxPipeline <positive_integer>
- show dns parameter

Example

```
> set dns parameter -maxPipeline 1000
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 5
        .
        .
        .
        Max DNS Pipeline Requests: 1000
 Done
>
```

Parameters for specifying the maximum number of concurrent DNS requests on a single client connection

maxPipeline

Specifies the maximum number of concurrent DNS requests that are allowed on a single client connection. A value of 0 (zero) implies that there is no limit to the number of concurrent DNS requests that are allowed on a single client connection. Default value: 255

To specify the maximum number of concurrent DNS requests allowed on a single client connection by using the configuration utility

1. In the navigation pane, click DNS.
2. In the details pane, click Change DNS settings.
3. In the Configure DNS Parameters dialog box, specify a value for Max DNS Pipeline Requests, which corresponds to the parameter described in "Parameters for specifying the maximum number of concurrent DNS requests on a single client connection."
4. Click OK.

Configuring the NetScaler as an End Resolver

A resolver is a procedure that is invoked by an application program that translates a domain/host name to its resource record. The resolver interacts with the LDNS, which looks up the domain name to obtain its IP address. The NetScaler can provide end-to-end resolution for DNS queries.

In recursive resolution, the NetScaler appliance queries different name servers recursively to access the IP address of a domain. When the NetScaler receives a DNS request, it checks its cache for the DNS record. If the record is not present in the cache, it queries the root servers configured in the ns.conf file. The root name server reports back with the address of a DNS server that has detailed information about the second-level domain. The process is repeated until the required record is found.

When you start the NetScaler appliance for the first time, 13 root name servers are added to the ns.conf file. The NS and Address records for the 13 root servers are also added. You can modify the ns.conf file, but the NetScaler does not allow you to delete all 13 records; at least one name server entry is required for the appliance to perform name resolution. The following diagram illustrates the process of name resolution.

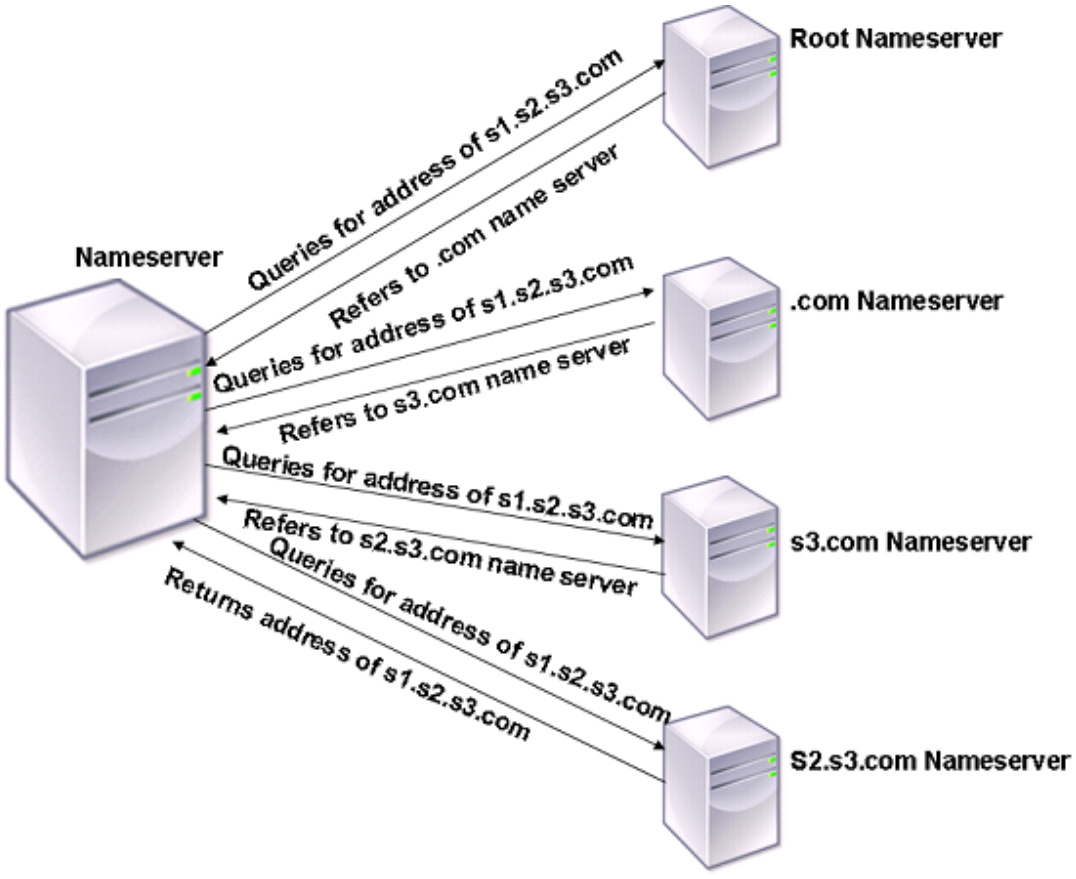


Figure 1. Recursive Resolution

In the process shown in the diagram, when the name server receives a query for the address of s1.s2.s3.com, it first checks the root name servers for s1.s2.s3.com. A root name server reports back with the address of the .com name server. If the address of s1.s2.s3.com is found in the name server, it responds with a suitable IP address. Otherwise, it queries other name servers for s3.com, then for s2.s3.com to retrieve the address of s1.s2.s3.com. In this way, resolution always starts from root name servers and ends with the domain's authoritative name server.

Note: For recursive resolution functionality, caching should be enabled.

Enabling Recursive Resolution

To configure the NetScaler appliance to function as an end resolver, you must enable recursive resolution on the appliance.

To enable recursive resolution by using the command line interface

At the command prompt, type the following commands to enable recursive resolution and verify the configuration:

- set dns parameter -recursion ENABLED
- show dns parameter

Example

```
> set dns parameter -recursion ENABLED
 Done
> show dns parameter
      DNS parameters:
          .
          .
          .
      Recursive Resolution : ENABLED
          .
          .
          .
 Done
>
```

To enable recursive resolution by using the configuration utility

1. In the navigation pane, click DNS.
2. In the details pane, under Settings, click Change DNS settings.
3. In the Configure DNS Parameters dialog box, select the Enable recursion check box, and then click OK.

Setting the Number of Retries

The NetScaler appliance can be configured to make a preconfigured number of attempts (called DNS retries) when it does not receive a response from the server to which it sends a query. By default, the number of DNS retries is set to 5.

To set the number of DNS retries by using the command line interface

At the command prompt, type the following commands to set the number of retries and verify the configuration:

- set dns parameter -retries <positive_integer>
- show dns parameter

Example

```
> set DNS parameter -retries 3
 Done
> show dns parameter
       DNS parameters:
       DNS retries: 3
           .
           .
           .
 Done
>
```

To set the number of retries by using the configuration utility

1. In the navigation pane, click DNS.
2. In the details pane, under Settings, click Change DNS settings.
3. In the Configure DNS Parameters dialog box, in the DNS Retries text box, type the DNS resolver request retry count, and then click OK.

Configuring the NetScaler as a Forwarder

A forwarder is a server that forwards DNS queries to DNS servers that are outside the forwarder server's network. Queries that cannot be resolved locally are forwarded to other DNS servers. A forwarder accumulates external DNS information in its cache as it resolves DNS queries. To configure the NetScaler as a forwarder, you must add an external name server (a name server other than the Citrix NetScaler appliance).

The NetScaler appliance allows you to add external name servers to which it can forward the name resolution queries that cannot be resolved locally. To configure the NetScaler appliance as a forwarder, you must add the name servers to which it should forward name resolution queries. You can specify the lookup priority to specify the name service that the NetScaler appliance must use for name resolution.

Adding a Name Server

You can create a name server by specifying its IP address or by configuring an existing virtual server as the name server.

While adding name servers, you can provide an IP address or a virtual IP address (VIP). If you add an IP address, the NetScaler load balances requests to the configured name servers in round robin method. If you add a VIP, you can configure any load balancing method.

Example 1, which follows the command synopsis below, adds a local name server. Example 2 specifies the name of a load balancing virtual server of service type DNS.

Note: To verify the configuration, you can also use the `sh dns <recordtype> <domain>` command. If the queried records are not present in the cache, the resource records are fetched from the configured external name servers.

To add a name server by using the command line interface

At the command prompt, type the following commands to add a name server and verify the configuration:

- add dns nameServer ((<IP> [-local]) | <dnsVserverName>)
- show dns nameServer [<IP> | <dnsVserverName>]

Example 1

```
> add dns nameServer 10.102.9.20 -local
 Done
> show dns nameServer 10.102.9.20
1)      10.102.9.20: LOCAL  -  State: UP
Done
>
```

Example 2

```
> add dns nameServer dnsVirtualNS
 Done
> show dns nameServer dnsVirtualNS
1)      dnsVirtualNS  -  State: DOWN
 Done
>
```

To remove a name server by using the NetScaler command line, at the NetScaler command prompt, type the rm dns nameServer command followed by the IP address of the name server.

Parameters for adding a name server

IP

The IP address of the name server.

local

Specifies that the IP address belongs to a local recursive name server.

dnsVserverName

The name of a DNS virtual server. Maximum length: 127.

To add a name server by using the configuration utility

1. In the navigation pane, expand DNS, and then click Name Servers.
2. In the details pane, click Add.
3. In the Create Name Server dialog box, do one of the following:
   - To add an IP address, click IP Address, and in the IP Address text box, type the IP address of the name server, for example, **10.102.29.10**. If you are adding an external name server, clear the Local check box.
   - To add a DNS virtual server, click DNS Virtual Server, and select a DNS virtual server. Click New if you want to create a new load balancing virtual server. The Create Virtual Server (Load Balancing) dialog box appears.
4. Click Create, and then click Close.

Note: When name servers are added in the Forwarder mode, the Local option must be cleared. When name servers are added in the End Resolver mode, the Local option must be selected.

Setting DNS Lookup Priority

You can set the lookup priority to either DNS or WINS. This option is used in the SSL VPN mode of operation.

To set the lookup priority to DNS by using the command line interface

At the command prompt, type the following commands to set the lookup priority to DNS and verify the configuration:

- set dns parameter -nameLookupPriority (DNS | WINS)
- show dns parameter

Example

```
> set dns parameter -nameLookupPriority DNS
 Done
> show dns parameter
          .
          .
          .
      Name lookup priority : DNS
          .
          .
          .
 Done
>
```

To set lookup priority to DNS by using the configuration utility

1. In the navigation pane, click DNS.
2. In the details pane, under Settings, click Change DNS settings.
3. In the Configure DNS Parameters dialog box, under Name Lookup Priority, select DNS or WINS, and then click OK.

Note: If the DNS virtual server that you have configured is DOWN and if you set the -nameLookupPriority to DNS, the NetScaler does not attempt WINS lookup. Therefore, if a

DNS virtual server is not configured or is disabled, set the -nameLookupPriority to WINS.

Disabling and Enabling Name Servers

The following procedure describes the steps to enable or disable an existing name server.

To enable or disable a name server by using the command line interface

At the command prompt, type the following commands to enable or disable a name server and verify the configuration:

- (enable | disable) dns nameServer <IPAddress>
- show dns nameServer <IPAddress>

Example

```
> disable dns nameServer 10.102.9.19
 Done
> show dns nameServer 10.102.9.19
1)      10.102.9.19: LOCAL  -  State: OUT OF SERVICE
 Done
>
```

To enable or disable a name server by using the configuration utility

1. In the navigation pane, expand DNS, and then click Name Servers.
2. In the details pane, select the name server that you want to enable or disable.
3. Click Enable or Disable. If a name server is enabled, the Disable option is available. If a name server is disabled, the Enable option is available.

Configuring DNS Suffixes

You can configure DNS suffixes that enable the NetScaler appliance to complete non-fully qualified domain names (non-FQDNs) during name resolution. For example, during the process of resolving the domain name abc (which is not fully qualified), if a DNS suffix example.com is configured, the appliance appends the suffix to the domain name (abc.example.com) and resolves it. If DNS suffixes are not configured, the appliance appends a period to the non-FQDNs and resolves the domain name.

Creating DNS Suffixes

DNS suffixes have significance and are valid only when the NetScaler is configured as an end resolver or forwarder. You can specify a suffix of up to 127 characters.

To create DNS suffixes by using the command line interface

At the command prompt, type the following commands to create a DNS suffix and verify the configuration:

- add dns suffix <dnsSuffix>
- show dns suffix <dnsSuffix>

Example

```
> add dns suffix example.com
 Done
> show dns suffix example.com
1)      Suffix: example.com
 Done
>
```

To remove a DNS suffix by using the NetScaler command line, at the NetScaler command prompt, type the rm dns suffix command and the name of the DNS suffix.

To create DNS suffixes by using the configuration utility

1. In the navigation pane, expand DNS, and then click DNS Suffix.
2. In the details pane, click Add.
3. In the Create DNS Suffix dialog box, type the suffix (for example, **example.com**).
4. Click Create, and then click Close.

DNS ANY Query

An ANY query is a type of DNS query that retrieves all records available for a domain name. The ANY query must be sent to a name server that is authoritative for a domain.

Behavior in ADNS Mode

In the ADNS mode, the NetScaler appliance returns the records held in its local cache. If there are no records in the cache, the appliance returns the NXDOMAIN (negative) response.

If the NetScaler can match the domain delegation records, it returns the NS records. Otherwise, it returns the NS records of the root domain.

Behavior in DNS Proxy Mode

In proxy mode, the NetScaler appliance checks its local cache. If there are no records in the cache, the appliance passes the query to the server.

Behavior for GSLB Domains

If a GSLB domain is configured on the NetScaler appliance and an ANY query is sent for the GSLB domain (or GSLB site domain), the appliance returns the IP address of the GSLB service that it selects through the Load Balancing decision. If the multiple IP response (MIR) option is enabled, the IP addresses of all GSLB services are sent.

For the NetScaler to return these records when it responds to the ANY query, all records corresponding to a GSLB domain must be configured on the NetScaler.

Note: If records for a domain are distributed between the NetScaler and a server, only records configured on the NetScaler are returned.

The NetScaler provides the option to configure DNS views and DNS policies. These are used for performing global server load balancing. For more information, see Global Server Load Balancing.

Domain Name System Security Extensions

DNS Security Extensions (DNSSEC) is an Internet Engineering Task Force (IETF) standard that aims to provide data integrity and data origin authentication in communications between name servers and clients while still transmitting User Datagram Protocol (UDP) responses in clear text. DNSSEC specifies a mechanism that uses asymmetric key cryptography and a set of new resource records that are specific to its implementation.

The DNSSEC specification is described in RFC 4033, “DNS Security Introduction and Requirements,” RFC 4034, “Resource Records for the DNS Security Extensions,” and RFC 4035, “Protocol Modifications for the DNS Security Extensions.” The operational aspects of implementing DNSSEC within DNS are discussed in RFC 4641, “DNSSEC Operational Practices.”

You can configure DNSSEC on the Citrix® NetScaler® ADC. You can generate and import keys for signing DNS zones. You can configure DNSSEC for zones for which the NetScaler ADC is authoritative. You can configure the ADC as a DNS proxy server for signed zones hosted on a farm of backend name servers. If the ADC is authoritative for a subset of the records belonging to a zone for which the ADC is configured as a DNS proxy server, you can include the subset of records in the DNSSEC implementation.

Configuring DNSSEC

Configuring DNSSEC involves enabling DNSSEC on the Citrix® NetScaler® appliance, creating a Zone Signing Key and a Key Signing Key for the zone, adding the two keys to the zone, and then signing the zone with the keys.

The NetScaler ADC does not act as a DNSSEC resolver. DNSSEC on the ADC is supported only in the following deployment scenarios:

1. ADNS—NetScaler is the ADNS and generates the signatures itself.

2. Proxy—NetScaler acts as a DNSSEC proxy. It is assumed that the NetScaler is placed in front of the ADNS/LDNS servers in a trusted mode. The ADC acts only as a proxy caching entity and does not validate any signatures.

Enabling and Disabling DNSSEC

You must enable DNSSEC on the NetScaler ADC for the ADC to respond to DNSSEC-aware clients. By default, DNSSEC is enabled.

You can disable the DNSSEC feature if you do not want the NetScaler ADC to respond to clients with DNSSEC-specific information.

To enable or disable DNSSEC by using the command line interface

At the command prompt, type the following commands to enable or disable DNSSEC and verify the configuration:

- set dns parameter -dnssec (ENABLED | DISABLED)
- show dns parameter

Example

```
> set dns parameter -dnssec ENABLED
 Done
> show dns parameter
       DNS parameters:
       DNS retries: 5
        .
        .
        .
        DNSEC Extension: ENABLED
       Max DNS Pipeline Requests: 255
 Done
>
```

Parameters for enabling and disabling DNSSEC

dnssec

Enable or disable DNSSEC on the NetScaler appliance. Possible values: ENABLED, DISABLED. Default value: ENABLED

To enable or disable DNSSEC by using the configuration utility

1. In the navigation pane, click DNS.
2. In the details pane, click Change DNS settings.
3. In the Configure DNS Parameters dialog box, select or clear the Enable DNSSEC Extension check box.

Creating DNS Keys for a Zone

For each DNS zone that you want to sign, you must create two pairs of asymmetric keys. One pair, called the Zone Signing Key, is used to sign all the resource record sets in the zone. The second pair is called the Key Signing Key and is used to sign only the DNSKEY resource records in the zone.

When the Zone Signing Key and Key Signing Key are created, the suffix .key is automatically appended to the names of the public components of the keys and the suffix .private is automatically appended to the names of their private components.

Additionally, the NetScaler ADC also creates a Delegation Signer (DS) record and appends the suffix .ds to the name of the record. If the parent zone is a signed zone, you must publish the DS record in the parent zone to establish the chain of trust.

When you create a key, the key is stored in the /nsconfig/dns/ directory, but it is not automatically published in the zone. After you create a key by using the create dns key command, you must explicitly publish the key in the zone by using the add dns key command. The process of generating a key has been separated from the process of publishing the key in a zone to enable you to use alternative means to generate keys. For example, you can import keys generated by other key-generation programs (such as `bind-keygen`) by using Secure File Transfer Protocol (SFTP) and then publish the keys in the zone. For more information about publishing a key in a zone, see Publishing a DNS Key in a Zone.

Perform the steps described in this topic to create a Zone Signing Key and then repeat the steps to create a Key Signing Key. The example that follows the command syntax first creates a Zone Signing Key pair for the zone `example.com`. The example then uses the command to create a Key Signing Key pair for the zone.

To create a DNS key by using the command line interface

At the NetScaler command prompt, type the following command to create a DNS key:

create dns key -zoneName <string> -keyType <keyType> -algorithm RSASHA1 -keySize <positive_integer> -fileNamePrefix <string>

Example

```
> create dns key -zoneName example.com -keyType zsk -algorithm RSASHA1 -keySize 1024 -fileNamePrefix e
File Name: /nsconfig/dns/example.com.zsk.rsasha1.1024.key (public); /nsconfig/dns/example.com.zsk.rsas
This operation may take some time, Please wait...
 Done
> create dns key -zoneName example.com -keyType ksk -algorithm RSASHA1 -keySize 4096 -fileNamePrefix e
File Name: /nsconfig/dns/example.com.ksk.rsasha1.4096.key (public); /nsconfig/dns/example.com.ksk.rsas
This operation may take some time, Please wait...
```

```
 Done
>
```

Parameters for creating a DNS Key

zoneName

The name of the zone for which the key is being added. This is a mandatory argument.

keyType

The type of key. This is a mandatory argument. Possible values: KSK, KeySigningKey, ZSK, ZoneSigningKey.

Default value: ZSK

algorithm

The algorithm that must be used to generate the keys. This is a mandatory argument. Possible values: RSASHA1. Default value: RSASHA1.

keySize

The key strength. This is a mandatory argument. Default value: 512

fileNamePrefix

A common prefix for the public and private components of the key pair. During key generation, the .key and .private suffixes are appended automatically to the file name prefix.

To create a DNS key by using the configuration utility

1. In the navigation pane, click DNS.
2. In the details area, click Create DNS Key.
3. In the Create DNS Key dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating a DNS Key,” as shown:
   - Zone Name*—zoneName
   - Type*—keyType
   - Algorithm*—algorithm
   - Size*—keySize
   - File Name Prefix*—fileNamePrefix

   * A required parameter

   Note: For File Name Prefix, if you want to modify the file name prefix of an existing key, click the arrow next to the Browse button, click either Local or Appliance (depending on whether the existing key is stored on your local computer or in the /nsconfig/dns/ directory on the appliance), browse to the location of the key, and then double-click the key. The File Name Prefix box is populated with only the prefix of the existing key. Modify the prefix accordingly.
4. Click Create, and then click Close.

Publishing a DNS Key in a Zone

A key (Zone Signing Key or Key Signing Key) is published in a zone by adding the key to the NetScaler ADC. A key must be published in a zone before you sign the zone.

Before you publish a key in a zone, the key must be available in the /nsconfig/dns/ directory. Therefore, if you used other means to generate the key—means other than the create dns key command on the NetScaler ADC (for example, by using the `bind-keygen` program on another computer)—make sure that the key is added to the /nsconfig/dns/ directory before you publish the key in the zone.

If the key has been generated by another program, you can import the key to your local computer and use the NetScaler configuration utility to add the key to the /nsconfig/dns/ directory. Or, you can use other means to import the key to the directory, such as the Secure File Transfer Protocol (SFTP).

You must use the add dns key command for each public-private key pair that you want to publish in a given zone. If you created a Zone Signing Key pair and a Key Signing Key pair for a zone, use the add dns key command to first publish one of the key pairs in the zone and then repeat the command to publish the other key pair. For each key that you publish in a zone, a DNSKEY resource record is created in the zone.

The example that follows the command syntax first publishes the Zone Signing Key pair (that was created for the `example.com` zone) in the zone. The example then uses the command to publish the Key Signing Key pair in the zone.

To publish a key in a zone by using the command line interface

At the command prompt, type the following command to publish a key in a zone and verify the configuration:

- add dns key <keyName> <publickey> <privatekey> [-expires <positive_integer> [<units>]] [-notificationPeriod <positive_integer> [<units>]] [-TTL <secs>]
- show dns zone [<zoneName> | -type <type>]

Example

```
> add dns key example.com.zsk example.com.zsk.rsasha1.1024.key example.com.zsk.rsasha1.1024.private
 Done
> add dns key example.com.ksk example.com.ksk.rsasha1.4096.key example.com.ksk.rsasha1.4096.private
 Done
> show dns zone example.com
        Zone Name : example.com
        Proxy Mode : NO
        Domain Name : example.com
```

```
            Record Types : NS SOA DNSKEY
        Domain Name : ns1.example.com
            Record Types : A
        Domain Name : ns2.example.com
            Record Types : A
 Done
>
```

Parameters for publishing a key in a zone

keyName

The name given to a public-private key pair. This is a mandatory argument. Maximum length: 31.

publickey

File name of the public key that is used for signing the zone. This is a mandatory argument. Maximum length: 63

privatekey

File name of the private key that is used for signing the zone. This is a mandatory argument. Maximum length: 63

expires

Time for which the key is valid. Default value: 120 days. Minimum value: 1. Maximum value: 32767.

units

Units for the expiry time. Possible values: MINUTES, HOURS, DAYS. Default value: DAYS.

notificationPeriod

Number of days, hours, or minutes prior to expiry of a key when a notification should be generated. Default value: 7 days. Minimum value: 1. Maximum value: 32767.

units

Units for the notification period. Possible values: MINUTES, HOURS, DAYS. Default value: DAYS.

TTL

Time to Live, in seconds. Default value: 3600. Minimum value: 0. Maximum value: 2147483647.

To publish a key in a DNS zone by using the NetScaler configuration utility

1. In the navigation pane, expand DNS, and then click Keys.
2. In the details pane, click Add.
3. In the Add DNS Key dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for adding a key to the NetScaler ADC,” as shown:
   - DNS Key Name*—keyName
   - Public Key*—publickey
   - Private Key*—privatekey
   - Expires—expires
   - Notification Period—notificationPeriod
   - TTL—TTL

   * A required parameter

   Note: For Public Key and Private Key, to add a key that is stored on your local computer, click the arrow next to the Browse button, click Local, browse to the location of the key, and then double-click the key.
4. Click Create, and then click Close.

Configuring a DNS Key

You can configure the parameters of a key that has been published in a zone. You can modify the key's expiry time period, notification period, and time-to-live (TTL) parameters. If you change the expiry time period of a key, the NetScaler ADC automatically re-signs all the resource records in the zone with the key, provided that the zone is currently signed with the particular key.

To configure a key by using the command line interface

At the command prompt, type the following command to configure a key and verify the configuration:

- set dns key <keyName> [-expires <positive_integer> [<units>]] [-notificationPeriod <positive_integer> [<units>]] [-TTL <secs>]
- show dns key [<keyName>]

Example

```
> set dns key example.com.ksk -expires 30 DAYS -notificationPeriod 3 DAYS -TTL 3600
 Done
> show dns key example.com.ksk
1)      Key Name: example.com.ksk
       Expires: 30 DAYS        Notification: 3 DAYS    TTL: 3600
       Public Key File: example.com.ksk.rsasha1.4096.key
       Private Key File: example.com.ksk.rsasha1.4096.private
 Done
>
```

Parameters for configuring a key

keyName

The name given to a public/private key pair. This is a mandatory argument. Maximum length: 31.

expires

Time for which the key is valid. Default value: 120 days. Minimum value: 1. Maximum value: 32767.

units

Units for the expiry time. Possible values: MINUTES, HOURS, DAYS. Default value: DAYS.

notificationPeriod

Number of days, hours, or minutes prior to expiry of a key when a notification should be generated. Default value: 7 days. Minimum value: 1. Maximum value: 32767.

units

Units for the notification period Possible values: MINUTES, HOURS, DAYS. Default value: DAYS.

TTL

Time to Live, in seconds. Default value: 3600. Minimum value: 0. Maximum value: 2147483647.

To configure a key by using the configuration utility

1. In the navigation pane, expand DNS, and then click Keys.
2. In the details pane, click the key that you want to configure, and then click Open.
3. In the Configure DNS Key dialog box, modify the values of the following parameters, which correspond to parameters described in “Parameters for configuring a key,” as shown:
   - Expires—expires
   - Notification Period—notificationPeriod
   - TTL—TTL
4. Click OK.

Signing and Unsigning a DNS Zone

To secure a DNS zone, you must sign the zone with the keys that have been published in the zone. When you sign a zone, the NetScaler ADC creates a Next Secure (NSEC) resource record for each owner name. Then, it uses the Key Signing Key to sign the DNSKEY resource record set. Finally, it uses the Zone Signing Key to sign all the resource record sets in the zone, including the DNSKEY resource record sets and NSEC resource record sets. Each sign operation results in a signature for the resource record sets in the zone. The signature is captured in a new resource record called the RRSIG resource record.

After you sign a zone, you must save the configuration.

To sign a zone by using the command line interface

At the command prompt, type the following command to sign a zone and verify the configuration:

- sign dns zone <zoneName> [-keyName <string> ...]
- show dns zone [<zoneName> | -type (ADNS | PROXY | ALL)]
- save config

Example

```
> sign dns zone example.com -keyName example.com.zsk example.com.ksk
 Done
> show dns zone example.com
        Zone Name : example.com
        Proxy Mode : NO
        Domain Name : example.com
                Record Types : NS SOA DNSKEY RRSIG NSEC
        Domain Name : ns1.example.com
                Record Types : A RRSIG NSEC
        Domain Name : ns2.example.com
                Record Types : A RRSIG
        Domain Name : ns2.example.com
                Record Types : RRSIG NSEC
Done
> save config
 Done
>
save config
```

To unsign a zone by using the command line interface

At the command prompt, type the following command to unsign a zone and verify the configuration:

- unsign dns zone <zoneName> [-keyName <string> ...]
- show dns zone [<zoneName> | -type (ADNS | PROXY | ALL)]

Example

```
> unsign dns zone example.com -keyName example.com.zsk example.com.ksk
 Done
> show dns zone example.com
        Zone Name : example.com
        Proxy Mode : NO
        Domain Name : example.com
                Record Types : NS SOA DNSKEY
        Domain Name : ns1.example.com
                Record Types : A
        Domain Name : ns2.example.com
                Record Types : A
 Done
>
```

Parameters for signing and unsigning a DNS zone

zoneName

The name of the zone being signed. This is a mandatory argument. Maximum length: 255.

keyName

The name given to a public/private key pair. Maximum length: 127

To sign or unsign a zone by using the configuration utility

1. In the navigation pane, expand DNS, and then click Zones.
2. In the details pane, click the zone that you want to sign, and then click Sign/Unsign.
3. In the Sign/Unsign DNS Zone dialog box, do one of the following:
   - To sign the zone, select the check boxes for the keys (Zone Signing Key and Key Signing Key) with which you want to sign the zone.

     You can sign the zone with more than one Zone Signing Key or Key Signing Key pair.
   - To unsign the zone, clear the check boxes for the keys (Zone Signing Key and Key Signing Key) with which you want to unsign the zone.

     You can unsign the zone with more than one Zone Signing Key or Key Signing Key pair.
4. Click OK.

Viewing the NSEC Records for a Given Record in a Zone

You can view the NSEC records that the NetScaler ADC automatically creates for each owner name in the zone.

To view the NSEC record for a given record in a zone by using the command line interface

At the command prompt, type the following command to view the NSEC record for a given record in a zone:

show dns nsecRec [<hostName> | -type (ADNS | PROXY | ALL)]

Example

```
> show dns nsecRec example.com
1)      Domain Name : example.com
       Next Nsec Name: ns1.example.com
       Record Types : NS SOA DNSKEY RRSIG NSEC
 Done
>
```

Parameters for viewing the NSEC record for a given record in a zone

hostName

The domain name whose information is to be displayed.

Maximum length: 255

type

The NSEC record type. The type can take 3 values:

ADNS - If this is specified, all of the authoritative NSEC records will be displayed.

PROXY - If this is specified, all of the proxy NSEC records will be displayed.

ALL - If this is specified, all of the NSEC records will be displayed.

Possible values: ALL, ADNS, PROXY

To view the NSEC record for given record in a zone by using the configuration utility

1. In the navigation pane, expand DNS, expand Records, and then click Next Secure Records.

2. In the details pane, click the name of the record for which you want to view the NSEC record. The NSEC record for the record you select is displayed in the Details area.

Removing a DNS Key

You remove a key from the zone in which it is published when the key has expired or if the key has been compromised. When you remove a key from the zone, the zone is automatically unsigned with the key. Removing the key with this command does not remove the key files present in the /nsconfig/dns/ directory. If the key files are no longer needed, they have to be explicitly removed from the directory.

To remove a key from the NetScaler ADC by using the command line interface

At the command prompt, type the following command to remove a key and verify the configuration:

- rm dns key <keyName>
- show dns key <keyName>

Example

```
> rm dns key example.com.zsk
 Done
> show dns key example.com.zsk
ERROR: No such resource [keyName, example.com.zsk]
>
```

Parameters for removing a key from the NetScaler ADC

keyName

The name given to a public/private key pair. This is a mandatory argument. Maximum length: 31

To remove a key from the NetScaler ADC by using the configuration utility

1. Navigate to Traffic Management > DNS > Keys.
2. In the navigation pane, expand DNS, and then click Keys.
3. In the details pane, click the name of the key that you want to remove from the ADC, and then click Remove.

Configuring DNSSEC When the NetScaler ADC is Authoritative for a Zone

When the Citrix® NetScaler® ADC is authoritative for a given zone, all the resource records in the zone are configured on the ADC. To sign the authoritative zone, you must create keys (the Zone Signing Key and the Key Signing Key) for the zone, add the keys to the ADC, and then sign the zone, as described in Creating DNS Keys for a Zone, Publishing a DNS Key in a Zone, and Signing and Unsigning a DNS Zone, respectively.

If any global server load balancing (GSLB) domains configured on the ADC belong to the zone being signed, the GSLB domain names are signed along with the other records that belong to the zone.

After you sign a zone, responses to requests from DNSSEC-aware clients include the RRSIG resource records along with the requested resource records. DNSSEC must be enabled on the ADC. For more information about enabling DNSSEC, see Enabling and Disabling DNSSEC.

Finally, after you configure DNSSEC for the authoritative zone, you must save the NetScaler configuration.

Configuring DNSSEC for a Zone for Which the NetScaler ADC Is a DNS Proxy Server

The procedure for signing a zone for which the Citrix® NetScaler® ADC is configured as a DNS proxy server depends on whether or not the ADC owns a subset of the zone information owned by the backend name servers. If it does, the configuration is considered a *partial zone ownership configuration*. If the ADC does not own a subset of the zone information, the NetScaler configuration for managing the backend servers is considered a *zone-less DNS proxy server configuration*. The basic DNSSEC configuration tasks for both NetScaler configurations are the same. However, signing the partial zone on the NetScaler ADC requires some additional configuration steps.

Note: The terms *zone-less proxy server configuration* and *partial zone* are used only in the context of the NetScaler appliance.

Important: When configured in proxy mode, the ADC does not perform signature verification on DNSSEC responses before updating the cache.

If you configure the ADC as a DNS proxy to load balance DNSSEC aware resolvers (servers), you must set the Recursion Available option while configuring the DNS virtual server. If a DNSSEC query arrives with Checking Disabled (CD) bit set, the query is passed on to the server with the CD bit retained, and the response from the server is not cached. In releases prior to 10.5.e build xx.x, the ADC unset the CD bit before passing it to the server and also cached the server response.

Configuring DNSSEC for a Zone-Less DNS Proxy Server Configuration

For a zone-less DNS proxy server configuration, zone signing must be performed on the backend name servers. On the NetScaler ADC, you configure the ADC as a DNS proxy server for the zone. You create a load balancing virtual server of protocol type DNS, configure services on the ADC to represent the name servers, and then bind the services to the load balancing virtual server. For more information about these configuration tasks, see Configuring the NetScaler as a DNS Proxy Server.

When a client sends the ADC a DNS request with the DNSSEC OK (DO) bit set, the ADC checks its cache for the requested information. If the resource records are not available in its cache, the ADC forwards the request to one of the DNS name servers, and then relays the response from the name server to the client. Additionally, the ADC caches the RRSIG resource records along with the response from the name server. Subsequent requests from DNSSEC-aware clients are served from the cache (including the RRSIG resource records), subject to the time-to-live (TTL) parameter. If a client sends a DNS request without setting the DO bit, the ADC responds with only the requested resource records, and does not include the RRSIG resource records that are specific to DNSSEC.

Configuring DNSSEC for a Partial Zone Ownership Configuration

In some NetScaler configurations, even though the authority for a zone lies with the backend name servers, a subset of the resource records that belong to the zone might be configured on the NetScaler ADC. The ADC owns (or is authoritative for) only this subset of records. Such a subset of records can be considered to constitute a *partial zone* on the ADC. The ADC owns the partial zone. All other records are owned by the backend name servers.

A typical partial zone configuration on the NetScaler ADC is seen when global server load balancing (GSLB) domains are configured on the ADC, and the GSLB domains are a part of a zone for which the backend name servers are authoritative.

Signing a zone that includes only a partial zone on the ADC involves including the partial zone information in the backend name server zone files, signing the zone on the backend name servers, and then signing the partial zone on the ADC. The same key set must be used to sign the zone on the name servers and the partial zone on the ADC.

To sign the zone on the backend name servers

1. Include the resource records that are contained in the partial zone, in the zone files of the name servers.

2. Create keys and use the keys to sign the zone on the backend name servers.

To sign the partial zone on the NetScaler ADC

1. Create a zone with the name of the zone that is owned by the backend name servers. When configuring the partial zone, set the proxyMode parameter to YES. This zone is the partial zone that contains the resource records owned by the ADC.

   For example, if the name of the zone that is configured on the backend name servers is example.com, you must create a zone named example.com on the ADC, with the proxyMode parameter set to YES. For more information about adding a zone, see Configuring a DNS Zone.

   Note: Do not add SOA and NS records for the zone. These records should not exist on the ADC for a zone for which the ADC is not authoritative.

2. Import the keys (from one of the backend name servers) to the ADC and then add them to the /nsconfig/dns/ directory. For more information about how you can import a key and add it to the ADC, see Publishing a DNS Key in a Zone.

3. Sign the partial zone with the imported keys. When you sign the partial zone with the keys, the ADC generates RRSIG and NSEC records for the resource record sets and individual resource records in the partial zone, respectively. For more information about signing a zone, see Signing and Unsigning a DNS Zone.

Configuring DNSSEC for GSLB Domain Names

If global server load balancing (GSLB) is configured on the Citrix® NetScaler® ADC and the ADC is authoritative for the zone to which the GSLB domain names belong, all GLSB domain names are signed when the zone is signed. For more information about signing a zone for which the ADC is authoritative, see Configuring DNSSEC When the NetScaler Appliance Is Authoritative for a Zone.

If the GSLB domains belong to a zone for which the backend name servers are authoritative, you must first sign the zone on the name servers, and then sign the partial zone on the ADC to complete the DNSSEC configuration for the zone. For more information, see Configuring DNSSEC for a Partial Zone Ownership Configuration.

Zone Maintenance

From a DNSSEC perspective, zone maintenance involves rolling over Zone Signing Keys and Key Signing Keys when key expiry is imminent. These zone maintenance tasks have to be performed manually. The process of re-signing a zone is performed automatically and does not require manual intervention.

Re-Signing an Updated Zone

When a zone is updated, that is, when new records are added to the zone or existing records are changed, the process of re-signing the new (or modified) record is performed automatically by the Citrix® NetScaler® ADC. If a zone contains multiple Zone Signing Keys, the ADC re-signs the new (or modified) record with the key with which the zone is signed at the point in time when the re-signing is to be performed.

Rolling Over DNSSEC Keys

On the NetScaler ADC, you can use the pre-publish and double signature methods to perform a rollover of the Zone Signing Key and Key Signing Key. More information about these two rollover methods is available in RFC 4641, “DNSSEC Operational Practices.”

The following topics map commands on the ADC to the steps in the rollover procedures discussed in RFC 4641.

The key expiry notification is sent through an SNMP trap called dnskeyExpiry. Three MIB variables, dnskeyName, dnskeyTimeToExpire, and dnskeyUnitsOfExpiry are sent along with the dnskeyExpiry SNMP trap. For more information, see *Citrix NetScaler SNMP OID Reference* at http://support.citrix.com/article/CTX132381.

Pre-Publish Key Rollover

RFC 4641, “DNSSEC Operational Practices” defines four stages for the pre-publish key rollover method: initial, new DNSKEY, new RRSIGs, and DNSKEY removal. Each stage is associated with a set of tasks that you must perform on the ADC. Following are the descriptions of each stage and the tasks that you must perform. The rollover procedure described here can be used for both Key Signing Keys and Zone Signing Keys.

- **Stage 1: Initial.** The zone contains only those key sets with which the zone has currently been signed. The state of the zone in the initial stage is the state of the zone just before you begin the key rollover process.

  Example

  Consider the key, `example.com.zsk1`, with which the zone `example.com` is currently signed. The zone contains only those RRSIGs that were generated by the `example.com.zsk1` key, which is due for expiry. The Key Signing Key is `example.com.ksk1`.

- **Stage 2: New DNSKEY.** A new key is created and published in the zone (that is, the key is added to the ADC), but the zone is not signed with the new key until the pre-roll phase is complete. In this stage, the zone contains the old key, the new key, and the RRSIGs generated by the old key. Publishing the new key for the complete duration of the pre-roll phase gives the DNSKEY resource record (that corresponds to the new key) enough time to propagate to the secondary name servers.

  Example

  A new key `example.com.zsk2` is added to the `example.com` zone. The zone is not signed with `example.com.zsk2` until the pre-roll phase is complete. The example.com zone contains DNSKEY resource records for both `example.com.zsk1` and `example.com.zsk2`.

  NetScaler commands

  Perform the following tasks on the ADC:

- Create a new DNS key by using the create dns key command.

  For more information about creating a DNS key, including an example, see Creating DNS Keys for a Zone.

- Publish the new DNS key in the zone by using the add dns key command.

  For more information about publishing the key in the zone, including an example, see Publishing a DNS Key in a Zone.

- **Stage 3: New RRSIGs.** The zone is signed with the new DNS key and then unsigned with the old DNS key. The old DNS key is not removed from the zone and remains published until the RRSIGs that were generated by the old key expire.

  Example

  The zone is signed with `example.com.zsk2` and then unsigned with `example.com.zsk1`. The zone continues to publish `example.com.zsk1` until the RRSIGs that were generated by `example.com.zsk1` expire.

  NetScaler commands

  Perform the following tasks on the ADC:

  - Sign the zone with the new DNS key by using the sign dns zone command.
  - Unsign the zone with the old DNS key by using the unsign dns zone command.

  For more information about signing and unsigning a zone, including examples, see Signing and Unsigning a DNS Zone.

- **Stage 4: DNSKEY Removal.** When the RRSIGs that were generated by the old DNS key expire, the old DNS key is removed from the zone.

  Example

  The old DNS key `example.com.zsk1` is removed from the `example.com` zone.

  NetScaler commands

  On the ADC, you remove the old DNS key by using the rm dns key command. For more information about removing a key from a zone, including an example, see Removing a DNS Key.

Double Signature Key Rollover

RFC 4641, “DNSSEC Operational Practices” defines three stages for double signature key rollover: initial, new DNSKEY, and DNSKEY removal. Each stage is associated with a set of tasks that you must perform on the ADC. Following are the descriptions of each stage and the tasks that you must perform. The rollover procedure described here can be used for both Key Signing Keys and Zone Signing Keys.

- **Stage 1: Initial.** The zone contains only those key sets with which the zone has currently been signed. The state of the zone in the initial stage is the state of the zone just before you begin the key rollover process.

Example

Consider the key, `example.com.zsk1`, with which the zone `example.com` is currently signed. The zone contains only those RRSIGs that were generated by the `example.com.zsk1` key, which is due for expiry. The Key Signing Key is `example.com.ksk1`.

- **Stage 2: New DNSKEY.** The new key is published in the zone and the zone is signed with the new key. The zone contains the RRSIGs that are generated by the old and the new keys. The minimum duration for which the zone must contain both sets of RRSIGs is the time required for all the RRSIGs to expire.

  Example

  A new key `example.com.zsk2` is added to the `example.com` zone. The zone is signed with `example.com.zsk2`. The `example.com` zone now contains the RRSIGs generated from both keys.

  NetScaler commands

  Perform the following tasks on the ADC:

  - Create a new DNS key by using the create dns key command.

    For more information about creating a DNS key, including an example, see Creating DNS Keys for a Zone.

  - Publish the new key in the zone by using the add dns key command.

    For more information about publishing the key in the zone, including an example, see Publishing a DNS Key in a Zone.

  - Sign the zone with the new key by using the sign dns zone command.

    For more information about signing a zone, including examples, see Signing and Unsigning a DNS Zone.

- **Stage 3: DNSKEY Removal.** When the RRSIGs that were generated by the old DNS key expire, the old DNS key is removed from the zone.

  Example

  The old DNS key `example.com.zsk1` is removed from the `example.com` zone.

  NetScaler commands

  On the ADC, you remove the old DNS key by using the rm dns key command.

  For more information about removing a key from a zone, including an example, see Removing a DNS Key.

Offloading DNSSEC Operations to the NetScaler ADC

For DNS zones for which your DNS servers are authoritative, you can offload DNSSEC operations to the NetScaler ADC. In a DNSSEC offloading deployment, a DNS server sends unsigned responses. The ADC signs the response on the fly before relaying it to the client. The ADC also caches the signed response. Apart from reducing the load on the DNS servers, offloading DNSSEC operations to the ADC gives you the following benefits:

- You can sign records that the DNS servers generate programmatically. Such records cannot be signed by routine zone signing operations performed on the DNS servers.
- You can serve signed responses to clients even if you have not implemented DNSSEC on your servers.

For setting up DNSSEC offloading, you must configure a DNS load balancing virtual server, configure services that represent the DNS servers, and then bind the services to the virtual server. For information about configuring a DNS load balancing virtual server, configuring services, and binding the services to the virtual server, see Configuring a DNS Zone.

You must create a zone entity on the ADC for each DNS zone whose DNSSEC operations you want to offload. For each DNS zone, you must enable the Proxy Mode and DNSSEC Offload parameters. You can optionally configure NSEC record generation for an offloaded zone. To create a DNS zone entity for DNSSEC offloading, follow the instructions in this topic.

To complete the configuration, you must generate DNS keys for the zone, add the keys to the zone, and then sign the zone with the keys. This process is the same as for normal DNSSEC. For information about creating keys, adding keys to a zone, and signing the zone, see Domain Name System Security Extensions.

After you configure DNS offloading, you must flush the DNS cache on the ADC. Flushing the DNS cache ensures that any unsigned records in the cache are removed and subsequently replaced by signed records. For information about flushing the DNS cache, see Enabling Caching of DNS Records.

Note: DNSSEC offloading is supported on all NetScaler MPX platforms, except the NetScaler MPX 9700/10500/12500/15500 FIPS platform. The feature is also supported on NetScaler virtual appliances hosted on NetScaler SDX platforms.

To enable DNSSEC offloading for a zone by using the command line interface

At the command line, type the following commands to enable DNSSEC offloading for a zone and verify the configuration:

- add dns zone <zoneName> -proxyMode YES -dnssecOffload ENABLED [-nsec (ENABLED | DISABLED)

- show dns zone

Example

```
> add dns zone example.com -proxyMode YES -dnssecOffload ENABLED nsec ENABLED
 Done
> show dns zone example.com
    Zone Name : example.com
    Proxy Mode : YES
    DNSSEC Offload: ENABLED    NSEC: ENABLED
 Done
>
```

Parameters for enabling DNSSEC offloading for a zone

dnssecOffload

Offload DNSSEC operations for the DNS zone to the NetScaler appliance.

nsec

Generate NSEC records for the zone. The NetScaler appliance typically includes NSEC records in its response to the client when a DNS server sends an NXDOMAIN or NODATA response. When disabled, the NetScaler appliance does not include NSEC records in its response.

To enable DNSSEC offloading for a zone by using the configuration utility

1. In the navigation pane, expand DNS, and then click Zones.
2. In the details pane, do one of the following:
   - To create a zone on the ADC, click Add.
   - To configure DNSSEC offloading for an existing zone, click the zone, and then click Open.
3. In the Create DNS Zone or Configure DNS Zone dialog box, select the Proxy Mode and DNSSEC Offload check boxes.
4. Optionally, if you want the ADC to generate NSEC records for the zone, select the NSEC check box.
5. Click OK.

Firewall Load Balancing

Firewall load balancing distributes traffic across multiple firewalls, providing fault tolerance and increased throughput. Firewall load balancing protects your network by:

- Dividing the load between the firewalls, which eliminates a single point of failure and allows the network to scale.
- Increasing high availability.

Configuring a NetScaler appliance for firewall load balancing is similar to configuring load balancing, with the exception that the recommended service type is ANY, recommended monitor type is PING, and the load balancing virtual server mode is set to MAC.

You can set up firewall load balancing in a sandwich, an enterprise, or multiple-firewall environment configuration. The sandwich environment is used for load balancing traffic entering the network from outside and traffic leaving the network to the internet and involves configuring two NetScaler appliances, one on each side of a set of firewalls. You configure an enterprise environment for load balancing traffic leaving the network to the internet. The enterprise environment involves configuring a single NetScaler appliance between the internal network and the firewalls that provide access to the Internet. The multiple-firewall environment is used for load balance traffic coming from another firewall. Having firewall load balancing enabled on both the sides of NetScaler improves the traffic flow in both the egress and ingress direction and ensures faster processing of the traffic. The multiple-firewall environment involves configuring a NetScaler appliance sandwiched between two firewalls.

Important: If you configure static routes on the NetScaler for the destination IP address and enable L3 mode, the NetScaler uses its routing table to route the traffic instead of sending the traffic to the load balancing vserver.

Note: For FTP to work, an additional virtual server or service should be configured on the NetScaler with IP address and port as * and 21 respectively, and the service type specified as FTP. In this case, the NetScaler manages the FTP protocol by accepting the FTP control connection, modifying the payload, and managing the data connection, all through the same firewall.

Firewall Load Balancing supports only some of the load balancing methods supported on the NetScaler. Also, you can configure only a few types of persistence and monitors.

Firewall Load Balancing Methods

The following load balancing methods are supported for firewall load balancing.

- Least Connections
- Round Robin
- Least Packets

- Least Bandwidth
- Source IP Hash
- Destination IP Hash
- Source IP Destination IP Hash
- Source IP Source Port hash
- Least Response Time Method (LRTM)
- Custom Load

Firewall Persistence

Only SOURCEIP, DESTIP, and SOURCEIPDESTIP based persistence are supported for firewall load balancing.

Firewall Server Monitoring

Only PING and transparent monitors are supported in firewall load balancing. You can bind a PING monitor (default) to the backend service that represents the firewall. If a firewall is configured not to respond to ping packets, you can configure transparent monitors to monitor hosts on the trusted side through individual firewalls.

Sandwich Environment

A NetScaler deployment in a sandwich mode is capable of load balancing network traffic through firewalls in both directions: ingress (traffic entering the network from the outside, such as the internet) and egress (traffic leaving the network to the internet).

In this setup, a NetScaler is located on each side of a set of firewalls. The NetScaler placed between the firewalls and the Internet, called the *external* NetScaler that handles ingress traffic selects the best firewall, based on the configured method. The NetScaler between the firewalls and the private network, called the *internal* NetScaler tracks the firewall from which the initial packet for a session is received. It then makes sure that all subsequent packets for that session are sent to the same firewall.

The internal NetScaler can be configured as a regular traffic manager to load balance traffic across the private network servers. This configuration also allows traffic originating from the private network (egress) to be load balanced across the firewalls.

The following diagram shows the sandwich firewall load balancing environment.

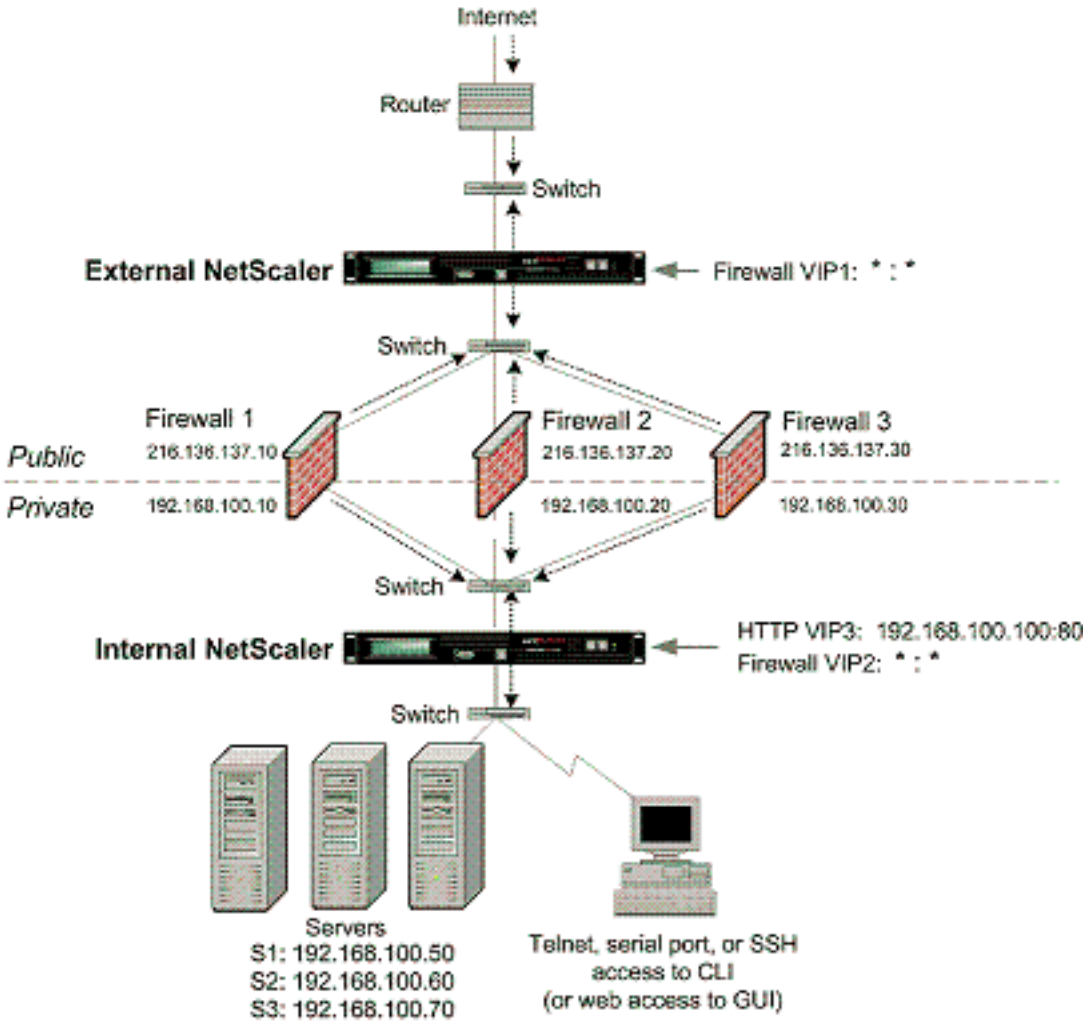


Figure 1. Firewall Load Balancing (Sandwich)

The service type ANY configures the NetScaler to accept all traffic.

To avail benefits related to HTTP and TCP, configure the service and virtual server with type HTTP or TCP. For FTP to work, configure the service with type FTP.

Configuring the External NetScaler in a Sandwich Environment

Perform the following tasks to configure the external NetScaler in a sandwich environment

- Enable the load balancing feature.
- Configure a wildcard service for each firewall.
- Configure a monitor for each wildcard service.
- Configure a wildcard virtual server for traffic coming from the Internet.
- Configure the virtual server in MAC rewrite mode.
- Bind services to the wildcard virtual server.
- Save and Verify the Configuration.

Enable the load balancing feature

To enable load balancing by using the command line interface

At the command prompt, type the following command to enable load balancing and verify the configuration:

- enable ns feature LB
- show ns feature

Example

```
> enable ns feature LoadBalancing
 Done
> show ns feature

      Feature                Acronym          Status
      -------                -------          ------
 1)   Web Logging              WL               OFF
 2)   Surge Protection         SP               ON
 3)   Load Balancing           LB               ON
 .
 .
```

.
24) NetScaler Push push OFF
Done

Configure a wildcard service for each firewall

To configure a wildcard service for each firewall by using the command line interface

At the command prompt, type:

add service <name> <serverName> ANY *

Example

add service Service-HTTP-1 10.102.29.5 ANY *

Parameters for configuring a wildcard service for each firewall

name

Name of the service. This alphanumeric string is required and cannot be changed after the service is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serverName

Either the name of a previously created server object, or the IP address of the load-balanced server, that is associated with this service, in either IPv4 or IPv6 format. When you provide the IP address of the service, a server object is created with this IP address as its name. You can also create a server object manually, and then select the server name instead of an IP address from the drop-down menu that is associated with this field.

If the server is not reachable from the NetScaler or is not active, the service is designated as DOWN.

serviceType

The type of connections that the service will handle. Possible values: HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP, and RTSP. Default: HTTP. For a wildcardservice, specify a service type of ANY.

port

Port on which the service listens. The port number must be a positive number not greater than 65535. For a wildcard service, specify an asterisk (*) as the port number.

Note: For more information about the SSL and SSL_TCP service types, see SSL Offload and Acceleration.

To configure a wildcard service for each firewall by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring a wildcard service for each firewall" as shown:
   - Service Name—name
   - Server—serverName
4. In Protocol, select ANY, and in Port, select *.
5. Click Create, and then click Close. The service you created appears in the Services pane.

Configure a monitor for each wildcard service

A PING monitor is bound by default to the service. You will need to configure a transparent monitor to monitor hosts on the trusted side through individual firewalls. You can then bind the transparent monitor to services. The default PING monitor monitors the connectivity only between the NetScaler appliance and the upstream device. The transparent monitor monitors all the devices existing in the path from the appliance to the device that owns the destination IP address specified in the monitor. If a transparent monitor is not configured and the status of the firewall is UP but one of the next hop devices from that firewall is down, the appliance includes the firewall while performing load balancing and forwards the packet to the firewall. However, the packet is not delivered to the final destination because one of the next hop devices is down. By binding a transparent monitor, if any of the devices (including the firewall) are down, the service is marked as DOWN and the firewall is not included when the appliance performs firewall load balancing.

Binding a transparent monitor will override the PING monitor. To configure a PING monitor in addition to a transparent monitor, after you create and bind a transparent monitor, you need to bind a PING monitor to the service.

To configure a transparent monitor by using the command line interface

At the command prompt, type the following commands to configure a transparent monitor and verify the configuration:

- add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-transparent (YES | NO)]
- bind lb monitor <monitorName> <serviceName>

Example

add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
To bind a PING monitor, type the following command:
bind monitor PING fw-svc1

Parameters for configuring a monitor

monitorName (Name)

The name of the monitor. This is a mandatory argument. Maximum Length: 31.

type (Type)

The type of monitor. This is a mandatory argument. Default: PING.

destIP (Destination IP)

The IP address to which the probe is sent. If the destination IP address is set to 0, the destination IP address is that of the server to which the monitor is bound. Default value: 0

transparent (Transparent)

The state of the monitor for transparent devices, such as firewalls, based on the responsiveness of the services behind them. If the monitoring of transparent devices is enabled, the destination IP address should be specified. The probe is sent to the specified destination IP address using the MAC address of the transparent device. Possible values: YES, NO. Default value: NO

To create and bind a transparent monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. In the details pane, click Add.
3. In the Create Monitor dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a monitor" as shown:
   - Name*
   - Type*
   - Destination IP
   - Transparent

   * A required parameter
4. Click Create, and then click Close. In the Monitors pane, select the monitor that you just configured and verify that the settings displayed at the bottom of the screen are correct.

Configure a wildcard virtual server for traffic coming from the Internet

To configure a wildcard virtual server for traffic coming from the Internet by using the command line interface

At the command prompt, type:

add lb vserver <name> ANY * *

Example

add lb vserver Vserver-LB-1 ANY * *

Parameters for configuring a wildcard virtual server for traffic coming from the Internet

name

Name of the virtual server. This alphanumeric string is required and cannot be changed after the virtual server is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( )

IPAddress

IP address of the virtual server. This IP address can be an IPv4 or IPv6 address, and is usually a public IP address. Clients send connection requests to this IP address.

serviceType

The type of services to which the virtual server distributes requests. Possible values: HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP, and RTSP. Default: HTTP

port

Port on which the virtual server listens for client connections. The port number must be between 0-65535.

To configure a wildcard virtual server for traffic coming from the Internet by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Load Balancing) dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a wildcard virtual server for traffic coming from the Internet” as shown:
   - Name—name
4. In Protocol, select ANY, and in IP Address and Port, select *.
5. Click Create, and then click Close. The virtual server you created appears in the Load Balancing Virtual Servers pane.

Configure the virtual server in MAC rewrite mode

To configure the virtual server in MAC rewrite mode by using the command line interface

At the command prompt, type:

set lb vserver <name>@ -m <RedirectionMode>

Example

set lb vserver Vserver-LB-1 -m MAC

Paarmeter for configuring the virtual server in MAC rewrite mode

m

The load balancing redirection mode. Possible Values: IP, MAC. Default: IP.

If set to IP, the destination IP address of the request is changed to the IP address of the server to which you are redirecting traffic, and the traffic is then forwarded to that server.

If set to MAC, the destination MAC address is changed to the MAC address of the server to which you are redirecting traffic, and the traffic is then forwarded to that server. With this setting, the destination IP address of the traffic is not changed.

To configure the virtual server in MAC rewrite mode by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure the redirection mode (for example, Vserver-LB-1), and then click Open.
3. On the Advanced tab, under Redirection Mode, click MAC-Based.
4. Click OK.

Bind services to the wildcard virtual server

To bind a service to the wildcard virtual server by using the command line interface

At the command prompt, type:

bind lb vserver <name> <serviceName>

Example

bind lb vserver Vserver-LB-1 Service-HTTP-1

To bind a service to the wildcard virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.

2. In the details pane, select the virtual server for which you want to bind the service.
3. Click Open.
4. In the Configure Virtual Server (Load Balancing) dialog box, on the Services tab, select the Active check box next to the service that you want to bind to the virtual server.
5. Click OK.

Note: You can bind a service to multiple virtual servers.

Save and Verify the Configuration

When you've finished the configuration tasks, be sure to save the configuration. You should also check to make sure that the settings are correct.

To save and verify the configuration by using the command line interface

At the command prompt, type the following commands to configure a transparent monitor and verify the configuration:

- save ns config
- show vserver

Example

```
save config
sh lb vserver FWLBVIP1
FWLBVIP1 (*:*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 06:40:14 2010
        Time since last state change: 0 days, 00:00:11.240
        Effective State: UP  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: SRCIPDESTIPHASH
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw_svc_1 (10.102.29.251: *) - ANY State: UP  Weight: 1
2) fw_svc_2 (10.102.29.18: *) - ANY State: UP   Weight: 1
 Done
show service fw-svc1
        fw-svc1 (10.102.29.251:*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 10:04:50 2010
```

```
        Time since last state change: 0 days, 00:00:38.120
        Server Name: 10.102.29.251
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
            State: DOWN     Weight: 1
            Probes: 5       Failed [Total: 5 Current: 5]
            Last response: Failure - Time out during TCP connection establishment stage
            Response Time: 2000.0 millisec
2)      Monitor Name: ping
            State: UP       Weight: 1
            Probes: 3       Failed [Total: 0 Current: 0]
            Last response: Success - ICMP echo reply received.
            Response Time: 1.415 millisec
 Done
```

To save and verify the configuration by using the configuration utility

1. In the details pane, click Save.
2. In the Save Config dialog box, click Yes.
3. In the navigation pane, click Load Balancing, and then click Virtual Servers.
4. In the details pane, select the virtual server that you created in step 5 and verify that the settings displayed in the Details pane are correct.
5. In the navigation pane, click Load Balancing, and then click Services.
6. In the details pane, select the service that you created in step 5 and verify that the settings displayed in the Details pane are correct.

Configuring the Internal NetScaler ADC in a Sandwich Environment

Perform the following tasks to configure the internal NetScaler in a sandwich environment

For traffic from the server (egress)

- Enable the load balancing feature.
- Configure a wildcard service for each firewall.
- Configure a monitor for each wildcard service.
- Configure a wildcard virtual server to load balance the traffic sent to the firewalls.
- Configure the virtual server in MAC rewrite mode.
- Bind firewall services to the wildcard virtual server.

For traffic across private network servers

- Configure a service for each virtual server.
- Configure a monitor for each service.
- Configure an HTTP virtual server to balance traffic sent to the servers.
- Bind HTTP services to the HTTP virtual server.
- Save and Verify the Configuration.

Enable the load balancing feature

You can configure load balancing entities such as services and virtual servers when the load balancing feature is disabled, but they will not function until you enable the feature.

To enable load balancing by using the command line interface

At the command prompt, type the following command to enable load balancing and verify the configuration:

- enable ns feature LB
- show ns feature

Example

```
> enable ns feature LoadBalancing
 Done
> show ns feature

      Feature                 Acronym           Status
      -------                 -------           ------
1)    Web Logging               WL               OFF
2)    Surge Protection          SP               ON
3)    Load Balancing            LB               ON
.
.
.
24)   NetScaler Push            push             OFF
Done
```

To enable load balancing by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features, click Change basic features.
3. In the Configure Basic Features dialog box, select the Load Balancing check box, and then click OK.
4. In the Enable/Disable Feature(s)? message box, click Yes.

Configure a wildcard service for each firewall

To configure a wildcard service for each firewall by using the command line interface

At the command prompt, type:

add service <name> <serverName> ANY *

Example

```
add service Service-HTTP-1 10.102.29.5 ANY *
```

Parameters for configuring a wildcard service for each firewall

name

Name of the service. This alphanumeric string is required and cannot be changed after the service is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serverName

Either the name of a previously created server object, or the IP address of the load-balanced server, that is associated with this service, in either IPv4 or IPv6 format. When you provide the IP address of the service, a server object is created with this IP address as its name. You can also create a server object manually, and then select the server name instead of an IP address from the drop-down menu that is associated with this field.

If the server is not reachable from the NetScaler or is not active, the service is designated as DOWN.

serviceType

The type of connections that the service will handle. Possible values: HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP, and RTSP. Default: HTTP. For a wildcardservice, specify a service type of ANY.

port

Port on which the service listens. The port number must be a positive number not greater than 65535. For a wildcard service, specify an asterisk (*) as the port number.

Note: For more information about the SSL and SSL_TCP service types, see SSL Offload and Acceleration.

To configure a wildcard service for each firewall by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a wildcard service for each firewall” as shown:
   - Service Name—name
   - Server—serverName
4. In Protocol, select ANY, and in Port, select *.
5. Click Create, and then click Close. The service you created appears in the Services pane.

Configure a monitor for each wildcard service

A PING monitor is bound by default to the service. You will need to configure a transparent monitor to monitor hosts on the trusted side through individual firewalls. You can then bind the transparent monitor to services. The default PING monitor monitors the connectivity only between the NetScaler appliance and the upstream device. The transparent monitor monitors all the devices existing in the path from the appliance to the device that owns the destination IP address specified in the monitor. If a transparent monitor is not configured and the status of the firewall is UP but one of the next hop devices from that firewall is down, the appliance includes the firewall while performing load balancing and forwards the packet to the firewall. However, the packet is not delivered to the final destination because one of the next hop devices is down. By binding a transparent monitor, if any of the devices (including the firewall) are down, the service is marked as DOWN and the firewall is not included when the appliance performs firewall load balancing.

Binding a transparent monitor will override the PING monitor. To configure a PING monitor in addition to a transparent monitor, after you create and bind a transparent monitor, you need to bind a PING monitor to the service.

To configure a transparent monitor by using the command line interface

At the command prompt, type the following commands to configure a transparent monitor and verify the configuration:

- add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-transparent (YES | NO)]
- bind lb monitor <monitorName> <serviceName>

Example

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
```

Parameters for configuring a monitor

monitorName (Name)

The name of the monitor. This is a mandatory argument. Maximum Length: 31.

type (Type)

The type of monitor. This is a mandatory argument. Default: PING.

destIP (Destination IP)

The IP address to which the probe is sent. If the destination IP address is set to 0, the destination IP address is that of the server to which the monitor is bound. Default value: 0

transparent (Transparent)

The state of the monitor for transparent devices, such as firewalls, based on the responsiveness of the services behind them. If the monitoring of transparent devices is enabled, the destination IP address should be specified. The probe is sent to the specified destination IP address using the MAC address of the transparent device. Possible values: YES, NO. Default value: NO

To create and bind a transparent monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. In the details pane, click Add.
3. In the Create Monitor dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a monitor", as shown:
   - Name*
   - Type*
   - Destination IP
   - Transparent

   * A required parameter
4. Click Create, and then click Close. In the Monitors pane, select the monitor that you just configured and verify that the settings displayed at the bottom of the screen are correct.

Configure a wildcard virtual server to load balance the traffic sent to the firewalls

To configure a wildcard virtual server to load balance the traffic sent to the firewalls by using the command line interface

At the command prompt, type:

add lb vserver <name> ANY * *

Example

add lb vserver Vserver-LB-1 ANY * *

Parameters for creating a virtual server

name

Name of the virtual server. This alphanumeric string is required and cannot be changed after the virtual server is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( )

IPAddress

IP address of the virtual server. This IP address can be an IPv4 or IPv6 address, and is usually a public IP address. Clients send connection requests to this IP address.

serviceType

The type of services to which the virtual server distributes requests. Possible values: HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP, and RTSP. Default: HTTP

port

Port on which the virtual server listens for client connections. The port number must be between 0-65535.

To configure a wildcard virtual server to load balance the traffic sent to the firewalls by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Load Balancing) dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating a virtual server” as shown:
   - Name—name
4. In Protocol, select ANY, and in IP Address and Port, select *.
5. Click Create, and then click Close. The virtual server you created appears in the Load Balancing Virtual Servers pane.

Configure the virtual server in MAC rewrite mode

To configure the virtual server in MAC rewrite mode by using the command line interface

At the command prompt, type:

set lb vserver <name>@ -m <RedirectionMode>

Example

```
set lb vserver Vserver-LB-1 -m MAC
```

Parameter for configuring the virtual server in MAC rewrite mode

m

The load balancing redirection mode. Possible Values: IP, MAC. Default: IP.

If set to IP, the destination IP address of the request is changed to the IP address of the server to which you are redirecting traffic, and the traffic is then forwarded to that server.

If set to MAC, the destination MAC address is changed to the MAC address of the server to which you are redirecting traffic, and the traffic is then forwarded to that server. With this setting, the destination IP address of the traffic is not changed.

To configure the virtual server in MAC rewrite mode by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure the redirection mode (for example, Vserver-LB-1), and then click Open.
3. On the Advanced tab, under Redirection Mode, click MAC-Based.
4. Click OK.

Bind firewall services to the wildcard virtual server

To bind firewall services to the wildcard virtual server by using the command line interface

At the command prompt, type:

bind lb vserver <name> <serviceName>

Example

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
```

To bind firewall services to the wildcard virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to bind the service.
3. Click Open.
4. In the Configure Virtual Server (Load Balancing) dialog box, on the Services tab, select the Active check box next to the service that you want to bind to the virtual server.
5. Click OK.

Note: You can bind a service to multiple virtual servers.

Configure a service for each virtual server

To configure a service for each virtual server by using the command line interface

At the command prompt, type:

add service <name> <serverName> HTTP <port>

Example

add service Service-HTTP-1 10.102.29.5 HTTP 80

Parameters for configuring a service

name

Name of the service. This alphanumeric string is required and cannot be changed after the service is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serverName

Either the name of a previously-created server object, or the IP address of the load-balanced server, that is associated with this service, in either IPv4 or IPv6 format. When you provide the IP address of the service, a server object is created with this IP address as its name. You can also create a server object manually, and then select the server name instead of an IP address from the drop-down menu that is associated with this field.

If the server is not reachable from the NetScaler or is not active, the service is designated as DOWN.

serviceType

The type of connections that the service will handle. Possible values: HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP, and RTSP. Default: HTTP

port

Port on which the service listens. The port number must be a positive number not greater than 65535.

Note: For more information about the SSL and SSL_TCP service types, see SSL Offload and Acceleration.

To configure a service for each virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating a service” as shown:
   - Service Name—name
   - Server—serverName
   - Port—port
4. In Protocol, specify HTTP. Under Available Monitors, select HTTP.
5. Click Create, and then click Close. The service you created appears in the Services pane.

Configure a monitor for each service

To bind a monitor to a service by using the command line interface

At the command prompt, type:

bind lb monitor <monitorName> <ServiceName>

Example

bind mon monitor-HTTP-1 Service-HTTP-1

To bind a monitor to a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to bind the monitor (for example, Service-HTTP-1), and then click Open.
3. On the Monitors tab, in the Available list box, select the monitor you want to bind the service (for example, monitor-HTTP-1), and then click Add.
4. In the Configured box, click OK.

Configure an HTTP virtual server to balance traffic sent to the servers

To configure an HTTP virtual server to balance traffic sent to the servers by using the command line interface

At the command prompt, type:

add lb vserver <name> HTTP <ip> <port>

Example

add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80

Parameters for creating a virtual server

name

Name of the virtual server. This alphanumeric string is required and cannot be changed after the virtual server is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( )

IPAddress

IP address of the virtual server. This IP address can be an IPv4 or IPv6 address, and is usually a public IP address. Clients send connection requests to this IP address.

serviceType

The type of services to which the virtual server distributes requests. Possible values: HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP, and RTSP. Default: HTTP

port

Port on which the virtual server listens for client connections. The port number must be between 0-65535.

To configure an HTTP virtual server to balance traffic sent to the servers by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Load Balancing) dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating a virtual server” as shown:
   - Name—name
   - IP Address—IPAddress

     Note: If the virtual server uses IPv6, select the IPv6 check box and enter the address in IPv6 format (for example, **1000:0000:0000:0000:0005:0600:700a:888b**).
   - Port—port
4. Under Protocol, select HTTP.
5. Click Create, and then click Close. The virtual server you created appears in the Load Balancing Virtual Servers pane.

Bind HTTP services to the HTTP virtual server

To bind HTTP services to the wildcard virtual server by using the command line interface

At the command prompt, type:

bind lb vserver <name> <serviceName>

Example

bind lb vserver Vserver-LB-1 Service-HTTP-1

To bind HTTP services to the wildcard virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.

2. In the details pane, select the virtual server for which you want to bind the service.
3. Click Open.
4. In the Configure Virtual Server (Load Balancing) dialog box, on the Services tab, select the Active check box next to the service that you want to bind to the virtual server.
5. Click OK.

Note: You can bind a service to multiple virtual servers.

Save and Verify the Configuration

When you've finished the configuration tasks, be sure to save the configuration. You should also check to make sure that the settings are correct.

To save and verify the configuration by using the command line interface

At the command prompt, type the following commands to configure a transparent monitor and verify the configuration:

- save ns config
- show vserver

Example

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (*:*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
2) fw-int-svc2 (10.102.29.9: *) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:*) - ANY
        State: DOWN
```

```
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 10.102.29.5
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
            State: DOWN     Weight: 1
            Probes: 9       Failed [Total: 9 Current: 9]
            Last response: Failure - Time out during TCP connection establishment stage
            Response Time: 2000.0 millisec
2)      Monitor Name: ping
            State: UP       Weight: 1
            Probes: 3       Failed [Total: 0 Current: 0]
            Last response: Success - ICMP echo reply received.
            Response Time: 1.275 millisec
 Done
```

To save and verify the configuration by using the configuration utility

1. In the details pane, click Save.
2. In the Save Config dialog box, click Yes.
3. In the navigation pane, click Load Balancing, and then click Virtual Servers.
4. In the details pane, select the virtual server that you created in step 5 and verify that the settings displayed in the Details pane are correct.
5. In the navigation pane, click Load Balancing, and then click Services.
6. In the details pane, select the service that you created in step 5 and verify that the settings displayed in the Details pane are correct.

Monitoring a Firewall Load Balancing Setup in a Sandwich Environment

After the configuration is up and running, you should view the statistics for each service and virtual server to check for possible problems.

Viewing the Statistics of a Virtual Server

To evaluate the performance of virtual servers or to troubleshoot problems, you can display details of the virtual servers configured on the NetScaler appliance. You can display a summary of statistics for all the virtual servers, or you can specify the name of a virtual server to display the statistics only for that virtual server. You can display the following details:

- Name
- IP address
- Port
- Protocol
- State of the virtual server
- Rate of requests received
- Rate of hits

To display virtual server statistics by using the command line interface

To display a summary of the statistics for all the virtual servers currently configured on the NetScaler, or for a single virtual server, at the command prompt, type:

stat lb vserver [-detail] [<name>]

Example

```
>stat lb vserver -detail
Virtual Server(s) Summary
                vsvrIP  port    Protocol      State   Req/s  Hits/s
One                *    80       HTTP         UP      5/s     0/s
Two                *     0       TCP         DOWN     0/s     0/s
Three              *  2598        TCP        DOWN     0/s     0/s
dnsVirtualNS   10.102.29.90   53        DNS        DOWN     0/s     0/s
```

```
BRVSERV          10.10.1.1    80        HTTP         DOWN      0/s      0/s
LBVIP         10.102.29.66    80        HTTP           UP      0/s      0/s
 Done
```

Parameters for displaying statistics

detail

Include the statistics for hits per second and the total number of hits.

name

Name of the virtual server whose statistics are displayed.

To display virtual server statistics by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. If you want to display the statistics for only one virtual server, in the details pane, select the virtual server whose statistics you want to display.
3. In the details pane, click Statistics.

Viewing the Statistics of a Service

You can view the rate of requests, responses, request bytes, response bytes, current client connections, requests in surge queue, current server connections, and so forth using the service statistics.

To view the statistics of a service by using the command line interface

At the command prompt, type:

stat service <name>

Example

stat service Service-HTTP-1

To view the statistics of a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service whose statistics you want to view (for example, Service-HTTP-1).
3. Click Statistics. The statistics appear in a new window.

Enterprise Environment

In the enterprise setup, the NetScaler is placed between the firewalls connecting to the public Internet and the internal private network and handles egress traffic. The NetScaler selects the best firewall based on the configured load balancing policy.

The following diagram shows the enterprise firewall load balancing environment

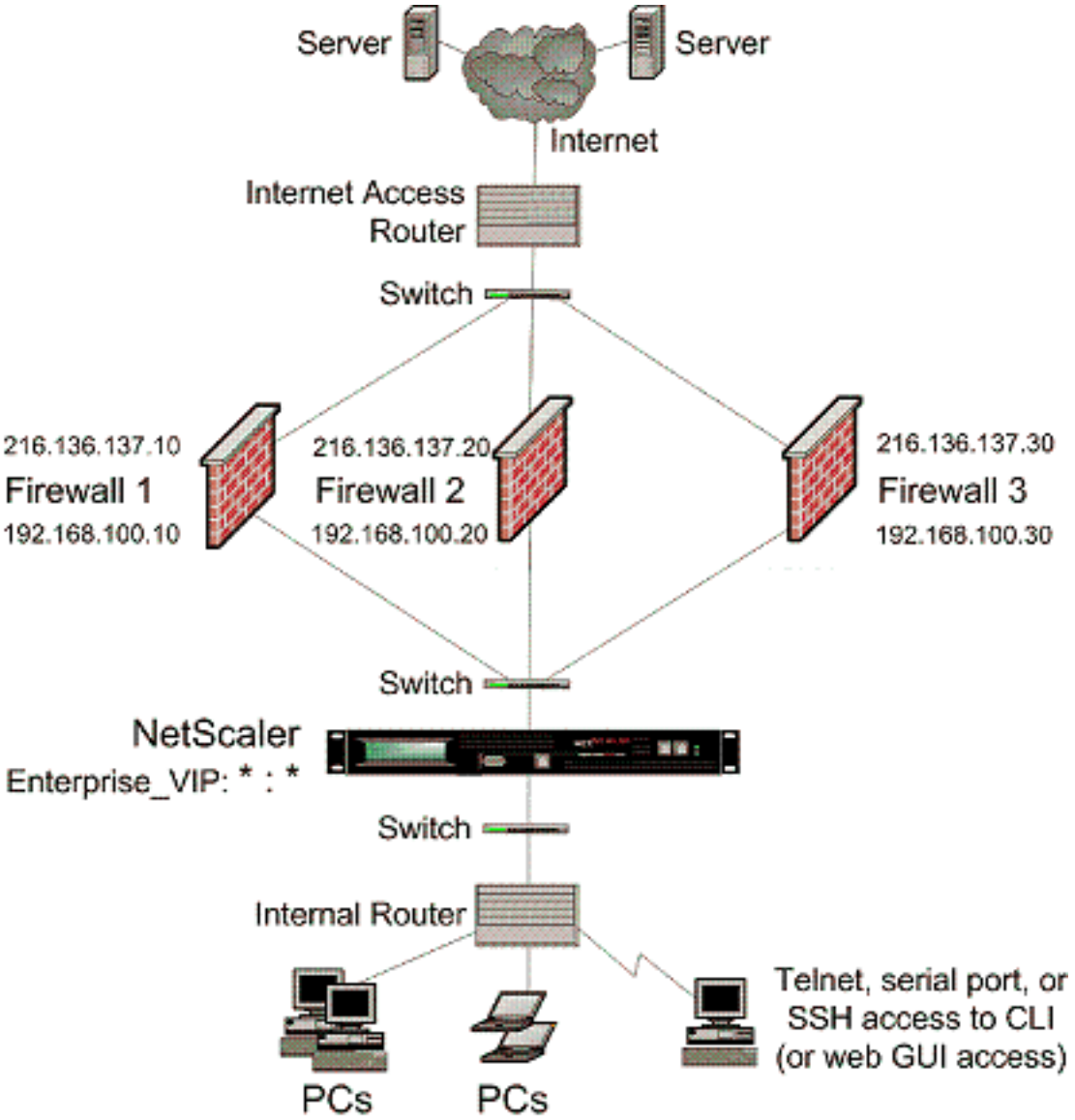


Figure 1. Firewall Load Balancing (Enterprise)

The service type ANY configures the NetScaler to accept all traffic.

To avail benefits related to HTTP and TCP, configure the service and vserver with type HTTP or TCP. For FTP to work, configure the service with type FTP.

Configuring the NetScaler in an Enterprise Environment

Perform the following tasks to configure a NetScaler in an enterprise environment.

For traffic from the server (egress)

- Enable the load balancing feature.
- Configure a wildcard service for each firewall.
- Configure a monitor for each wildcard service.
- Configure a wildcard virtual server to load balance the traffic sent to the firewalls.
- Configure the virtual server in MAC rewrite mode.
- Bind firewall services to the wildcard virtual server.

For traffic across private network servers

- Configure a service for each virtual server.
- Configure a monitor for each service.
- Configure an HTTP virtual server to balance traffic sent to the servers.
- Bind HTTP services to the HTTP virtual server.
- Save and Verify the Configuration.

Enable the load balancing feature

You can configure load balancing entities such as services and virtual servers when the load balancing feature is disabled, but they will not function until you enable the feature.

To enable load balancing by using the command line interface

At the command prompt, type the following command to enable load balancing and verify the configuration:

- enable ns feature LB
- show ns feature

Example

```
> enable ns feature LoadBalancing
 Done
> show ns feature

      Feature                 Acronym           Status
      -------                 -------           ------
1)    Web Logging               WL              OFF
2)    Surge Protection          SP              ON
3)    Load Balancing            LB              ON
.
.
.
24)   NetScaler Push            push            OFF
Done
```

To enable load balancing by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features, click Change basic features.
3. In the Configure Basic Features dialog box, select the Load Balancing check box, and then click OK.
4. In the Enable/Disable Feature(s)? message box, click Yes.

Configure a wildcard service for each firewall

To configure a wildcard service for each firewall by using the command line interface

At the command prompt, type:

add service <name> <serverName> ANY *

Example

```
add service Service-HTTP-1 10.102.29.5 ANY *
```

Parameters for configuring wildcard service for each firewall

name

Name of the service. This alphanumeric string is required and cannot be changed after the service is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serverName

Either the name of a previously created server object, or the IP address of the load-balanced server, that is associated with this service, in either IPv4 or IPv6 format. When you provide the IP address of the service, a server object is created with this IP address as its name. You can also create a server object manually, and then select the server name instead of an IP address from the drop-down menu that is associated with this field.

If the server is not reachable from the NetScaler or is not active, the service is designated as DOWN.

serviceType

The type of connections that the service will handle. Possible values: HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP, and RTSP. Default: HTTP. For a wildcardservice, specify a service type of ANY.

port

Port on which the service listens. The port number must be a positive number not greater than 65535. For a wildcard service, specify an asterisk (*) as the port number.

Note: For more information about the SSL and SSL_TCP service types, see SSL Offload and Acceleration.

To configure a wildcard service for each firewall by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a wildcard service for each firewall” as shown:
   - Service Name—name
   - Server—serverName
4. In Protocol, select ANY, and in Port, select *.
5. Click Create, and then click Close. The service you created appears in the Services pane.

Configure a monitor for each wildcard service

A PING monitor is bound by default to the service. You will need to configure a transparent monitor to monitor hosts on the trusted side through individual firewalls. You can then bind the transparent monitor to services. The default PING monitor monitors the connectivity only between the NetScaler appliance and the upstream device. The transparent monitor monitors all the devices existing in the path from the appliance to the device that owns the destination IP address specified in the monitor. If a transparent monitor is not configured and the status of the firewall is UP but one of the next hop devices from that firewall is down, the appliance includes the firewall while performing load balancing and forwards the packet to the firewall. However, the packet is not delivered to the final destination because one of the next hop devices is down. By binding a transparent monitor, if any of the devices (including the firewall) are down, the service is marked as DOWN and the firewall is not included when the appliance performs firewall load balancing.

Binding a transparent monitor will override the PING monitor. To configure a PING monitor in addition to a transparent monitor, after you create and bind a transparent monitor, you need to bind a PING monitor to the service.

To configure a transparent monitor by using the command line interface

At the command prompt, type the following commands to configure a transparent monitor and verify the configuration:

- add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-transparent (YES | NO)]
- bind lb monitor <monitorName> <serviceName>

Example

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
```

Parameters for configuring a monitor

monitorName (Name)

The name of the monitor. This is a mandatory argument. Maximum Length: 31.

type (Type)

The type of monitor. This is a mandatory argument. Default: PING.

destIP (Destination IP)

The IP address to which the probe is sent. If the destination IP address is set to 0, the destination IP address is that of the server to which the monitor is bound. Default value: 0

transparent (Transparent)

The state of the monitor for transparent devices, such as firewalls, based on the responsiveness of the services behind them. If the monitoring of transparent devices is enabled, the destination IP address should be specified. The probe is sent to the specified destination IP address using the MAC address of the transparent device. Possible values: YES, NO. Default value: NO

To create and bind a transparent monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. In the details pane, click Add.
3. In the Create Monitor dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a monitor, as shown:
   - Name*
   - Type*—type
   - Destination IP
   - Transparent

   * A required parameter
4. Click Create, and then click Close. In the Monitors pane, select the monitor that you just configured and verify that the settings displayed at the bottom of the screen are correct.

Configure a wildcard virtual server to load balance the traffic sent to the firewalls

To configure a wildcard virtual server to load balance the traffic sent to the firewalls by using the command line interface

At the command prompt, type:

add lb vserver <name> ANY * *

Example

add lb vserver Vserver-LB-1 ANY * *

Paarmeters for creatinga virtual server

name

Name of the virtual server. This alphanumeric string is required and cannot be changed after the virtual server is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( )

IPAddress

IP address of the virtual server. This IP address can be an IPv4 or IPv6 address, and is usually a public IP address. Clients send connection requests to this IP address.

serviceType

The type of services to which the virtual server distributes requests. Possible values: HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP, and RTSP. Default: HTTP

port

Port on which the virtual server listens for client connections. The port number must be between 0-65535.

To configure a wildcard virtual server to load balance the traffic sent to the firewalls by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Load Balancing) dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating a virtual server” as shown:
   - Name—name
4. In Protocol, select ANY, and in IP Address and Port, select *.
5. Click Create, and then click Close. The virtual server you created appears in the Load Balancing Virtual Servers pane.

Configure the virtual server in MAC rewrite mode

To configure the virtual server in MAC rewrite mode by using the command line interface

At the command prompt, type:

set lb vserver <name>@ -m <RedirectionMode>

Example

```
set lb vserver Vserver-LB-1 -m MAC
```

Parameter for configuring the virtual server in MAC rewrite mode

m

The load balancing redirection mode. Possible Values: IP, MAC. Default: IP.

If set to IP, the destination IP address of the request is changed to the IP address of the server to which you are redirecting traffic, and the traffic is then forwarded to that server.

If set to MAC, the destination MAC address is changed to the MAC address of the server to which you are redirecting traffic, and the traffic is then forwarded to that server. With this setting, the destination IP address of the traffic is not changed.

To configure the virtual server in MAC rewrite mode by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure the redirection mode (for example, Vserver-LB-1), and then click Open.
3. On the Advanced tab, under Redirection Mode, click MAC-Based.
4. Click OK.

Bind firewall services to the wildcard virtual server

To bind firewall services to the wildcard virtual server by using the command line interface

At the command prompt, type:

bind lb vserver <name> <serviceName>

Example

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
```

To bind firewall services to the wildcard virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to bind the service.
3. Click Open.
4. In the Configure Virtual Server (Load Balancing) dialog box, on the Services tab, select the Active check box next to the service that you want to bind to the virtual server.
5. Click OK.

Note: You can bind a service to multiple virtual servers.

Configure a service for each virtual server

To configure a service for each virtual server by using the command line interface

At the command prompt, type:

add service <name> <serverName> HTTP <port>

Example

add service Service-HTTP-1 10.102.29.5 HTTP 80

Parameters for configuring a srvice

name

Name of the service. This alphanumeric string is required and cannot be changed after the service is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serverName

Either the name of a previously-created server object, or the IP address of the load-balanced server, that is associated with this service, in either IPv4 or IPv6 format. When you provide the IP address of the service, a server object is created with this IP address as its name. You can also create a server object manually, and then select the server name instead of an IP address from the drop-down menu that is associated with this field.

If the server is not reachable from the NetScaler or is not active, the service is designated as DOWN.

serviceType

The type of connections that the service will handle. Possible values: HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP, and RTSP. Default: HTTP

port

Port on which the service listens. The port number must be a positive number not greater than 65535.

Note: For more information about the SSL and SSL_TCP service types, see SSL Offload and Acceleration.

To configure a service for each virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating a service” as shown:
   - Service Name—name
   - Server—serverName
   - Port—port
4. In Protocol, specify HTTP. Under Available Monitors, select HTTP.
5. Click Create, and then click Close. The service you created appears in the Services pane.

Configure a monitor for each service

To bind a monitor to a service by using the command line interface

At the command prompt, type:

bind lb monitor <monitorName> <ServiceName>

Example

bind mon monitor-HTTP-1 Service-HTTP-1

To bind a monitor to a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to bind the monitor (for example, Service-HTTP-1), and then click Open.
3. On the Monitors tab, in the Available list box, select the monitor you want to bind the service (for example, monitor-HTTP-1), and then click Add.
4. In the Configured box, click OK.

Configure an HTTP virtual server to balance traffic sent to the servers

To configure an HTTP virtual server to balance traffic sent to the servers by using the command line interface

At the command prompt, type:

add lb vserver <name> HTTP <ip> <port>

Example

add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80

Parameters for creating a virtual server

name

Name of the virtual server. This alphanumeric string is required and cannot be changed after the virtual server is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( )

IPAddress

IP address of the virtual server. This IP address can be an IPv4 or IPv6 address, and is usually a public IP address. Clients send connection requests to this IP address.

serviceType

The type of services to which the virtual server distributes requests. Possible values: HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP, and RTSP. Default: HTTP

port

Port on which the virtual server listens for client connections. The port number must be between 0-65535.

To configure an HTTP virtual server to balance traffic sent to the servers by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Load Balancing) dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating a virtual server” as shown:
   - Name—name
   - IP Address—IPAddress

     Note: If the virtual server uses IPv6, select the IPv6 check box and enter the address in IPv6 format (for example, **1000:0000:0000:0000:0005:0600:700a:888b**).
   - Port—port
4. Under Protocol, select HTTP.
5. Click Create, and then click Close. The virtual server you created appears in the Load Balancing Virtual Servers pane.

Bind HTTP services to the HTTP virtual server

To bind HTTP services to the wildcard virtual server by using the command line interface

At the command prompt, type:

bind lb vserver <name> <serviceName>

Example

bind lb vserver Vserver-LB-1 Service-HTTP-1

To bind HTTP services to the wildcard virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.

2. In the details pane, select the virtual server for which you want to bind the service.
3. Click Open.
4. In the Configure Virtual Server (Load Balancing) dialog box, on the Services tab, select the Active check box next to the service that you want to bind to the virtual server.
5. Click OK.

Note: You can bind a service to multiple virtual servers.

Save and Verify the Configuration

When you've finished the configuration tasks, be sure to save the configuration. You should also check to make sure that the settings are correct.

To save and verify the configuration by using the command line interface

At the command prompt, type the following commands to configure a transparent monitor and verify the configuration:

- save ns config
- show vserver

Example

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (*:*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
2) fw-int-svc2 (10.102.29.9: *) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:*) - ANY
        State: DOWN
```

```
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 10.102.29.5
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
            State: DOWN     Weight: 1
            Probes: 9       Failed [Total: 9 Current: 9]
            Last response: Failure - Time out during TCP connection establishment stage
            Response Time: 2000.0 millisec
2)      Monitor Name: ping
            State: UP       Weight: 1
            Probes: 3       Failed [Total: 0 Current: 0]
            Last response: Success - ICMP echo reply received.
            Response Time: 1.275 millisec
 Done
```

To save and verify the configuration by using the configuration utility

1. In the details pane, click Save.
2. In the Save Config dialog box, click Yes.
3. In the navigation pane, click Load Balancing, and then click Virtual Servers.
4. In the details pane, select the virtual server that you created in step 5 and verify that the settings displayed in the Details pane are correct.
5. In the navigation pane, click Load Balancing, and then click Services.
6. In the details pane, select the service that you created in step 5 and verify that the settings displayed in the Details pane are correct.

Monitoring a Firewall Load Balancing Setup in an Enterprise Environment

After the configuration is up and running, you should view the statistics for each service and virtual server to check for possible problems.

Viewing the Statistics of a Virtual Server

To evaluate the performance of virtual servers or to troubleshoot problems, you can display details of the virtual servers configured on the NetScaler appliance. You can display a summary of statistics for all the virtual servers, or you can specify the name of a virtual server to display the statistics only for that virtual server. You can display the following details:

- Name
- IP address
- Port
- Protocol
- State of the virtual server
- Rate of requests received
- Rate of hits

To display virtual server statistics by using the command line interface

To display a summary of the statistics for all the virtual servers currently configured on the NetScaler, or for a single virtual server, at the command prompt, type:

stat lb vserver [-detail] [<name>]

Example

```
>stat lb vserver -detail
Virtual Server(s) Summary
                vsvrIP  port    Protocol      State   Req/s  Hits/s
One                *    80       HTTP         UP      5/s     0/s
Two                *     0        TCP        DOWN     0/s     0/s
Three              *  2598        TCP        DOWN     0/s     0/s
dnsVirtualNS   10.102.29.90   53        DNS        DOWN     0/s     0/s
```

```
BRVSERV          10.10.1.1    80        HTTP        DOWN      0/s      0/s
LBVIP         10.102.29.66    80        HTTP          UP      0/s      0/s
 Done
```

Parameters for displaying statistics

detail

Include the statistics for hits per second and the total number of hits.

name

Name of the virtual server whose statistics are displayed.

To display virtual server statistics by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. If you want to display the statistics for only one virtual server, in the details pane, select the virtual server whose statistics you want to display.
3. In the details pane, click Statistics.

Viewing the Statistics of a Service

You can view the rate of requests, responses, request bytes, response bytes, current client connections, requests in surge queue, current server connections, and so forth using the service statistics.

To view the statistics of a service by using the command line interface

At the command prompt, type:

stat service <name>

Example

stat service Service-HTTP-1

To view the statistics of a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service whose statistics you want to view (for example, Service-HTTP-1).
3. Click Statistics. The statistics appear in a new window.

Multiple-Firewall Environment

Note: This feature is available in NetScaler release 9.3.e and 10.

In a multiple-firewall environment, the NetScaler appliance is placed between two sets of firewalls, the external set connecting to the public Internet, and the internal set connecting to the internal private network. The external set typically handles the egress traffic. These firewalls mainly implement access control lists to allow or deny access to external resources. The internal set typically handles the ingress traffic. These firewalls implement security to safeguard the intranet from malicious attacks apart from load-balancing the ingress traffic. The multiple-firewall environment allows you to load-balance traffic coming from another firewall. By default, the traffic coming from a firewall is not load balanced on the other firewall across a NetScaler. Having firewall load balancing enabled on both the sides of NetScaler improves the traffic flow in both the egress and ingress direction and ensures faster processing of the traffic.

Figure 1 shows a multiple-firewall load balancing environment

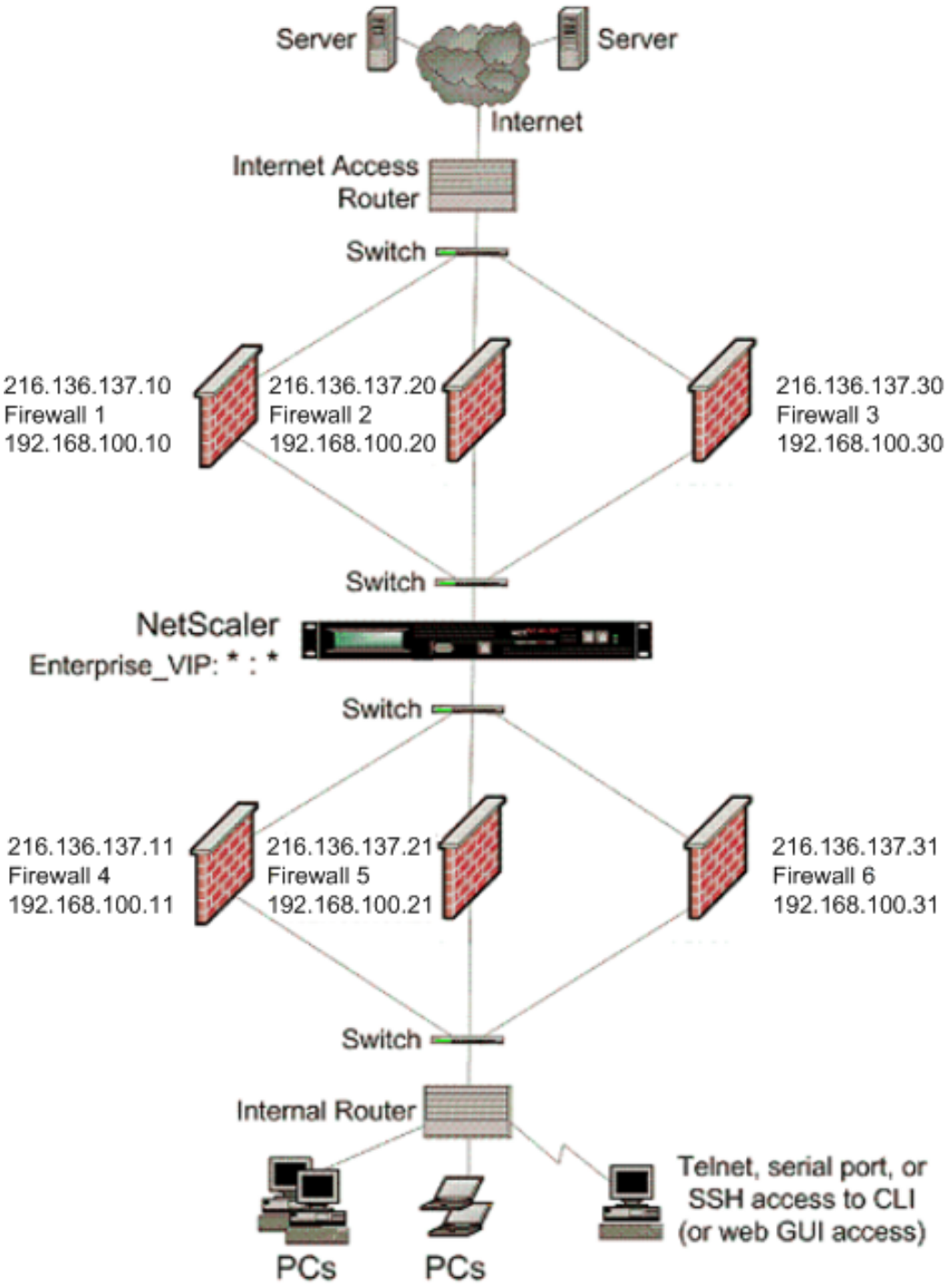


Figure 1. Firewall Load Balancing (multiple-firewall)

With a configuration like the one shown in Figure 1, you can configure the NetScaler to load balance the traffic through the an internal firewall even if it is load balanced by an external firewall. For example, with this feature configured, the traffic coming from the external firewalls (firewalls 1, 2, and 3) is load balanced on the internal firewalls (firewalls 4, 5, and 6) and vice versa.

Firewall load balancing is supported only for MAC mode LB virtual server.

The service type ANY configures the NetScaler to accept all traffic.

To avail benefits related to HTTP and TCP, configure the service and virtual server with type HTTP or TCP. For FTP to work, configure the service with type FTP.

Configuring the NetScaler in a Multiple-Firewall Environment

To configure a NetScaler appliance in a multiple-firewall environment, you have to enable the load balancing feature, configure a virtual server to load balance the egress traffic across the external firewalls, configure a virtual server to load balance the ingress traffic across the internal firewalls, and enable firewall load balancing on the NetScaler. To configure a virtual server to load balance traffic across a firewall in the multiple-firewall environment, you need to:

1. Configure a wildcard service for each firewall
2. Configure a monitor for each wildcard service
3. Configure a wildcard virtual server to load balance the traffic sent to the firewalls
4. Configure the virtual server in MAC rewrite mode
5. Bind firewall services to the wildcard virtual server

Enabling the load balancing feature

To configure and implement load balancing entities such as services and virtual servers, you need to enable the load balancing feature on the NetScaler device.

To enable load balancing by using the command line interface

At the command prompt, type the following command to enable load balancing and verify the configuration:

- enable ns feature <featureName>
- show ns feature

Example

```
enable ns feature LoadBalancing
Done
show ns feature
Feature Acronym Status
------- ------- ------
1) Web Logging WL OFF
2) Surge Protection SP ON
3) Load Balancing LB ON
```

.
.
.
24) NetScaler Push push OFF
Done

Parameters for enabling load balancing

featureName (Name)

The name of the feature you want to enable. This is a mandatory argument.

To enable load balancing by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the Settings pane, under Modes and Features, click Change basic features.
3. In the Configure Basic Features dialog box, select the Load Balancing check box, and then click Ok.

Configuring a wildcard service for each firewall

To accept traffic from all the protocols, you need to configure wildcard service for each firewall by specifying support for all the protocols and ports.

To configure a wildcard service for each firewall by using the command line interface

At the command prompt, type the following command to configure support for all the protocols and ports:

add service <name>@ <serverName> <serviceType> <port_number>

Example

add service fw-svc1 10.102.29.5 ANY *

Parameters for configuring a wildcard service for each firewall

service_name

Name of the service. This alphanumeric string is required and cannot be changed after the service is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - .(period) : (colon) # and space ( ).

serverName

Either the name of a previously created server object, or the IP address of the load-balanced server, that is associated with this service, in either IPv4 or IPv6 format. When you provide the IP address of the service, a server object is created with this IP address as its name. You can also create a server object manually, and then select the server name instead of an IP address from the drop-down menu that is associated with this field. If the server is not reachable from the NetScaler or is not active, the service is designated as DOWN.

serviceType

The type of connections that the service will handle. Possible values: HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP, and RTSP. Default: HTTP. For a wildcardservice, specify the service type as ANY.

port

Port on which the service listens. The port number must be a positive number not greater than 65535. For a wildcard service, specify an asterisk (*) as the port number.

Note: For more information about the SSL and SSL_TCP service types, see SSL Offload and Acceleration.

To configure a wildcard service for each firewall by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add.
3. In the Create Services dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a wildcard service for each firewall", as shown:
   - Service Name—name
   - Server—serverName

   * A required parameter
4. In Protocol, select Any and in Port, select *.
5. Click Create, and then click Close. The service you created appears in the Services pane.

Configuring a monitor for each service

A PING monitor is bound by default to the service. You will need to configure a transparent monitor to monitor hosts on the trusted side through individual firewalls. You can then bind the transparent monitor to services. The default PING monitor monitors the connectivity only between the NetScaler appliance and the upstream device. The transparent monitor monitors all the devices existing in the path from the appliance to the device that owns the destination IP address specified in the monitor. If a transparent monitor is not configured and the status of the firewall is UP but one of the next hop devices from that firewall is down, the appliance includes the firewall while performing load balancing and forwards the packet to the firewall. However, the packet is not delivered to the final destination because one of the next hop devices is down. By binding a transparent monitor, if any of the devices (including the firewall) are down, the service is marked as DOWN and the firewall is not included when the appliance performs firewall load balancing.

Binding a transparent monitor will override the PING monitor. To configure a PING monitor in addition to a transparent monitor, after you create and bind a transparent monitor, you need to bind a PING monitor to the service.

To configure a transparent monitor by using the command line interface

At the command prompt, type the following commands to configure a transparent monitor and verify the configuration:

- add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-transparent (YES | NO)]
- bind lb monitor <monitorName> <serviceName>

Example

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
```

Parameters for configuring a monitor

monitorName (Name)

The name of the monitor. This is a mandatory argument. Maximum Length: 31.

type (Type)

The type of monitor. This is a mandatory argument. Default: PING.

destIP (Destination IP)

The IP address to which the probe is sent. If the destination IP address is set to 0, the destination IP address is that of the server to which the monitor is bound. Default value: 0

transparent (Transparent)

The state of the monitor for transparent devices, such as firewalls, based on the responsiveness of the services behind them. If the monitoring of transparent devices is enabled, the destination IP address should be specified. The probe is sent to the specified destination IP address using the MAC address of the transparent device. Possible values: YES, NO. Default value: NO

To create and bind a transparent monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. In the details pane, click Add.
3. In the Create Monitor dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a monitor, as shown:
   - Name*
   - Type*—type
   - Destination IP
   - Transparent

   * A required parameter
4. Click Create, and then click Close. In the Monitors pane, select the monitor that you just configured and verify that the settings displayed at the bottom of the screen are correct.

Configuring a virtual server to load balance the traffic sent to the firewalls

To load balance any kind of traffic, you need to configure a wildcard virtual server specifying the protocol and port as any value.

To configure a virtual server to load balance the traffic sent to the firewalls by using the command line interface

At the command prompt, type the following command:

add lb vserver <name>@ <serviceType> <IPAddress> <port_number>

Example

add lb vserver Vserver-LB-1 ANY * *

Parameters for creating a virtual server

name

Name of the virtual server. This alphanumeric string is required and cannot be changed after the virtual server is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serviceType

The type of services to which the virtual server distributes requests. Possible values: HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP, and RTSP. Default: HTTP.

IPAddress

IP address of the virtual server. This IP address can be an IPv4 or IPv6 address, and is usually a public IP address. Clients send connection requests to this IP address.

port

Port on which the virtual server listens for client connections. The port number must be between 0-65535.

To configure a virtual server to load balance the traffic sent to the firewalls by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Load Balancing) dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating a virtual server", as shown:
   - Name—name
4. In Protocol, select Any, and in IP Address and Port, select *.
5. Click Create, and then click Close. The virtual server you created appears in the Load Balancing Virtual Servers pane.

Configuring the virtual server to MAC rewrite mode

To configure the virtual server to use MAC address for forwarding the incoming traffic, you need to enable the MAC rewrite mode.

To configure the virtual server in MAC rewrite mode by using the command line interface

At the command prompt, type the following command:

set lb vserver <name>@ -m <RedirectionMode>

Example

set lb vserver Vserver-LB-1 -m MAC

Parameters for creating a virtual server

m

The load balancing redirection mode. Possible values are IP, IPTUNNEL, TOS, MAC. Default: IP.

If set to IP, the destination IP address of the request is changed to the IP address of the server to which you are redirecting traffic, and the traffic is then forwarded to that server.

If set to MAC, the destination MAC address is changed to the MAC address of the server to which you are redirecting traffic, and the traffic is then forwarded to that server. With this setting, the destination IP address of the traffic is not changed.

If set to IPTUNNEL, NetScaler uses an IP tunnel to communicate to the server.

If set to TOS, NetScaler uses the TOS id to communicate to the server.

To configure the virtual server in MAC rewrite mode by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure the redirection mode (for example, Vserver-LB1), and then click Open.
3. On the Advanced tab, under the Redirection Mode mode, click Open.
4. Click Ok.

Binding firewall services to the virtual server

To access a service on NetScaler, you need to bind it to a wildcard virtual server.

To bind firewall services to the virtual server by using the command line interface

At the command prompt, type the following command:

bind lb vserver <name>@ <serviceName>

Example

bind lb vserver Vserver-LB-1 Service-HTTP-1

To bind firewall services to the virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure the redirection mode (for example, Vserver-LB1), and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, on the Services tab, select the Active check box next to the service that you want to bind to the virtual server(for example, Service-HTTP-1).
4. Click Ok.

Configuring the multiple-firewall load balancing on the NetScaler Appliance

To load balance traffic on both the sides of a NetScaler using firewall load balancing, you need to enable mulitpl-firewall load balancing by using the vServerSpecificMac parameter.

To configure multiple-firewall load balancing by using the command line interface

At the command prompt, type the following command:

set lb parameter -vServerSpecificMac <status>

Example

set lb parameter -vServerSpecificMac ENABLED

Parameters for configuring multiple-firewall load balancing

vServerSpecificMac

Specifies the two-fold firewall load balancing mode. If set to ENABLED, the traffic from a set of firewalls is load balanced by another set of firewalls on the other side of NetScaler. If set to DISABLED, NetScaler adopts the default behavior and the traffic that is already load balanced is not re-load balanced.

To configure multiple-firewall load balancing by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then in the Load Balancing pane click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure the redirection mode (for example, Configure Load Balancing parameters).
3. In the Set Load Balancing Parameters dialog box, select the Virtual Server Specific MAC check box.
4. Click Ok.

Saving and Verifying the Configuration

When you've finished the configuration tasks, be sure to save the configuration. You should also check to make sure that the settings are correct.

To save and verify the configuration by using the command line interface

At the command prompt, type the following commands to configure a transparent monitor and verify the configuration:

- save ns config
- show vserver

Example

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (*:*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
```

```
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
2) fw-int-svc2 (10.102.29.9: *) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 10.102.29.5
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
              State: DOWN     Weight: 1
              Probes: 9       Failed [Total: 9 Current: 9]
              Last response: Failure - Time out during TCP connection establishment stage
              Response Time: 2000.0 millisec
2)      Monitor Name: ping
              State: UP       Weight: 1
              Probes: 3       Failed [Total: 0 Current: 0]
              Last response: Success - ICMP echo reply received.
              Response Time: 1.275 millisec
 Done
```

To save and verify the configuration by using the configuration utility

1. In the details pane, click Save.
2. In the Save Config dialog box, click Yes.
3. In the navigation pane, click Load Balancing, and then click Virtual Servers.
4. In the details pane, select the virtual server that you created in step 5 and verify that the settings displayed in the Details pane are correct.
5. In the navigation pane, click Load Balancing, and then click Services.
6. In the details pane, select the service that you created in step 5 and verify that the settings displayed in the Details pane are correct.

Monitoring a Firewall Load Balancing Setup in a Multiple-Firewall Environment

After the configuration is up and running, you should view the statistics for each service and virtual server to check for possible problems.

Viewing the Statistics of a Virtual Server

To evaluate the performance of virtual servers or to troubleshoot problems, you can display details of the virtual servers configured on the NetScaler appliance. You can display a summary of statistics for all the virtual servers, or you can specify the name of a virtual server to display the statistics only for that virtual server. You can display the following details:

- Name
- IP address
- Port
- Protocol
- State of the virtual server
- Rate of requests received
- Rate of hits

To display virtual server statistics by using the command line interface

To display a summary of the statistics for all the virtual servers currently configured on the NetScaler, or for a single virtual server, at the command prompt, type:

stat lb vserver [-detail] [<name>]

Example

```
>stat lb vserver -detail
Virtual Server(s) Summary
                 vsvrIP  port    Protocol      State   Req/s   Hits/s
One                   *    80        HTTP         UP     5/s     0/s
Two                   *     0         TCP       DOWN     0/s     0/s
Three                 *  2598         TCP       DOWN     0/s     0/s
```

```
dnsVirtualNS    10.102.29.90    53        DNS        DOWN      0/s      0/s
BRVSERV          10.10.1.1     80        HTTP       DOWN      0/s      0/s
LBVIP          10.102.29.66    80        HTTP         UP      0/s      0/s
 Done
```

Parameters for displaying statistics

detail

Include the statistics for hits per second and the total number of hits.

name

Name of the virtual server whose statistics are displayed.

To display virtual server statistics by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. If you want to display the statistics for only one virtual server, in the details pane, select the virtual server whose statistics you want to display.
3. In the details pane, click Statistics.

Viewing the Statistics of a Service

You can view the rate of requests, responses, request bytes, response bytes, current client connections, requests in surge queue, current server connections, and so forth using the service statistics.

To view the statistics of a service by using the command line interface

At the command prompt, type:

stat service <name>

Example

stat service Service-HTTP-1

To view the statistics of a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service whose statistics you want to view (for example, Service-HTTP-1).
3. Click Statistics. The statistics appear in a new window.

Global Server Load Balancing

NetScaler appliances configured for global server load balancing (GSLB) provide for disaster recovery and ensure continuous availability of applications by protecting against points of failure in a wide area network (WAN). GSLB can balance the load across data centers by directing client requests to the closest or best performing data center, or to surviving data centers in case of an outage.

Following are some typical GSLB configurations:

- **Active-active data center setup**. Consists of multiple active data centers. Client requests are load balanced across active data centers.
- **Active-standby data center setup**. Consists of an active and a standby data center. When a failover occurs as a result of a disaster event, the standby data center becomes operational.
- **Proximity setup**. Directs client requests to the data center that is closest in geographical distance or network distance.

In a typical configuration, a local DNS server sends client requests to a GSLB virtual server, to which are bound GSLB services. A GSLB service identifies a load balancing or content switching virtual server, which can be at the local site or a remote site. If the GSLB virtual server selects a load balancing or content switching virtual server at a remote site, it sends the virtual server's IP address to the DNS server, which sends it to the client. The client then resends the request to the new virtual server at the new IP.

The GSLB entities that you must configure are the GSLB sites, the GSLB services, the GSLB virtual servers, load balancing or content switching virtual servers, and authoritative DNS (ADNS) services. You must also configure MEP. You can also configure DNS views to expose different parts of your network to clients accessing the network from different locations.

Note: To take full advantage of the NetScaler GSLB features, you should use NetScaler appliances for load balancing or content switching at each data center, so that your GSLB configuration can use the proprietary Metric Exchange Protocol (MEP) to exchange site metrics.

How GSLB Works

With ordinary DNS, when a client sends a domain name system (DNS) request, it receives a list of IP addresses of the domain or service. Generally, the client chooses the first IP address in the list and initiates a connection with that server. The DNS server uses a technique called DNS round robin to rotate through the IPs on the list, sending the first IP address to the end of the list and promoting the others after it responds to each DNS request. This technique ensures equal distribution of the load, but it does not support disaster recovery, load balancing based on load or proximity of servers, or persistence.

When you configure GSLB on NetScaler appliances and enable Metric Exchange Protocol (MEP), the appliances use the DNS infrastructure to connect the client to the data center that best meets the criteria that you set. The criteria can designate the least loaded data center, the closest data center, the data center that responds most quickly to requests from the client's location, a combination of those metrics, and SNMP metrics. An appliance keeps track of the location, performance, load, and availability of each data center and uses these factors to select the data center to which to send a client request.

A GSLB configuration consists of a group of GSLB entities on each appliance in the configuration. These entities include GSLB sites, GSLB services, GSLB virtual servers, load balancing and/or content switching servers, and ADNS services.

GSLB Sites

A typical GSLB setup consists of data centers, each of which has various network appliances that may or may not be NetScaler appliances. The data centers are called GSLB sites. Each GSLB site is managed by a NetScaler appliance that is local to that site. Each of these appliances treats its own site as the local site and all other sites, managed by other appliances, as remote sites.

If the appliance that manages a site is the only NetScaler appliance in that data center, the GSLB site hosted on that appliance acts as a bookkeeping placeholder for auditing purposes, because no metrics can be collected. Typically, this happens when the appliance is used only for GSLB, and other products in the data center are used for load balancing or content switching.

GSLB Services

A GSLB service is usually a representation of a load balancing or content switching virtual server, although it can represent any type of virtual server. The GSLB service identifies the virtual server's IP address, port number, and service type. GSLB services are bound to GSLB virtual servers on the NetScaler appliances managing the GSLB sites. A GSLB service bound to a GSLB virtual server in the same data center is local to the GSLB virtual server. A GSLB service bound to a GSLB virtual server in a different data center is remote from that GSLB virtual server.

GSLB Virtual Servers

A GSLB virtual server has one or more GSLB services bound to it, and load balances traffic among those services. It evaluates the configured GSLB methods (algorithms) to select the appropriate service to which to send a client request. Because the GSLB services can represent either local or remote servers, selecting the optimal GSLB service for a request has the effect of selecting the data center that should serve the client request.

The domain for which global server load balancing is configured must be bound to the GSLB virtual server, because one or more services bound to the virtual server will serve requests made for that domain.

Unlike other virtual servers configured on a NetScaler appliance, a GSLB virtual server does not have its own virtual IP address (VIP).

Load Balancing or Content Switching Virtual Servers

A load balancing or content switching virtual server represents one or many physical servers on the local network. Clients send their requests to the load balancing or content switching virtual server's virtual IP (VIP) address, and the virtual server balances the load across the physical servers. After a GSLB virtual server selects a GSLB service representing either a local or a remote load balancing or content switching virtual server, the client sends the request to that virtual server's VIP address.

For more information about load balancing or content switching virtual servers and services, see Load Balancing, or Content Switching .

ADNS Services

An ADNS service is a special kind of service that responds only to DNS requests for domains for which the NetScaler appliance is authoritative. When an ADNS service is configured, the appliance owns that IP address and advertises it. Upon reception of a DNS request by an ADNS service, the appliance checks for a GSLB virtual server bound to that domain. If a GSLB virtual server is bound to the domain, it is queried for the best IP address to which to send the DNS response.

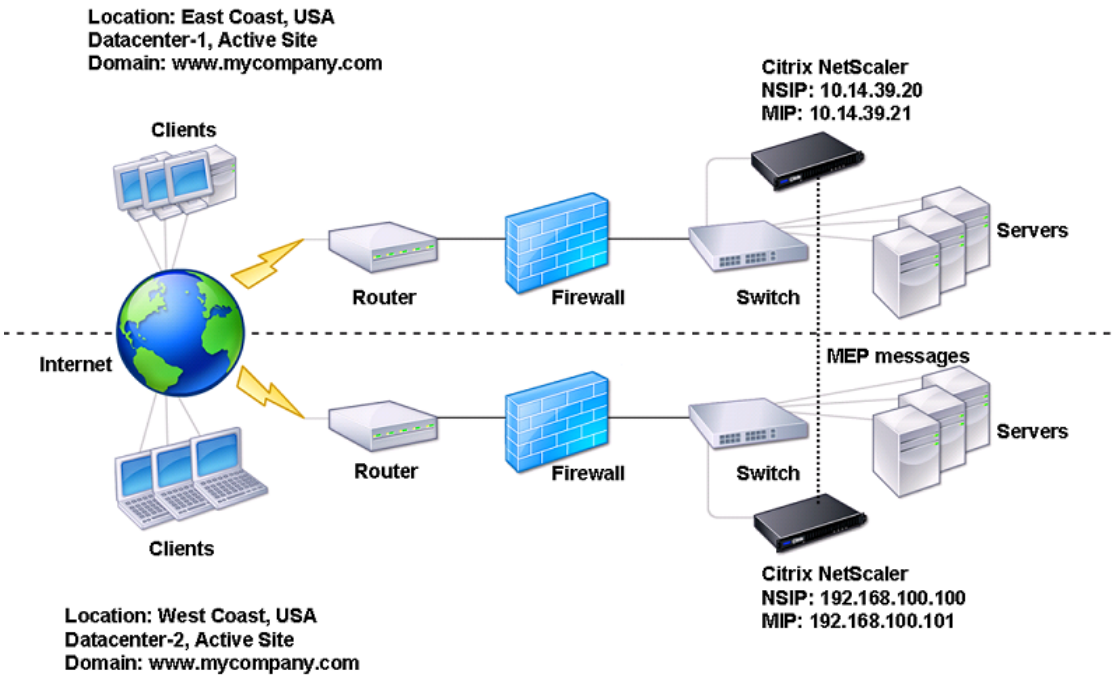
DNS VIPs

A DNS virtual IP is a virtual IP (VIP) address that represents a load balancing DNS virtual server on the NetScaler appliance. DNS requests for domains for which the NetScaler appliance is authoritative can be sent to a DNS VIP.

Configuring Global Server Load Balancing (GSLB)

Global server load balancing is used to manage traffic flow to a web site hosted on two separate server farms that ideally are in different geographic locations. For example, consider a Web site, www.mycompany.com, which is hosted on two geographically separated server farms or data centers. Both server farms use NetScaler appliances. The NetScaler appliances in these server farms are set up in one-arm mode and function as authoritative DNS servers for the www.mycompany.com domain. The following figure illustrates this configuration.

Figure 1. Basic GSLB Topology



To configure such a GSLB setup, you must first configure a standard load balancing setup for each server farm or data center. This enables you to balance load across the different servers in each server farm. Then, configure both NetScaler appliances as authoritative DNS (ADNS) servers. Next, create a GSLB site for each server farm, configure GSLB virtual servers for each site, create GLSB services, and bind the GSLB services to the GSLB virtual servers. Finally, bind the domain to the GSLB virtual servers. The GSLB configurations on the two appliances at the two different sites are identical, although the load-balancing configurations for each site is specific to that site.

Note: To configure a GSLB site in a NetScaler cluster setup, see Setting Up GSLB in a Cluster.

Configuring a Standard Load Balancing Setup

A load balancing virtual server balances the load across different physical servers in the data center. These servers are represented as services on the NetScaler appliance, and the services are bound to the load balancing virtual server.

For details on configuring a basic load balancing setup, see Load Balancing.

Configuring an Authoritative DNS Service

When you configure the NetScaler appliance as an authoritative DNS server, it accepts DNS requests from the client and responds with the IP address of the data center to which the client should send requests.

Note: For the NetScaler to be authoritative, you must also create SOA and NS records. For more information about SOA and NS records, see "Domain Name System".

To create an ADNS service by using the command line interface

At the command prompt, type the following commands to create an ADNS service and verify the configuration:

- add service <name> <IP>@ ADNS <port>
- show service <name>

Example

```
add service Service-ADNS-1 10.14.39.21 ADNS 53
show service Service-ADNS-1
```

To modify an ADNS service by using the command line interface

At the command prompt, type the following command:

set service <name> <IPAddress> ADNS <port>

Example

```
set service Service-ADNS-1 10.14.39.21 ADNS 53
```

To remove an ADNS service by using the command line interface

At the command prompt, type the following command:

rm service <name>

Example

rm service Service-ADNS-1

Parameters for configuring an ADNS service

name

The name of the ADNS service you are creating. This alphanumeric string is required and cannot be changed after the service is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

IPAddress

The IP address of the server that the ADNS service represents. You can configure the ADNS service to use a mapped IP address (MIP), subnet IP address (SNIP), or any new NetScaler-owned IP address.

port

The port on which the service communicates with the application on the server. This number must correspond to the protocol that the application supports. The port number must always be a positive number not exceeding 65535.

To configure an ADNS service by using the configuration utility

1. In the navigation pane, expand Load Balancing and click Services.
2. In the details pane, do one of the following:
   - To create a new service, click Add.
   - To modify an existing service, select the service, and then click Open.
3. In the Create Service or Configure Service dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring an ADNS service” as shown:
   - Service Name*—name
   - Service Name*—name
   - Protocol*—(Select ADNS as the protocol.)
   - Port*—port
4. Click Create or OK, and then click Close. The server that you created appears in the GSLB Services pane.

Configuring a Basic GSLB Site

A GSLB site is a representation of a data center in your network and is a logical grouping of GSLB virtual servers, services, and other network entities. Typically, in a GSLB set up, there are many GSLB sites that are equipped to serve the same content to a client. These are usually geographically separated to ensure that the domain is active even if one site goes down completely. All of the sites in the GSLB configuration must be configured on every NetScaler appliance hosting a GSLB site. In other words, at each site, you configure the local GSLB site and each remote GSLB site.

Once GSLB sites are created for a domain, the NetScaler appliance sends client requests to the appropriate GSLB site as determined by the GSLB algorithms configured.

To create a GSLB site by using the command line interface

At the command prompt, type the following commands to create a GSLB site and verify the configuration:

- add gslb site <siteName> <siteIPAddress>
- show gslb site <siteName>

Example

add gslb site Site-GSLB-East-Coast 10.14.39.21
show glsb site Site-GSLB-East-Coast

To modify or remove a GSLB Site by using the command line interface

- To modify a GSLB site, use the set gslb site command, which is just like using the add gslb site command, except that you enter the name of an existing GSLB Site.
- To unset a site parameter, use the unset gslb site command, followed by the siteName value and the name of the parameter to be reset to its default value.
- To remove a GSLB site, use the rm gslb site command, which accepts only the <name> argument.

Parameters for configuring a GSLB site

siteName

A name for the data center you are adding as a GSLB site. This alphanumeric string is required and cannot be changed after the site is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

siteIPAddress

The IP address of the GSLB site. This IP address is a system-owned IP address. You can use any IP address configured as a SNIP, MIP, or GSLB site IP address. This is a mandatory parameter.

Note: To avoid a site going down during an HA failover event in a GSLB setup with an independent network configuration high availability deployment, the GSLB site IP address must be on the same subnet as the virtual IP (VIP) address of the load balancing or content switching virtual server that is bound to the service(s) provided by that GSLB site. In an independent network configuration high availability deployment, two nodes do not share the same subnet IPs (SNIPs) or mapped IPs (MIPs), but they have common VIPs.

To configure a basic GSLB site by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Sites.
2. In the details pane, do one of the following:
   - To create a new site, click Add.
   - To modify an existing site, select the site, and then click Open.
3. In the Create GSLB Site or Configure GSLB Site dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a GSLB site” as shown:
   - Name*—siteName
   - Site IP Address*—siteIPAddress

   * A required parameter
4. Click Create or OK, and then click Close. The GSLB site you created appears in the GSLB Sites pane.

To view the statistics of a GSLB site by using the command line interface

At the command prompt, type:

stat gslb site <siteName>

Example

stat gslb site Site-GSLB-East-Coast

To view the statistics of a GSLB site by using the configuration utility

1. In the navigation pane, expand GSLB and click Sites.
2. In the GSLB Sites pane, select the GSLB site whose statistics you want to view.
3. Click Statistics.

Configuring a GSLB Service

A GSLB service is a representation of a load balancing or content switching virtual server. A local GSLB service represents a local load balancing or content switching virtual server. A remote GSLB service represents a load balancing or content switching virtual server configured at one of the other sites in the GSLB setup. At each site in the GSLB setup, you can create one local GSLB service and any number of remote GSLB services.

Creating GSLB Services

To create a GSLB service by using the command line interface

At the command prompt, type the following commands to create a GSLB service and verify the configuration:

- add gslb service <serviceName> <serverName | IP> <serviceType> <port>-siteName <string>
- show gslb service <serviceName>

Example

add gslb service Service-GSLB-1 10.14.39.14 HTTP 80 –siteName Site-GSLB-East-Coast
show gslb service Service-GSLB-1

To modify or remove a GSLB service by using the command line interface

- To modify a GSLB service, use the set gslb service <serviceName> command. For this command, specify the name of the GSLB service whose configuration you want to modify. You can change the existing values of the parameters either specified by you or set by default. You can change the value of more than one parameter in the same command. Refer to the add gslb service command for details about the parameters. Example

  ```
  > set gslb service SKP_GSLB_NOTCNAME_SVC2 -maxBandWidth 25 -maxClient 8
  Done
  > sh gslb service SKP_GSLB_NOTCNAME_SVC2
  SKP_GSLB_NOTCNAME_SVC2 (21.211.21.21: 80)- HTTP
  ...
  Max Conn: 8  Max Bandwidth: 25 kbits
  ```

- To reset a parameter to its default value, you can use the unset gslb service <serviceName> command and the parameters to be unset. Example

  ```
  > unset gslb service SKP_GSLB_NOTCNAME_SVC2 maxBandWidth
  Done
  > sh gslb service SKP_GSLB_NOTCNAME_SVC2
  SKP_GSLB_NOTCNAME_SVC2 (21.211.21.21: 80)- HTTP
  ...
  Max Conn: 8  Max Bandwidth: 0 kbits
  ```

- To remove a GSLB service, use the rm gslb service <serviceName> command.

Parameters for configuring a GSLB service

serviceName (Service Name)

The name of the service being configured. This alphanumeric string is required. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

siteName (Site Name)

The name of the GSLB site that this service represents.

serviceType (Service Type)

The type of service or protocol used in client requests. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, MSSQL, MYSQL, RADIUS, RDP, SIP_UDP, RTSP.

port (Port)

Port number on which the service runs.

serverName or ipAddress (Server IP)

The server name or IP address of the GSLB service being configured. Must be the same as the virtual IP (VIP) address of a local or remote load balancing or content switching virtual server.

publicIP (Public IP)

The public IP address of the NAT translator for a GSLB service that is on a private network.

To create a GSLB service by using the configuration utility

1. In the navigation pane, expand GSLB and click Services.
2. In the details pane, do one of the following:
   - To create a new service, click Add.
   - To modify an existing service, select the service, and then click Open.
3. In the Create GSLB Service or Configure GSLB Service dialog box, set the following parameters:
   - Service Name*
   - Site Name*
   - Server Name - The servers added to the NetScaler configuration are displayed in a dropdown list. If you want to add a new server, click New..., and then in the Create Server dialog box, type the necessary details. For more information about creating servers, see "Adding a Server."
   - Service Type
   - Port

   Note: In the Site Name and Server Name lists, the most recently used value is displayed as selected. Make sure that you select the site and server you want to specify.
4. Click Create, and then click Close. The GSLB service you created appears in the GSLB Services pane.

To view the statistics of a GSLB service by using the command line interface

At the command prompt, type:

stat gslb service <serviceName>

Example

stat gslb service Service-GSLB-1

To view the statistics of a GSLB service by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the GSLB Services pane, select the GSLB Service whose statistics you want to view.
3. Click Statistics.

Enabling and Disabling GSLB Services

Before you use a GSLB service for load balancing, it must be enabled. If the service is disabled, it is not included in load balancing even though it exists on the NetScaler appliance.

To enable or disable a GSLB service by using the command line interface

At the command prompt, type one of the following commands:

- enable service <name>
- disable service <name>

Example

```
> enable service Service-GSLB-1
 Done
> disable service Service-GSLB-1
 Done
```

To enable or disable a GSLB service by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Services.
2. In the GSLB Services pane, select the GSLB service which you want to enable or disable.
3. Click enable or disable.

Configuring a GSLB Virtual Server

A GSLB virtual server is an entity that represents one or more GSLB services and balances traffic between them. It evaluates the configured GSLB methods or algorithms to select a GSLB service to which to send the client request.

Creating GSLB Virtual Servers

To create a GSLB virtual server by using the command line interface

At the command prompt, type the following commands to add a GSLB virtual server and verify the configuration:

- add gslb vserver <name> <serviceType> -ipType (IPv4 | IPv6)
- show gslb vserver <name>

Example

```
add gslb vserver Vserver-GSLB-1 HTTP -ipType IPv4
add gslb vserver Vserver-GSLB-2 HTTP -ipType IPv6
show gslb vserver Vserver-GSLB-1
show gslb vserver Vserver-GSLB-2
```

To modify or remove a GSLB virtual server by using the command line interface

- To modify a GSLB virtual server, use the set gslb vserver command, which is just like using the add gslb vserver command, except that you enter the name of an existing GSLB virtual server.
- To reset a parameter to is default value, you can use the unset gslb vserver command followed by the vserverName value and the name of the parameter to be unset.
- To remove a GSLB virtual server, use the rm gslb vserver command, which accepts only the <name> argument.

Parameters for configuring a GSLB server

name

The name of the GSLB virtual server. This alphanumeric string is required and cannot be changed after the virtual server is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serviceType

The service type of the virtual server, that is, the type of content in the processed requests. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RDP, ANY.

ipType

Specifies whether this virtual server supports services that use the IPv4 or IPv6 protocol for IP addresses. Possible values: IPv4, IPv6. Default: IPv4.

To create a GSLB virtual server by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the details pane, do one of the following:
   - To create a new GSLB virtual server, click Add.
   - To modify an existing GSLB virtual server, select the service, and then click Open.
3. In the Create GSLB Virtual Server or Configure GSLB Virtual Server dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a GSLB virtual server” as shown:
   - Name*—name
   - Service Type*—serviceType
   - IPv6—ipType (To specify IPv6, select the check box. For IPv4, clear the check box.)

   * A required parameter
4. Click Create or OK, and then click Close. The GSLB virtual server that you created appears in the GSLB Virtual Servers pane.

To view the statistics of a GSLB virtual server by using the command line interface

At the command prompt, type:

stat gslb vserver <name>

Example

stat gslb vserver Vserver-GSLB-1

To view the statistics of a GSLB virtual server by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the details pane, select the GSLB virtual server whose statistics you want to view.
3. Click Statistics.

Statistics of a GSLB service

When you run the stat gslb service command from the command line or click on the Statistics link from the configuration utility, the following details of the service will be displayed:

- **Request bytes.** Total number of request bytes received on this service or virtual server.
- **Response bytes.** Number of response bytes received by this service or virtual server.
- **Current client established connections.** Number of client connections in ESTABLISHED state.
- **Current load on the service.** Load on the service (Calculated from the load monitor bound to the service).

The data of number of requests and responses, and the number of current client and server connections may not be displayed or may not be synchronized with the data of the corresponding load balancing virtual server.

Enabling and Disabling GSLB Virtual Servers

When you create a GSLB virtual server, it is enabled by default. If you disable it, it cannot process traffic. A disabled GSLB virtual server is not included in GSLB configuration but is not removed from the NetScaler appliance.

To enable or disable a GSLB virtual server by using the command line interface

At the command prompt, type one of the following commands:

- enable gslb vserver <name>@
- disable gslb vserver <name>@

Example

enable gslb vserver Vserver-GSLB-1
disable gslb vserver Vserver-GSLB-1

To enable or disable a GSLB virtual server by using the configuration utility

1. Select a virtual server and, from the **Action** list, select **enable** or **disable**.

Binding GSLB Services to a GSLB Virtual Server

Once the GSLB services and virtual server are configured, relevant GSLB services must be bound to the GSLB virtual server to activate the configuration.

To bind a GSLB service to a GSLB virtual server by using the command line interface

At the command prompt, type the following commands to bind a GSLB service to a GSLB virtual server and verify the configuration:

- bind gslb vserver <name> -serviceName <string>
- show gslb vserver <name>

Example

bind gslb vserver Vserver-GSLB-1 -serviceName Service-GSLB-1
show gslb vserver Vserver-GSLB-1

To unbind a GSLB service from a GSLB virtual server by using the command line interface

At the command prompt, type:

unbind gslb vserver <name> -serviceName <string>

To bind GSLB services by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the details pane, select the GSLB Virtual Server to which you want to bind the services (for example, Vserver-GSLB-1).
3. Click Open.
4. On the Services tab, in the Active column, select the check boxes next to the GSLB services that you want to bind to the GSLB virtual server.
5. Click OK.

Binding a Domain to a GSLB Virtual Server

To make a NetScaler appliance the authoritative DNS server for a domain, you must bind the domain to the GSLB virtual server. When you bind a domain to a GSLB virtual server, the NetScaler adds an address record for the domain, containing the name of the GSLB virtual server. The start of authority (SOA) and name server (NS) records for the GSLB domain must be added manually.

For details on configuring SOA and NS records, see "Domain Name System".

To bind a domain to a GSLB virtual server by using the command line interface

At the command prompt, type the following commands to bind a domain to a GSLB virtual server and verify the configuration:

- bind gslb vserver <name> -domainName <string>
- show gslb vserver <name>

Example

```
bind gslb vserver Vserver-GSLB-1 -domainName www.mycompany.com
show gslb vserver Vserver-GSLB-1
```

To unbind a GSLB domain from a GSLB virtual server by using the command line interface

At the command prompt, type:

unbind gslb vserver <name> -domainName <string>

To bind a domain to a GSLB virtual server by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In GSLB Virtual Servers pane, select the GSLB Virtual Server to which you want to bind the domain (for example, Vserver-GSLB-1) and click Open.
3. In the Configure GSLB Virtual Server dialog box, on the Domains tab, do one of the following:
   - To create a new Domain, click Add.
   - To modify an existing Domain, select the domain, and then click Open.
4. In the Create GSLB Domain or Configure GSLB Domain dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for Binding or Unbinding a Domain to a GSLB Virtual Server” as shown:
   - Domain Name*—domainName (for example, www.mycompany.com)

   * A required parameter
5. Click Create.
6. Click OK.

To view the statistics of a domain by using the command line interface

At the command prompt, type:

stat gslb domain <name>

Example

stat gslb domain www.mycompany.com

Note: To view statistics for a particular GSLB domain, enter the name of the domain exactly as it was added to the NetScaler appliance. If you do not specify the domain name, or if you specify an incorrect domain name, statistics for all configured GSLB domains are displayed.

To view the statistics of a domain by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In GSLB Virtual Servers pane, select the GSLB Virtual Server (for example, Vserver-GSLB-1) and click Open.
3. In the Configure GSLB Virtual Server dialog box, on the Domains tab, select the domain, and then click Statistics.

Synchronizing a Configuration in a GSLB Setup

Typically, a GSLB setup has a few data centers with a GSLB site configured for each data center. In each NetScaler, participating in GSLB, configure one GSLB site as a local site and the others as remote sites. When you add another GSLB site at a later point of time, ensure that all the GSLB sites have the same configuration. To have the same configuration on all the GSLB sites, you can use the NetScaler appliance's GSLB configuration synchronization option.

The NetScaler appliance from which you use the synchronization option is referred to as the 'master node' and the GSLB sites on which the configuration is copied as 'slave nodes'. When you synchronize a GSLB configuration, the configurations on all the GSLB sites participating in the GSLB setup are made similar to that on the master node.

Synchronization (may also be referred to as 'auto sync') is carried out in the following manner:

- The master node finds the differences between the configuration of the master node and slave node, and changes the configuration of the slave node to make it similar to the master node.

  If you force a synchronization (use the 'force sync' option), the NetScaler deletes the GSLB configuration from the slave node and then configures the slave to make it similar to the master node.

- During synchronization, if a command fails, synchronization is not aborted.

- Synchronization is done only on the parent sites. If a GSLB site is configured as a child site, its configuration is not affected by synchronization.

Note: On the remote GSLB site RPC node, configure the firewall to accept auto-sync connections by specifying the remote site IP (cluster IP address for cluster setup) and port (3010 for RPC and 3008 for secure RPC). The source IP address that will be used for auto-sync is the NSIP of the master node (NSIP of the configuration coordinator in a cluster setup).

If you use the `saveconfig` option, the sites that participate in the synchronization process automatically save their configuration, in the following way:

1. The master node saves its configuration immediately before it initiates the process of synchronization.

2. After the process of synchronization is complete, the slave nodes save their configuration. A slave node saves its configuration only if the configuration difference was applied successfully on it. If synchronization fails on a slave node, you must manually investigate the cause of the failure and take corrective action.

Limitations of synchronization:

- On the master node, the names of the remote GSLB sites must be identical to the names of sites configured on the NetScaler appliances hosting those sites.
- During the synchronization, traffic disruptions may occur.
- NetScaler can synchronize only up to 80000 lines of the configuration.
- Synchronization may fail:
  - If the spill over method is changed from CONNECTION to DYNAMIC CONNECTION.
  - If you interchange the site prefix of the GSLB services bound to a GSLB virtual server on the master node and then try to synchronize.
  - If the RPC node passwords are different for NetScaler IP address (NSIP) and GSLB Site IP address.
  - If the RPC node passwords are different for NetScaler IP address (NSIP) and loopback IP address.
- If you have configured the GSLB sites as High Availability (HA) pairs, the RPC node passwords of primary and secondary nodes should be same.
- If you rename any GLSB entity that are part of your GSLB configuration (use “show gslb runningConfig” command to display the GSLB configuration). You need to use the force sync option to synchronize the configuration to other GSLB sites.

Note: To overcome the limitations due to some settings in the GSLB configuration, you can use the force sync option. But, if you use the force sync option the GSLB entities are removed and re-added to the configuration and the GSLB statistics are reset to zero. Hence the traffic is disrupted during the configuration change.

Before you start the synchronization of a GSLB setup, make sure that:

- On all the GSLB sites including the master node, management access should be enabled for the IP address of the corresponding GSLB site. The IP address of a GSLB site must be an IP address owned by the NetScaler.

  For more information about adding the GSLB site IP addresses and enabling Management Access, see "Configuring a Basic GSLB Site" and "Configuring NetScaler-Owned IP Addresses".
- The GSLB configuration on the NetScaler appliance that is considered as the master node is complete and appropriate to be copied on all the sites.
- If you are synchronizing the GSLB configuration for the first time, all the sites participating in GSLB need to have the GSLB site entity of their respective local sites.
- You are not synchronizing sites that, by design, do not have the same configuration.

Important: After a GSLB configuration is synchronized, the configuration cannot be rolled back on any of the GSLB sites. Run the `sync gslb config` command only if you are sure that the synchronization process will not overwrite the configuration on the remote site. Site synchronization is undesirable when the local and remote sites have different configurations by design, and can lead to site outage. If some commands fail and some commands succeed, the successful commands cannot be rolled back.

To synchronize a GSLB configuration by using the command line interface

At the command prompt, type the following commands to synchronize GSLB sites and verify the configuration:

- sync gslb config [-preview | -forceSync <string> | -nowarn | -saveconfig] [-debug]
- show gslb syncStatus

Example

```
> sync gslb config
[WARNING]: Syncing config may cause configuration loss on other site.
Please confirm whether you want to sync-config (Y/N)? [N]:y
Sync Time: Dec 9 2011 10:56:9
Retrieving local site info: ok
Retrieving all participating gslb sites info: ok
Gslb_site1[Master]:
      Getting Config: ok
Gslb_site2[Slave]:
      Getting Config: ok
      Comparing config: ok
       Applying changes: ok
Done
```

Parameters for synchronizing a GSLB configuration

<no option>

If no option is passed to this command, synchronization happens on all the GSLB sites in the auto sync method.

preview (Preview)

Do not synchronize the GSLB sites, but only display the commands that would be applied on the slave node upon synchronization. Mutually exclusive with the saveConfig option.

forceSync <string> (Force Sync)

Forcibly synchronize the specified site even if a dependent configuration on the remote site is preventing synchronization or if one or more GSLB entities on the remote site have the same name but are of a different type. Possible values:

- The name of the remote site that you want to synchronize with the local site.
- The string `all-sites`.

If you specify `all-sites`, all the sites in the GSLB setup are synchronized with the site on the master node.

Note: If you select the force sync option, the synchronization starts without displaying the commands that are going to be executed.

nowarn

Suppress the warning and the confirmation prompt that are displayed before site synchronization begins. This option can be used in automation scripts that must not be interrupted by a prompt. Appears only if you use the `forceSync` and `debug` options.

saveconfig

Save the configuration on all the nodes participating in the synchronization process, automatically. The master saves its configuration immediately before synchronization begins. Slave nodes save their configuration after the process of synchronization is complete. A slave node saves its configuration only if the configuration difference was applied successfully on it. Mutually exclusive with the preview option.

debug (Debug)

Generate verbose output when synchronizing the GSLB sites. The `debug` option generates more verbose output than a `sync gslb config` command in which the option is not used, and is useful when you want to analyze synchronization issues.

To synchronize a GSLB configuration by using the configuration utility

1. In the navigation pane, click GSLB.
2. In the GSLB pane, under GSLB Configuration, click Synchronize configuration on remote sites.
3. In the Synchronize GSLB Configuration dialog box, select one of the following settings from the Synchronization Option list:
   - Preview
   - Force Sync
   - Debug
4. If you select Force Sync as the synchronization option, in the GSLB Site Name text box, type the name of the remote site that you want to synchronize with the local site, or type `all-sites`.
5. If you want the participating sites to save their configuration automatically, select Save Configuration.
6. Click Run.
7. If you want to save the output of the Run command to your local system, click Save output text to a file.
8. Click Close.

Viewing and Configuring a GSLB Setup by Using the GSLB Visualizer

The configuration utility includes a GSLB Visualizer tool, which provides an alternative way to view and configure entities in a GSLB configuration. The visualizer displays all configured GSLB domains, GSLB services, GSLB sites, ADNS services, and any monitors that are bound to the services. It also displays all the load balancing, content switching, cache redirection, and Access Gateway virtual servers that the GSLB services represent.

If you want to view the configurations of remote GSLB sites, you must configure the sites with public IP addresses and enable management access for each of them.

You can use the GSLB Visualizer to perform the following GSLB configuration tasks:

- Add, view, and configure GSLB domains and GSLB services.
- View and configure GSLB sites and ADNS services for each site.
- View and configure any monitors that are bound to the services.
- View and configure the content switching, load balancing, cache redirection, or Access Gateway virtual server that each GSLB service represents.
- View statistics for GSLB domains, sites, ADNS services, and virtual servers.
- View configuration details of any displayed entity.
- View load balancing and content switching virtual servers.
- View bindings for GSLB services, ADNS services, monitors, and virtual servers.
- Enable and disable GSLB services, ADNS services, monitors, and virtual servers.
- Copy the properties of any displayed entity to a document or spreadsheet.
- Remove a domain from the GSLB setup.
- Save the visual representation of the GSLB setup as an image.

To open the Visualizer and locate an entity

1. In the navigation pane, click GSLB.
2. In the details pane, under Getting Started, click GSLB Visualizer, and then do the following.
   - To pan the view of the displayed image, click as blank area of the image, hold down the mouse button, and drag the image.
   - To adjust the viewable area click Zoom In to increase or Zoom Out to decrease the size of the objects. You can readjust the viewable area by clicking Best Fit.
   - To locate a specific item, begin typing the item's name in the Search field. Entities whose names match the typed characters are highlighted. Continue typing until the item is uniquely identified. To clear the Search field, click the x adjacent to the field.

To add a GSLB domain and/or configure GSLB services and sites for the domain

1. Open the GSLB Visualizer and click Domain. Alternatively, if domains already exist in the GSLB setup, click the name of an existing domain.
2. Under Related Tasks, click Add.
3. Follow the instructions in the GSLB Wizard to add a GSLB domain and configure GSLB services and sites for the domain.

To view the configuration details of an entity

Open the GSLB Visualizer and do one of the following:

- To view a brief summary of an entity, place the pointer on the entity. A brief summary of the entity appears at the bottom of the viewable area.
- To view the detailed configuration information of the entity, click the entity. The configuration details for that entity appear in the Details area.

To modify a GSLB domain, site, service, monitor, or ADNS service

Open the GSLB Visualizer and do one of the following:

- Click the entity that you want to modify. Then, under Related Tasks, click Open.
- Double-click the entity that you want to modify.

- Right-click the entity that you want to modify, and then click Open. (This option is not available for GSLB sites.)

To view the entities to which a GSLB service, ADNS service, monitor, or virtual server is bound

Open the GSLB Visualizer and do one of the following:

- Click the entity whose binding information you want to view, and then, under Related Tasks, click Show Bindings.
- Right-click the entity, and then click Show Bindings.

To view the Visualizer for load balancing and content switching virtual servers from the GSLB Visualizer

Open the GSLB Visualizer and do one of the following:

- Click the load balancing or content switching virtual server whose Visualizer you want to view, and then, under Related Tasks, click Visualizer.
- Right-click the virtual server, and then click Visualizer.

To view statistics for a GSLB service, site, ADNS service, or virtual server

Open the GSLB Visualizer and do one of the following:

- Click the entity whose statistics you want to view, and then, under Related Tasks, click Statistics.
- Right-click the entity whose statistics you want to view, and then click Statistics. (This option is not available for GSLB sites.)

To enable or disable a GSLB service, ADNS service, monitor, or virtual server

Open the GSLB Visualizer and do one of the following to enable or disable the entity:

- To enable the entity, click the entity and, under Related Tasks, click Enable. Alternatively, right-click the entity that you want to enable, and then click Enable.
- To disable the entity, click the entity and, under Related Tasks, click Disable. Alternatively, right-click the entity that you want to disable, and then click Disable.

To copy the properties of an entity to a document or spreadsheet

Open the GSLB Visualizer and do one of the following:

- Click the entity whose properties you want to copy, and then, under Related Tasks, click Copy Properties.
- Right-click the entity, and then click Copy. (This option is not available for GSLB sites.)

To save the visual representation of the GSLB setup as an image

1. Open the GSLB Visualizer.
2. If necessary, adjust the viewable area by using the Best Fit, Zoom In, and Zoom Out buttons.
3. Click Save Image.
4. In the Save Graph Image dialog box, browse to the folder in which you want to save the image.
5. In File Name text box, type the name, and then click Save.

To remove a domain from the GSLB setup

1. Open the GSLB Visualizer and do one of the following:
   - Click the domain that you want to remove, and then, under Related Tasks, click Remove.
   - Right-click the domain, and then click Remove.
2. Under Remove?, click Yes.

Configuring the Metrics Exchange Protocol (MEP)

The data centers in a GSLB setup exchange metrics with each other through the metrics exchange protocol (MEP), which is a proprietary protocol for the Citrix NetScaler. The exchange of the metric information begins when you create a GSLB site. These metrics comprise load, network, and persistence information.

MEP is required for health checking of data centers to ensure their availability. A connection for exchanging network metrics can be initiated by either of the data centers involved in the exchange, but a connection for exchanging site metrics is always initiated by the data center with the lower IP address. By default, the data center uses a subnet IP address (SNIP) or a mapped IP address (MIP) to establish a connection to the IP address of a different data center. However, you can configure a specific SNIP, MIP, the NetScaler IP address (NSIP), or a virtual IP address (VIP) as the source IP address for metrics exchange. The communication process between GSLB sites uses TCP port 3011 or 3009, so this port must be open on firewalls that are between the NetScaler appliances.

Note: You cannot configure a GSLB site IP address as the source IP address for site metrics exchange.

If the source and target sites for a MEP connection (the site that initiates a MEP connection and the site that receives the connection request, respectively) have both private and public IP addresses configured, the sites exchange MEP information by using the public IP addresses.

You can also bind monitors to check the health of remote services. When monitors are bound, metric exchange does not control the state of the remote service. If a monitor is bound to a remote service and metrics exchange is enabled, the monitor controls the health status. Binding the monitors to the remote service allows the NetScaler to interact with a non-NetScaler load balancing device. The NetScaler can monitor non-NetScaler devices but cannot perform load balancing on them. The NetScaler can monitor non-NetScaler devices, and can perform load balancing on them if monitors are bound to all GSLB services and only static load balancing methods (such as the round robin, static proximity, or hash-based methods) are used.

Configuring Site Metric Exchange

Site metrics exchanged between the GSLB sites include the status of each load balancing and content switching virtual server, the current number of connections, the current packet rate, and current bandwidth usage information.

The NetScaler appliance needs this information to perform load balancing between the sites. The site metric exchange interval is 1 second. A remote GSLB service must be bound to a local GSLB virtual server to enable the exchange of site metrics with the remote service.

To enable or disable site metric exchange by using the command line interface

At a command prompt, type the following commands to enable or disable site metric exchange and verify the configuration:

- set gslb site <siteName> -metricExchange(ENABLED|DISABLED)
- show gslb site <siteName>

Example

```
set gslb site Site-GSLB-East-Coast -metricExchange ENABLED
set gslb site Site-GSLB-East-Coast -metricExchange DISABLED
show gslb site Site-GSLB-East-Coast
```

To enable or disable site metric exchange by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Sites.
2. In the details pane, select the site, and then click Open.
3. In the Configure GSLB Site dialog box, select or clear the check box next to the Metric Exchange and click OK.

Configuring Network Metric Information Exchange

You can enable or disable the exchange of round trip time (RTT) information about the client's local DNS when the GSLB dynamic method (RTT) is enabled. This information is exchanged every 5 seconds.

For details about changing the GSLB method to a method based on RTT, see Changing the GSLB Method.

To enable or disable network metric information exchange by using the command line interface

At the command prompt, type the following commands to enable or disable network metric information exchange and verify the configuration:

- set gslb site <siteName> -nwmetricExchange (ENABLED|DISABLED)
- show gslb site <<siteName>

Example

```
set gslb site Site-GSLB-East-Coast -nwmetricExchange ENABLED
set gslb site Site-GSLB-East-Coast -nwmetricExchange DISABLED
show gslb site Site-GSLB-East-Coast
```

To enable or disable network metric information exchange by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Sites.
2. In the details pane, select the site, and then click Open.
3. In the Configure GSLB Site dialog box, select or clear the check box next to the Network Metric Exchange and click OK.

Configuring Persistence Information Exchange

You can enable or disable the exchange of persistence information at each site. This information is exchanged every 5 seconds between NetScaler appliances participating in GSLB.

For details about configuring persistence, see "Configuring Persistent Connections".

To enable/disable persistence information exchange by using the command line interface

At the command prompt, type the following commands to enable or disable persistence information exchange and verify the configuration:

- set gslb site <siteName> -sessionExchange (ENABLED|DISABLED)
- show gslb site <siteName>

Example

```
set gslb site Site-GSLB-East-Coast -sessionExchange  ENABLED
set gslb site Site-GSLB-East-Coast -sessionExchange  DISABLED
show gslb site Site-GSLB-East-Coast
```

To enable/disable persistence information exchange by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Sites.
2. In the details pane, select the site, and then click Open.
3. In the Configure GSLB Site dialog box, select or clear the check box next to the Persistence Session Entry Exchange and click OK.

Configuring Site-to-Site Communication

GSLB site-to-site communication is between the remote procedure call (RPC) nodes that are associated with the communicating sites. A master GSLB site establishes connections with slave sites to synchronize GSLB configuration information and to exchange site metrics.

An RPC node is created automatically when a GSLB site is created, and is assigned an internally generated user name and password. The NetScaler appliance uses this user name and password to authenticate itself to remote GSLB sites during connection establishment. No configuration steps are necessary for an RPC node, but you can specify a password of your choice, enhance security by encrypting the information that GSLB sites exchange, and specify a source IP address for the RPC node.

The appliance needs a NetScaler-owned IP address to use as the source IP address when communicating with other GSLB sites. By default, the RPC nodes use either a subnet IP (SNIP) address or a mapped IP (MIP) address, but you might want to specify an IP address of your choice.

Changing the Password of an RPC Node

You can secure the communication between sites in your GSLB setup by changing the password of each RPC node. After you change the password for the RPC node of the local site, you must manually propagate the change to the RPC node at each of the remote sites.

The password is stored in encrypted form. You can verify that the password has changed by using the `show rpcNode` command to compare the encrypted form of the password before and after the change.

To change the password of an RPC node by using the command line interface

At the command line, type the following commands to change the password of an RPC node:

- set ns rpcNode <IPAddress> {-password}
- show ns rpcNode

Example

```
> set rpcNode 192.0.2.4 -password mypassword
 Done
> show rpcNode
.
.
.
2)  IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
    SrcIP:  *             Secure:  OFF
Done
>
```

To unset the password of an RPC node by using the command line interface

To unset the password of an RPC node by using the NetScaler command line, type the unset rpcNode command, the IP address of the RPC node, and the password parameter, without a value.

Parameters for changing the password of an RPC node

IPAddress

The IP address of the GSLB site to which the RPC node belongs. This is the value of the `IPAddress` field in the output of the `show rpcNode` CLI command.

password

The password that the RPC node must use to authenticate itself to other nodes in the GSLB configuration. By default, a password is configured for all RPC nodes. If you change the password for an RPC node, make sure you propagate that change to the RPC node at each of the other sites. Maximum length: 31 characters.

To change the password of an RPC node by using the configuration utility

1. In the navigation pane, expand Network, and then click RPC.
2. In the details pane, click the RPC node for which you want to change the password, and then click Open.
3. In the Configure RPC Node dialog box, in Password and Confirm Password, specify the password that you want the RPC node to use.

Encrypting the Exchange of Site Metrics

You can secure the information that is exchanged between GSLB sites by setting the secure option for the RPC nodes in the GSLB setup. With the secure option set, the NetScaler appliance encrypts all communication sent from the node to other RPC nodes.

To encrypt the exchange of site metrics by using the command line interface

At the command prompt, type the following commands to encrypt the exchange of site metrics and verify the configuration:

- set ns rpcNode <IPAddress> [-secure (YES | NO)]
- show rpcNode

Example

```
> set rpcNode 192.0.2.4 -secure YES
 Done
>
> show rpcNode
.
.
.
3) IPAddress: 192.0.2.4 Password: d336004164d4352ce39e SrcIP: 192.0.2.3 Secure: ON
 Done
>
```

To unset the secure parameter by using the command line interface

To unset the secure parameter by using the NetScaler command line, type the unset rpcNode command, the IP address of the RPC node, and the secure parameter, without a value.

Parameters for encrypting the exchange of site metrics

IPAddress

The IP address of the GSLB site to which the RPC node belongs. This is the value of the `IPAddress` field in the output of the `show rpcNode` CLI command.

secure (Secure)

Encrypt all communication sent from the RPC node. Possible values: YES, NO. Default: NO.

To encrypt the exchange of site metrics by using the NetScaler configuration utility

1. In the navigation pane, expand Network, and then click RPC.
2. In the details pane, click the RPC node whose communication you want to encrypt, and then click Open.
3. In the Configure RPC Node dialog box, click Secure.
4. Click OK.

Configuring the Source IP Address for an RPC Node

By default, the NetScaler appliance uses a NetScaler-owned subnet IP (SNIP) address or mapped IP (MIP) address as the source IP address for an RPC node, but you can configure the appliance to use a specific SNIP address or MIP address. If neither a SNIP address nor a MIP address is available, the GSLB site cannot communicate with other sites. In such a scenario, you must configure either the NetScaler IP (NSIP) address or a virtual IP (VIP) address as the source IP address for an RPC node. A VIP address can be used as the source IP address of an RPC node only if the RPC node is a remote node. If you configure a VIP address as the source IP address and remove the VIP address, the appliance uses a SNIP address or a MIP address.

To specify a source IP address for an RPC node by using the command line interface

At the command prompt, type the following commands to change the source IP address for an RPC node and verify the configuration:

- set ns rpcNode <IPAddress> [-srcIP <ip_addr|ipv6_addr|*>]
- show ns rpcNode

Example

```
> set rpcNode 192.0.2.4 -srcIP 192.0.2.3
 Done
> show rpcNode
.
.
.
2)  IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e SrcIP:  192.0.2.3       Secure:  OFF
 Done
>
```

To unset the source IP address parameter by using the command line interface

To unset the source IP address parameter by using the NetScaler command line, type the unset rpcNode command, the IP address of the RPC node, and the srcIP parameter, without a value.

Parameters for specifying a source IP address of an RPC node

IPAddress

The IP address of the GSLB site to which the RPC node belongs. This is the value of the `IPAddress` field in the output of the `show rpcNode` CLI command.

srcIP

The subnet IP (SNIP) address, mapped IP (MIP) address, NetScaler IP (NSIP) address, or virtual IP (VIP) address that you want the appliance to use as the source IP address for exchanging site metrics. By default, the appliance uses a SNIP address or a MIP address, but you can configure the node to use a SNIP address or MIP address of your choice, or the NSIP address. For a remote node, you also have the option of configuring a VIP address as the source IP address. If neither a SNIP address nor a MIP address is available, and you have not configured a source IP address, a GSLB site cannot exchange site metrics with other sites. The default setting is an asterisk (*), which indicates that the default setting (SNIP address or MIP address) is being used.

To specify a source IP address for an RPC node by using the NetScaler configuration utility

1. In the navigation pane, expand Network, and then click RPC.
2. In the details pane, click the RPC node for which you want to assign a specific source IP address for site metrics exchange, and then click Open.
3. In the Configure RPC Node dialog box, in Source IP Address, enter the IP address that you want the RPC node to use as the source IP address.

Customizing Your GSLB Configuration

Once your basic GSLB configuration is operational, you can customize it by modifying the bandwidth of a GSLB service, configuring CNAME based GSLB services, static proximity, dynamic RTT, persistent connections, or dynamic weights for services, or changing the GSLB Method.

You can also configure monitoring for GSLB services to determine their states.

These settings depend on your network deployment and the types of clients you expect to connect to your servers.

Modifying Maximum Connections or Maximum Bandwidth for a GSLB Service

You can restrict the number of new clients that can simultaneously connect to a load balancing or content switching virtual server by configuring the maximum number of clients and/or the maximum bandwidth for the GSLB service that represents the virtual server.

To modify the maximum clients or bandwidth of a GSLB service by using the command line interface

At the command prompt, type the following command to modify the maximum number of client connections or the maximum bandwidth of a GSLB service and verify the configuration:

- set gslb service <serviceName> [-maxClients <positive_integer>] [-maxBandwidth <positive_integer>]
- show gslb service <serviceName>

Example

```
set glsb service Service-GSLB-1 –maxBandwidth 100 –maxClients 100
show gslb service Service-GSLB-1
```

Parameters for modifying the maximum clients or bandwidth of a GSLB service

maxClients

The maximum number of simultaneous client connections that the GSLB service can handle.

maxBandwidth

The maximum bandwidth, in kbps, that a GSLB service can handle.

To modify the maximum clients or bandwidth of a GSLB service by using the configuration utility

1. In the navigation pane, expand GSLB and click Services.
2. In the details pane, select the service to be modified and click Open.
3. In the Configure GSLB Service dialog box specify values for one or both of the following parameters, which correspond to parameters described in “Parameters for modifying the maximum clients or bandwidth for a service” as shown:
   - Max Clients—maxClients
   - Max Bandwidth—maxBandwidth
4. Click OK.
5. Verify that the Details area displays the values that you entered.

Creating CNAME-Based GSLB Services

To configure a GSLB service, you can use the IP address of the server or a canonical name of the server. If you want to run multiple services (like an FTP and a Web server, each running on different ports) from a single IP address or run multiple HTTP services on the same port, with different names, on the same physical host, you can use canonical names (CNAMES) for the services.

For example, you can have two entries in DNS as ftp.example.com and www.example.com for FTP services and HTTP services on the same domain, example.com. CNAME-based GSLB services are useful in a multilevel domain resolver configuration or in multilevel domain load balancing. Configuring a CNAME-based GSLB service can also help if the IP address of the physical server is likely to change.

If you configure CNAME-based GSLB services for a GSLB domain, when a query is sent for the GSLB domain, the NetScaler appliance provides a CNAME instead of an IP address. If the A record for this CNAME record is not configured, the client must query the CNAME domain for the IP address. If the A record for this CNAME record is configured, the NetScaler provides the CNAME with the corresponding A record (IP address). The NetScaler appliance handles the final resolution of the DNS query, as determined by the GSLB method. The CNAME records can be maintained on a different NetScaler appliance or on a third-party system.

In an IP-address-based GSLB service, the state of a service is determined by the state of the server that it represents. However, a CNAME-based GSLB service has its state set to UP by default; the virtual server IP (VIP) address or metric exchange protocol (MEP) are not used for determining its state. If a desktop-based monitor is bound to a CNAME-based GSLB service, the state of the service is determined according to the result of the monitor probes.

You can bind a CNAME-based GSLB service only to a GSLB virtual server that has the DNS Record Type as CNAME. Also, a NetScaler appliance can contain at most one GSLB service with a given CNAME entry.

The following are some of the features supported for a CNAME-based GSLB service:

- GSLB-policy based site affinity is supported, with the CNAME as the preferred location.
- Source IP persistence is supported. The persistency entry contains the CNAME information instead of the IP address and port of the selected service.

The following are the limitations of CNAME-based GSLB services:

- Site persistence is not supported, because the service referenced by a CNAME can be present at any third-party location.
- Multiple-IP-address response is not supported because one domain cannot have multiple CNAME entries.
- Source IP Hash and Round Robin are the only load balancing methods supported. The Static Proximity method is not supported because a CNAME is not associated with an IP address and static proximity can be maintained only according to the IP addresses.

Note: The Empty-Down-Response feature should be enabled on the GSLB virtual server to which you bind the CNAME-based GSLB service. If you enable the Empty-Down-Response feature, when a GSLB virtual server is DOWN or disabled, the response to a DNS query, for the domains bound to this virtual server, contains an empty record without any IP addresses, instead of an error code.

To create a CNAME-based GSLB service by using the command line interface

At the command prompt, type:

add gslb service <serviceName> -cnameEntry <string> -siteName <string>

Example

add gslb service Service-GSLB-1 -cnameEntry transport.mycompany.com -siteName Site-GSLB-East-Coast
add gslb service Service-GSLB-2 -cnameEntry finance.mycompany.com -siteName Site-GSLB-West-Coast

Parameters for creating a CNAME based GSLB service

serviceName (Service Name)

The name of the CNAME-based GSLB service being configured.

cnameEntry (DNS Canonical Name)

The canonical name of the GSLB domain that the GSLB service will handle.

siteName (Site Name)

The name of the GSLB site that the GSLB service represents.

To create a CNAME-based GSLB service by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Services.
2. In the details pane, click Add.
3. In the Create GSLB Service dialog box, set the following parameters:
   - Service Name*
   - Site Name*
   - Type should be Canonical name based.
   - DNS Canonical name*

   * A required parameter
4. Click Create, and then click Close.

Changing the GSLB Method

Unlike traditional DNS servers that simply respond with the IP addresses of the configured servers, a NetScaler appliance configured for GSLB responds with the IP addresses of the services, as determined by the configured GSLB method. By default, the GSLB virtual server is set to the least connection method. If all GSLB services are down, the NetScaler responds with the IP addresses of all the configured GSLB services.

GSLB methods are algorithms that the GSLB virtual server uses to select the best-performing GSLB service. After the host name in the Web address is resolved, the client sends traffic directly to the resolved service IP address.

The NetScaler appliance provides the following GSLB methods:

- Round Robin
- Least Connections
- Least Response Time
- Least Bandwidth
- Least Packets
- Source IP Hash
- Custom Load
- Round Trip Time (RTT)
- Static Proximity

For GSLB methods to work with a remote site, either MEP must be enabled or explicit monitors must be bound to the remote services. If MEP is disabled, RTT, Least Connections, Least Bandwidth, Least Packets and Least Response Time methods default to Round Robin.

The Static Proximity and RTT load balancing methods are specific to GSLB.

Specifying a GSLB Method Other than Static Proximity or Dynamic (RTT)

For information about the Round Robin, Least Connections, Least Response Time, Least Bandwidth, Least Packets, Source IP Hash, or Custom Load method, see "Load Balancing."

To change the GSLB method by using the command line interface

At the command prompt, type:

set gslb vserver <name> -lbMethod GSLBMethod

Example

set gslb vserver Vserver-GSLB-1 -lbMethod ROUNDROBIN

To change the GSLB method by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the details pane, select a GSLB virtual server and click Open.
3. In the Configure GSLB Virtual Server dialog box, on the Method and Persistence tab, under Method, select a method from the Choose Method list.
4. Click OK, and verify that the method you selected appears under Details at the bottom of the screen.

Configuring Static Proximity

The static proximity method for GSLB uses an IP-address based static proximity database to determine the proximity between the client's local DNS server and the GSLB sites. The NetScaler appliance responds with the IP address of a site that best matches the proximity criteria.

If two or more GSLB sites at different geographic locations serve the same content, the NetScaler appliance maintains a database of IP address ranges and uses the database for decisions about the GSLB sites to which to direct incoming client requests.

For the static proximity method to work, you must either configure the NetScaler appliance to use an existing static proximity database populated through a location file or add custom entries to the static proximity database. After adding custom entries, you can set their location qualifiers. After configuring the database, you are ready to specify static proximity as the GSLB method.

Adding a Location File to Create a Static Proximity Database

A static proximity database is a UNIX-based ASCII file. Entries added to this database from a location file are called static entries. Only one location file can be loaded on a NetScaler appliance. Adding a new location file overrides the existing file. The number of entries in the static proximity database is limited by the configured memory in the NetScaler appliance.

The static proximity database can be created in the default format or in a format derived from commercially configured third party databases (such as www.maxmind.com and www.ip2location.com).

These databases vary in the details they provide. There is no strict enforcement of the database file format, except that the default file has format tags. The database files are ASCII files that use a comma as the field delimiter. There are differences in the structure of fields and the representation of IP addresses in the locations.

The format parameter describes the structure of the file to the NetScaler appliance. Specifying an incorrect value for the format option can corrupt the internal data.

Note: The default location of the database file is /var/netscaler/locdb, and on a high availability (HA) setup, an identical copy of the file must be present in the same location on both NetScaler appliances.

The following abbreviations are used in this section:

- **CSHN**. Short name of a country based on the country code standard of ISO-3166.
- **LCN**. Long name of the country.
- **RC**. Region code based on ISO-3166-2 (for US and Canada). The region code “FIPS-10-4” is used for the other regions.

Note: Some databases provide short country names according to ISO-3166 and long country names as well. The NetScaler uses short names when storing and matching qualifiers.

To create a static proximity database, log on to the UNIX shell of the NetScaler appliance and use an editor to create a file with the location details in one of the NetScaler-supported formats.

To add a static location file by using the command line interface

At the command prompt, type:

- add locationFile <locationFile> [-format <format>]

- show locationFile

Example

```
> add locationFile /var/nsmap/locdb/nsgeo1.0 -format netscaler
 Done
> show locationFile
Location File: /var/nsmap/locdb/nsgeo1.0
Format: netscaler
 Done
>
```

Parameters for adding a static location file

locationFile

The name of the location file. Must include the absolute path to the file. If the full path is not given, the default path /var/netscaler/locdb is assumed. In a high availability setup, the static database must be stored in the same location on both systems.

format

The format of the location file. Possible values: netscaler, ip-country, ip-country-isp, ip-country-region-city, ip-country-region-city-isp, geoip-country, geoip-region, geoip-city, geoip-country-org, geoip-country-isp, geoip-city-isp-org. Default: netscaler.

To add a static location file by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Location.
2. In the details pane, click the Static Database tab, and then click Add.
3. In the Create Location File dialog box, in the Location Filename text box, type the name of the location file, or click Browse to select the location file (for example, type or select /var/nsmap/locdb/nsgeo1.0).

   Note: The location file must be existing on the NetScaler appliance.
4. In the Location Format box, select the format of the location (for example, netscaler).
5. Click Create and click Close.

You can view an imported location file database by using the View Database dialog box in the configuration utility. There is no NetScaler command line equivalent.

To view a static location file by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Location.
2. On the Static Database tab, select the location file, and then click View Database.
3. In the View Database dialog box, and click Find to use the following controls to filter and sort the database information.
   a. **Search In**. Choose the field to search from the drop-down list.
   b. **Criterion**. Choose the search criterion from the drop-down list. The list contains a standard set of search criteria. "Contains" is the default choice.
   c. **Look For**. Type the text or number to search for.
   d. **Find Now**. Click this button to perform the search.
   e. **Clear**. Click this button to reset the search controls to their initial state.
4. Click Close to close the View Database dialog box and return to the Static Database tab.

To convert a location file into the netscaler format

By default, when you add a location file, it is saved in the netscaler format. You can convert a location file of other formats into the netscaler format. See the list of supported formats in the table, Parameters for adding a static location file.

Note: The nsmap option can be accessed only from the command line interface. The conversion is possible only into the netscaler format.

To convert the static database format, at the NetScaler command prompt, type the following command:

nsmap -f <inputFileFormat> -o <outputFileName> <inputFileName>

Example

nsmap -f ip-country-region-city -o nsfile.ns ip-country-region-city.cvs

Adding Custom Entries to a Static Proximity Database

Custom entries take precedence over static entries in the proximity database. You can add a maximum of 50 custom entries. For a custom entry, denote all omitted qualifiers with an asterisk (*) and, if qualifiers have a period or space in the name, enclose the parameter in double quotation marks. The first 31 characters are evaluated for each qualifier. You can also provide the longitude and latitude of the geographical location of the IP address-range for selecting a service with the static proximity GSLB method.

To add custom entries by using the command line interface

At the command prompt, type the following commands to add a custom entry to the static proximity database and verify the configuration:

- add location < IPfrom> < IPto> <preferredLocation> [-longitude <integer>[-latitude <integer>]]
- show location

Example

```
>add location 192.168.100.1 192.168.100.100 *.us.ca.mycity

>show location
```

Parameters for adding custom entries

IPfrom

First IP address in the range, in dotted decimal notation. This is a mandatory argument.

IPto

Last IP address in the range, in dotted decimal notation. This is a mandatory argument.

preferredLocation

String of qualifiers, in dotted notation, describing the geographical location of the IP address range. Each qualifier is more specific than the one that precedes it, as in continent.country.region.city.isp.organization. For example,"NA.US.CA.San Jose.ATT.citrix".

Note: A qualifier that includes a dot (.) or space ( ) must be enclosed in double quotation marks.

This is a mandatory argument. Maximum Length: 197

longitude

Numerical value, in degrees, specifying the longitude of the geographical location of the IP address-range.

Note: Longitude and latitude parameters are used for selecting a service with the static proximity GSLB method. If they are not specified, selection is based on the qualifiers specified for the location.

Maximum value: 180

latitude

Numerical value, in degrees, specifying the latitude of the geographical location of the IP address-range.

Note: Longitude and latitude parameters are used for selecting a service with the static proximity GSLB method. If they are not specified, selection is based on the qualifiers specified for the location.

Maximum value: 180

To add custom entries by using the configuration utility

1. Navigate to GSLB > Location.
2. On the Custom Entries tab, click Add.
3. Specify values for the following parameters, which correspond to parameters described in “Parameters for adding custom entries” as shown:
   - From IP Address*—IPfrom
   - To IP Address*—IPto
   - Location Name*—preferredLocation

   * A required parameter
4. Click Create, and then click Close. The custom entry that you have created appears on the Custom Entries tab.

Setting the Location Qualifiers

The database used to implement static proximity contains the location of the GSLB sites. Each location contains an IP address range and up to six qualifiers for that range. The qualifiers are literal strings and are compared in a prescribed order at run time. Every location must have at least one qualifier. The meaning of the qualifiers (context) is defined by the qualifier labels, which are user defined. The NetScaler has two built-in contexts:

Geographic context, which has the following qualifier labels:

- Qualifier 1 – “Continent”
- Qualifier 2 – “Country”
- Qualifier 3 – “State”
- Qualifier 4 – “City”
- Qualifier 5 – “ISP”
- Qualifier 6 – “Organization”

Custom entries, which have the following qualifier labels:

- Qualifier 1 – “Qualifier 1”
- Qualifier 2 – “Qualifier 2”
- Qualifier 3 – “Qualifier 3”
- Qualifier 4 – “Qualifier 4”
- Qualifier 5 – “Qualifier 5”
- Qualifier 6 – “Qualifier 6”

If the geographic context is set with no Continent qualifier, Continent is derived from Country. Even the built-in qualifier labels are based on the context, and the labels can be changed. These qualifier labels specify the locations mapped with the IP addresses used to make static proximity decisions.

To perform a static proximity-based decision, the NetScaler appliance compares the location attributes (qualifiers) derived from the IP address of the local DNS server resolver with the location attributes of the participating sites. If only one site matches, the appliance returns the IP address of that site. If there are multiple matches, the site selected is the result of a round robin on the matching GSLB sites. If there is no match, the site selected is a result of a round robin on all configured sites. A site that does not have any qualifiers is considered a match.

To set the location qualifiers by using the command line interface

At the command prompt, type:

set locationparameter -context <context> -q1label <string> [-q2label <string>] [-q3label <string>] [-q4label <string>] [-q5label <string>] [-q6label <string>]

Example

set locationparameter -context custom -q1label asia

Parameters for setting the location qualifiers

context

The context in which a static proximity decision is made. Possible Values: geographic, custom.

q1label

The label for the 1st qualifier.

q2label

The label for the 2nd qualifier.

q3label

The label for the 3rd qualifier.

q4label

The label for the 4th qualifier.

q5label

The label for the 5th qualifier.

q6label

The label for the 6th qualifier.

To set the location qualifiers by using the configuration utility

1. In the navigation pane, expand GSLB and click Location.
2. Click Location Parameters.
3. In the Context drop-down list, select the appropriate context (for example, Custom).
4. In the Qualifier Label -1 text box, type the qualifier (for example asia).
5. Click OK.

Specifying the Proximity Method

When you have configured the static proximity database, you are ready to specify static proximity as the GLSB method.

To specify static proximity by using the command line interface

At the command prompt, type the following commands to configure static proximity and verify the configuration:

- set gslb vserver <name> -lbMethod STATICPROXIMITY
- show gslb vserver <name>

Example

```
set gslb vserver Vserver-GSLB-1 -lbMethod STATICPROXIMITY
show gslb vserver
```

To specify static proximity by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the GSLB Virtual Servers pane, select the GSLB Virtual Server that you want to set to static proximity (for example, vserver-GSLB-1).
3. Click Open.
4. On the Method and Persistence tab, under Method, select Static Proximity from the Choose Method list.
5. Click OK.
6. Verify that the Details pane shows static proximity as the GSLB method.

Synchronizing GSLB Static Proximity Database

Synchronizing a global server load balancing (GSLB) static proximity database requires that one of the sites be identified as the master GSLB node. Any site in the topology can be designated as the master node. The rest of the GSLB nodes are automatically designated as slave nodes.

Synchronizing GSLB static proximity databases synchronizes the files in the /var/netscaler/locdb directory across the slave nodes. During the synchronization process, the master node fetches the running configuration from each of the slave nodes and compares it to the configuration on the master node. The master GSLB node uses the rsync program to synchronize the static proximity database across the slave nodes. To speed up the synchronization process, the rsync program makes only enough changes to eliminate the differences between the two files. The synchronization process cannot be rolled back.

The following example synchronizes Site2, which is a slave site, to master site Site1. The administrator enters the **sync gslb config** command on Site1:

```
sync gslb config -nowarn
Sync Time: Feb 24 2014 14:56:16
Retrieving local site info: ok
Retrieving all participating gslb sites info:
0 bytes in 0 blocks
ok
site1[Master]:
      Getting Config: ok
site2[Slave]:
      Syncing gslb static proximity database: ok
      Getting Config: ok
      Comparing config: ok
      Applying changes: ok
 Done
```

Configuring the Dynamic Method (RTT)

Dynamic round trip time (RTT) is a measure of time or delay in the network between the client's local DNS server and a data resource. To measure dynamic RTT, the NetScaler appliance probes the client's local DNS server and gathers RTT metric information. The appliance then uses this metric to make its load balancing decision. Global server load balancing monitors the real-time status of the network and dynamically directs the client request to the data center with the lowest RTT value.

When a client's DNS request for a domain comes to the NetScaler appliance configured as the authoritative DNS for that domain, the appliance uses the RTT value to select the IP address of the best performing site to send it as a response to the DNS request.

The NetScaler appliance uses different mechanisms, such as ICMP echo request / reply (PING), UDP, and TCP to gather the RTT metrics for connections between the local DNS server and participating sites. The appliance first sends a ping probe to determine the RTT. If the ping probe fails, a DNS UDP probe is used. If that probe also fails, the appliance uses a DNS TCP probe.

These mechanisms are represented on the Netscaler appliance as Load Balancing Monitors and are easily identified due to their use of the "ldns" prefix. The three monitors, in their default order, are:

- ldns-ping
- ldns-dns
- ldns-tcp

These monitors are built in to the appliance and are set to safe defaults, but may be customized just like any other monitor on the appliance.

The default order may also be changed by setting it explicitly as a GSLB parameter. For example, to set the order to be the DNS UDP query followed by the PING and then TCP, type the following command:

set gslb parameter -ldnsprobeOrder DNS PING TCP

Unless they have been customized, the NetScaler appliance performs UDP and TCP probing on port 53, however unlike regular load balancing monitors the probes need not be successful in order to provide valid RTT information. ICMP port unavailable messages, TCP Resets and DNS error responses, which would usually constitute a failure are all acceptable for calculating the RTT value.

Once the RTT data has been compiled, the Netscaler uses the proprietary metrics exchange protocol (MEP) to exchange RTT values between participating sites. After calculating RTT metrics, the appliance sorts the RTT values to identify the data center with the best (smallest) RTT metric."

If RTT information is not available (for example, when a client's local DNS server accesses the site for the first time), the NetScaler appliance selects a site by using the round robin

method and directs the client to the site.

To configure the dynamic method, you configure the site's GSLB virtual server for dynamic RTT. You can also set the interval at which local DNS servers are probed to a value other than the default.

Configuring a GSLB Virtual Server for Dynamic RTT

To configure a GSLB virtual server for dynamic RTT, you specify the RTT load balancing method.

The NetScaler appliance regularly validates the timing information for a given local server. If a change in latency exceeds the configured tolerance factor, the appliance updates its database with the new timing information and sends the new value to other GSLB sites by performing a MEP exchange. The default tolerance factor is 5 milliseconds (ms).

The RTT tolerance factor must be the same throughout the GSLB domain. If you change it for a site, you must configure identical RTT tolerance factors on all NetScaler appliances deployed in the GSLB domain.

To configure a GSLB virtual server for dynamic RTT by using the command line interface

At the command prompt, type:

set gslb vserver <name> -lbMethod RTT -tolerance <value>

Example

set gslb vserver Vserver-GSLB-1 -lbMethod RTT -tolerance 10

Parameters for configuring the dynamic RTT load balancing method

name

The name of the GSLB virtual server for which you are configuring the load balancing method.

lbMethod

The load balancing method being configured for the GSLB virtual server. For the dynamic method, specify RTT.

tolerance

The minimum number of milliseconds by which the RTT metric must change to trigger an update of this metric in the database.

To configure a GSLB virtual server for dynamic RTT by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the GSLB Virtual Servers pane, select the GSLB Virtual server that you want to set to dynamic RTT (for example, vserver-GSLB-1).
3. Click Open.
4. On the Method and Persistence tab, under Method, select Dynamic Method (RTT) from the Choose Method list.
5. To change the tolerance factor, type the new value in the Tolerance (ms) text box. (For a description of the tolerance factor, see “Parameters for configuring the dynamic RTT load balancing method.”)
6. Click OK.

Setting the Probing Interval of Local DNS Servers

The NetScaler appliance uses different mechanisms, such as ICMP echo request / reply (PING), TCP, and UDP to obtain RTT metrics for connections between the local DNS server and participating GSLB sites. By default, the appliance uses a ping monitor and probes the local DNS server every 5 seconds. The appliance then waits 2 seconds for the response and, if a response is not received in that time, it uses the TCP DNS monitor for probing.

However, you can modify the time interval for probing the local DNS server to accommodate your configuration.

To modify the probing interval by using the command line interface

At the command prompt, type:

set lb monitor <monitorName> <type> -interval <integer> <units> -resptimeout <integer> <units>

Example

set lb monitor monitor-HTTP-1 HTTP -interval 10 sec -resptimeout 5 sec

Parameters for modifying the probing interval

interval

Interval at which probes should be sent.

units

monitor-interval/resptimeout units. Possible values are SEC, MSEC,and MIN. Default value is NSTMUNT_SEC.

type

The type of monitor being configured. The following are valid monitor types:

- **TCP** - The NetScaler appliance establishes a TCP connection with the monitor destination and then closes the connection. If the NetScaler observes TCP traffic to the destination, it does not send TCP monitoring requests. This occurs if LRTM is

disabled. By default, LRTM is disabled on this monitor. This is done only for UDP, and the service goes down immediately.

- **TCP-ECV** - The NetScaler appliance establishes a TCP connection with the monitor destination. When the connection is established, the appliance sends specific data to the service by using the -send parameter, and the appliance and expects a specific response through the receive parameter.

- **HTTP** - the NetScaler establishes a TCP connection with the monitor destination. After the connection is established, the NetScaler sends HTTP requests and compares the response code, in the response from the service, with the configured set of response codes.

- **HTTP-ECV** - the NetScaler establishes a TCP connection with the monitor destination. When the connection is established, the NetScaler sends the HTTP data specified by the -send parameter to the service and expects the HTTP response that the -receive parameter specifies. (HTTP body part, not including HTTP headers.) Empty response data matches any response. Expected data may be anywhere in the first 24K bytes of the HTTP body of the response.

- **PING** - the NetScaler sends an ICMP echo request to the destination of the monitor and expects an ICMP echo response.

Note: The NetScaler also supports FTP, UDP, DNS, UDP-ECV, TCPS, HTTPS, TCPS-ECV, HTTPS-ECV, LDNS-PING, LDNS-TCP, and LDNS-DNS monitors.

For more information about monitors, see Load Balancing.

resptimeout

Interval after which probe should be marked as FAILED.

To modify the probing interval by using the configuration utility

- In the navigation pane, expand Load Balancing and click Monitors.
- Select the monitor that you want to modify (for example, ping).
- Click Open.
- In the Configure Monitor dialog box, on the Standard Parameters tab, specify values for the following parameters, which correspond to parameters described in “Parameters for modifying the probing interval” as shown:
  - Interval—interval
  - Response Time-out—resptimeout (type the interval after which the probe should be marked as FAILED. Specify whether the value represents minutes, milliseconds, or seconds by selecting a value from the adjacent list)
- Click OK.

Overriding Static Proximity Behavior by Configuring Preferred Locations

You might want to direct traffic from a local DNS (LDNS) server or network to a GSLB service other than the GSLB service that the static proximity method selects for that traffic. That is, you have a *preferred location* for that traffic. To override the static proximity method with preferred locations, you can do the following:

1. Configure a DNS action that consists of a list of preferred locations. For more information about configuring a DNS action, see Configuring a DNS Action.

2. Configure a DNS policy to identify the traffic arriving from the LDNS server or network for which you want to override static proximity, and apply the action in the policy.

3. Bind the policy to the global request bind point.

In the DNS action, you can configure a list of up to 8 preferred locations. The locations must be provided in the dotted qualifier notation, which is the notation in which you add custom locations to the static proximity database. The locations can include wildcards for qualifiers that you want to omit. For information about the dotted qualifier notation for locations, see Adding Custom Entries to a Static Proximity Database. When entering the preferred locations, you must enter them in the descending order of priority.

When a policy evaluates to TRUE, the NetScaler appliance matches the preferred locations, in priority order, with the locations of GSLB services. Matches are of the following two types:

- If all the non-wildcard qualifiers in a preferred location match the corresponding qualifiers in the location of a GSLB service, the match is considered a perfect match. For example, a GSLB service location of `*.UK.*.*` or `Europe.UK.*.*` is a perfect match for the preferred location `*.UK.*.*`.

- If only a subset of the non-wildcard qualifiers match, the match is considered a partial match. For example, a GSLB service location of `Europe.EG` is a partial match for the preferred location `Europe.UK`.

When a DNS policy evaluates to TRUE, the following algorithm is used to select a GSLB service:

1. The appliance evaluates the preferred location that has the highest priority and moves down the priority order until a perfect match is found between a preferred location and the location of a GSLB service.

   If a perfect match is found, the appliance checks whether the corresponding GSLB service is up. If it is up, it returns the IP address of the GSLB service in the DNS response. If multiple perfect matches are found (which can happen when one or more wildcards are used in a preferred location), the appliance checks the state of each of the corresponding GSLB services and load balances the GSLB services that are up.

2. If a perfect match is not found for any of the preferred locations, the appliance returns to the preferred location that has the highest priority and moves down the priority order until a partial match is found between a preferred location and the location of a GSLB service.

   If a partial match is found, the appliance checks whether the corresponding GSLB service is up. If it is up, it returns the IP address of the GSLB service in the DNS response. If multiple partial matches are found, the appliance checks the state of each of the corresponding GSLB services and load balances the GSLB services that are up.

3. If none of the perfect and partial matches are up, the appliance load balances all other available GSLB services.

In this way, the appliance implements a type of site affinity for traffic that matches the DNS policy.

Example

Consider a GSLB configuration that consists of the following eight GSLB services:

- Asia.IN
- Asia.JPN
- Asia.HK
- Europe.UK
- Europe.RU
- Europe.EG
- Africa.SD
- Africa.ZMB

Further consider the following DNS action and policy configuration:

```
> add dns action prefLoc11 GslbPrefLoc -preferredLocList "Asia.HK" "Europe.UK"
 Done
> add dns policy dnsPolPrefLoc "CLIENT.IP.SRC.MATCHES_LOCATION(\"*.ZMB.*.*\")" prefLoc11
 Done
```

When the appliance receives a request from the location `*.ZMB.*.*`, the preferred locations are evaluated as follows:

1. The appliance attempts to find a GSLB service whose location is a perfect match for `Asia.HK`, which is the preferred location that has the highest priority. It finds that the GSLB service at Asia.HK is a perfect match. If the GSLB service is up, it sends the client the IP address of the GSLB service.

2. If the GSLB service at Asia.HK is down, the appliance attempts to find a perfect match for the second preferred location, `Europe.UK`. It finds that the GSLB service at Europe.UK is a perfect match. If the GSLB service is up, it sends the client the IP address of the service.

3. If the GSLB service at Europe.UK is down, it returns to the preferred location that has the highest priority, `Asia.HK`, and looks for partial matches. For `Asia.HK`, it finds that Asia.IN and Asia.JPN are partial matches. If only one of the corresponding GSLB services is up, it sends the client the IP address of the service. If both locations are up, it load balances the two services.

4. If all partial matches for `Asia.HK` are down, the appliance looks for partial matches for `Europe.UK`. It finds that Europe.RU and Europe.EG are partial matches for the preferred location. If only one of the corresponding GSLB services is up, it sends the client the IP address of the service. If both locations are up, it load balances the two services.

5. If all partial matches for `Europe.UK` are down, the appliance load balances all other available GSLB services. In the current example, the appliance load balances Africa.SD and Africa.ZMB because the remaining six GSLB services have been found to be down.

Configuring Persistent Connections

Persistence ensures that a series of client requests for a particular domain name is sent to the same data center instead of being load balanced. If persistence is configured for a particular domain, it takes precedence over the configured GSLB method. Persistence is useful for deployments that deal with e-commerce, such as shopping card usage, where the server needs to maintain the state of the connection to track the transaction. To maintain the state of connection, you must configure persistence on a virtual server. With persistence configured, NetScaler selects a data center to process a client request and forwards the IP address of the selected data center for all subsequent DNS requests. If the configured persistence applies to a site that is down, the NetScaler appliance uses a GSLB method to select a new site, and the new site becomes persistent for subsequent requests from the client.

The GSLB virtual server is responsible for DNS-based site persistence, and it controls the site persistence for a remote GSLB service. The NetScaler appliance supports persistence based on the source IP address or on HTTP cookies.

When you bring a physical service DOWN with a delay time, the physical service goes into the transition out of service (TROFS) state. Site persistence is supported as long as the service is in the TROFS state. That is, if the same client sends a request for the same service within the specified delay time after a service is marked TROFS, the same GSLB site (data center) services the request.

Note: If connection proxy is specified as the site persistence method and if you also want to configure persistence of the physical servers, do not configure SOURCEIP persistence. When the connection is proxied, an IP address owned by the NetScaler is used, and not the actual IP address of the client. Configure methods such as cookie persistence or rule-based persistence on the load balancing virtual server.

Configuring Persistence Based on Source IP Address

With source-IP persistence, when a DNS request is received at a data center, the NetScaler appliance first looks for an entry in the persistence table and, if an entry for the local DNS server exists and the server mentioned in the entry is configured, the IP address of that server is sent as the DNS response.

For the first request from a particular client, the NetScaler appliance selects the best GSLB site for the request and sends its IP address to the client. Since persistence is configured for the source IP address of the client, all subsequent requests by that client or another local DNS server in the same IP subnet are sent the IP address of the GSLB site that was selected for the first request.

For source-IP address based persistence, the same set of persistence identifiers must be configured on the GSLB virtual servers in all data centers. A persistence identifier is a number used by the data centers to identify a particular GSLB virtual server. A cookie transmits the persistence identifier, enabling the NetScaler appliance to identify the domain so that it can forward all appropriate requests to the same domain. When persistence is enabled, the persistence information is also exchanged as part of metrics exchange.

For the NetScaler appliance to support persistence across sites, persistence must be enabled on the GSLB virtual servers of all participating sites. When you use source IP address persistence on the network identifier, you must configure a subnet mask. For any domain, persistence takes precedence over any other configured GSLB method.

To configure persistence based on source IP address by using the command line interface

At the command prompt, type:

set gslb vserver <name> -persistenceType (SOURCEIP|NONE) -persistenceId <positive_integer> [-persistMask <netmask>] –[timeout <mins>]

Example

set gslb vserver vserver-GSLB-1 -persistenceType SOURCEIP -persistenceId 23 -persistMask 255.255.255.255 -t

Parameters for configuring persistence based on source IP address

name

The name of the GSLB virtual server for which you are configuring source IP address based persistence.

persistenceType

The type of persistence being configured for the GSLB virtual server. Possible Values: SOURCEIP, None.

persistenceID

A positive integer used to identify the GSLB virtual server on all sites. Minimum value: 1. Maximum value: 65535.

persistMask

The subnet mask used when SOURCEIP based persistence is enabled. Minimum Value: 128.0.0.0. Default: 0xFFFFFFFF.

timeout

The time, in minutes, for which persistence should be in effect for the GSLB virtual server. Minimum value: 2. Maximum value: 1440. Default: 2.

To configure persistence based on source IP address by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the GSLB Virtual Servers pane, select the GSLB virtual server whose method you want to change (for example, vserver-GSLB-1).
3. Click Open.
4. On the Method and Persistence tab, under Persistence, select SOURCEIP from the Persistence list and specify values for the following parameters, which correspond to parameters described in “Parameters for configuring persistence based on source IP address” as shown:
   - Time-out—timeout
   - Persistence Id—persistenceID
   - IPv4 Netmask or IPv6 Mask length—persistMask
5. Click OK.

Configuring Persistence Based on HTTP Cookies

The NetScaler appliance provides persistence at the HTTP-request level by using connection proxy and HTTP redirect. With these persistence methods, the appliance uses an HTTP cookie (known as a “site cookie”) to reconnect the client to the same server. The NetScaler inserts the site cookie in the first HTTP response.

The site cookie contains information about the selected GSLB service on which the client has a persistent connection. The cookie expiration is based on the cookie timeout configured on the NetScaler appliance. If the virtual server names are not identical on all the sites, you must use the persistence identifier. Cookies inserted are compliant with RFC 2109.

When the NetScaler appliance responds to a client DNS request by sending the IP address of the selected GSLB site, the client sends an HTTP request to that GSLB site. The physical server in that GSLB site adds a site cookie to the HTTP header, and connection persistence is in effect.

If the DNS entry in the client cache expires, and then the client sends another DNS query and is directed to a different GSLB site, the new GSLB site uses the site cookie present in the client request header to implement persistence. If the GSLB configuration at the new site uses connection-proxy persistence, the new site creates a connection to the GSLB site that inserted the site cookie, proxies the client request to the original site, receives a response from the original GSLB site, relays that response back to the client, and closes the connection. If the GSLB configuration uses HTTP redirect persistence, the new site redirects the request to the site that originally inserted the cookie.

Note: Connection proxy persistence can be configured only for local services. However, connection proxy persistence must be enabled on both local and remote GSLB services that are configured for the GSLB virtual server.

Connection proxy occurs when the following conditions are satisfied:

- Requests are sent from a domain participating in GSLB. The domain is obtained from the URL/Host header.
- Requests are sent from a local GSLB service whose public IP address matches the public IP address of an active service bound to the GSLB virtual server.
- The local GSLB service has connection proxy enabled.
- The request includes a valid cookie that contains the IP address of an active remote GSLB service.

If one of the conditions is not met, connection proxy does not occur, but a site cookie is added if the local GSLB service has connection proxy enabled AND:

- No site cookie is supplied; OR,

- The site cookie refers to an IP address that is not an active GSLB remote service; OR,
- The cookie refers to the IP address of the virtual server on which the request is received.

The following are the limitations of using connection proxy site cookies:

- Site cookies do not work for non-HTTP(S) protocols.
- If an HTTP request is sent to a back-up virtual server, the virtual server does not add a cookie.
- Site cookies do not work if SSL client authentication is required.
- At the local site, the statistics for a GSLB service on a remote site are not the same as the statistics recorded for that service at the remote site. At the local site, the statistics for a remote GSLB service are slightly higher than the statistics that the remote site records for that same service.

Redirect persistence can be used only:

- For HTTP or HTTPS protocols.
- If the domain name is present in the request (either in the URL or in the HOST header), and the domain is a GSLB domain.
- When the request is received on a backup VIP or a GSLB local service that is in the down state.

To set persistence based on HTTP cookies by using the command line interface

At the command prompt, type:

set gslb service <serviceName> -sitePersistence (ConnectionProxy [-sitePrefix <prefix>] | HTTPredirect -sitePrefix <prefix>)

Example

set gslb service service-GSLB-1 -sitePersistence ConnectionProxy
set gslb service service-GSLB-1 -sitePersistence HTTPRedirect -sitePrefix vserver-GSLB-1

Parameters for setting persistence based on HTTP cookies

serviceName

The name of the GSLB service for which connection proxy based cookie persistence is being configured.

sitePersistence

The type of persistence. Possible Values: connectionProxy, HTTPredirect, None.

sitePrefix

This is a mandatory parameter when you configure HTTP redirect based persistence on a GSLB service. When the service is bound to a GSLB virtual server, for each bound service-domain pair, a GSLB site domain is generated internally by concatenating the service's siteprefix and the domain's name. If a special string "NONE" is specified, the siteprefix string is not set.

To set persistence based on cookies by using the configuration utility

1. In the navigation pane, expand GSLB and click Services.
2. In the GSLB Services pane, select the service that you want to configure for site persistence (for example, service-GSLB-1).
3. Click Open.
4. On the Advanced tab, under Site Persistence type, specify values for the following parameters, which correspond to parameters described in “Parameters for setting persistence based on HTTP cookies” as shown:
   - Site Persistence type—sitePersistence
   - Site Prefix—sitePrefix
5. Click OK.

Configuring Transition Out-Of-Service State (TROFS) in GSLB

When you configure persistence on a GSLB virtual server to which a service is bound, the service continues to serve requests from the client even after it is disabled, accepting new requests or connections only to honor persistence. After a configured period of time, known as the graceful shutdown period, no new requests or connections are directed to the service, and all of the existing connections are closed.

When disabling a service, you can specify a graceful shutdown period, in seconds, by using the delay argument. During the graceful shutdown period, if the service is bound to a virtual server, its state appears as Out of Service.

Configuring Dynamic Weights for Services

In a typical network, there are servers that have a higher capacity for traffic than others. However, with a regular load balancing configuration, the load is evenly distributed across all services even though different services represent servers with different capacities.

To optimize your GSLB resources, you can configure dynamic weights on a GSLB virtual server. The dynamic weights can be based on either the total number of services bound to the virtual server or the sum of the weights of the individual services bound to the virtual server. Traffic distribution is then based on the weights configured for the services.

When dynamic weights are configured on the GSLB virtual server, requests are distributed according to the load balancing method, the weight of the GSLB service, and the dynamic weight. The product of the weight of the GSLB service and the dynamic weight is known as the cumulative weight. Therefore, when dynamic weight is configured on the GSLB virtual server, requests are distributed on the basis of the load balancing method and the cumulative weight.

When dynamic weight for a virtual server is disabled, the numerical value is set to 1. This ensures that the cumulative weight is a non-zero integer at all times.

Dynamic weight can be based on the total number of active services bound to load balancing virtual servers or on the weights assigned to the services.

Consider a configuration with two GSLB sites configured for a domain and each site has two services that can serve the client. If a service at either site goes down, the other server in that site has to handle twice as much traffic as a service at the other site. If dynamic weight is based on the number of active services, the site with both services active has twice the weight of the site with one service down and therefore receives twice as much traffic.

Alternatively, consider a configuration in which the services at the first site represent servers that are twice as powerful as servers at the second site. If dynamic weight is based on the weights assigned to the services, twice as much traffic can be sent to the first site as to the second.

Note: For details on assigning weights to load balancing services, see " Assigning Weights to Services".

As an illustration of how dynamic weight is calculated, consider a GSLB virtual server that has a GSLB service bound to it. The GSLB service represents a load balancing virtual server that in turn has two services bound to it. The weight assigned to the GSLB service is 3. The weights assigned to the two services are 1 and 2 respectively. In this example, when dynamic weight is set to:

- **Disabled**:The cumulative weight of the GSLB virtual server is the product of the dynamic weight (disabled = 1) and the weight of the GSLB service (3), so the cumulative weight is 3.

- **SERVICECOUNT**: The count is the sum of the number of services bound to the load balancing virtual servers corresponding to the GSLB service (2), and the cumulative weight is the product of the dynamic weight (2) and the weight of the GSLB service (3), which is 6.
- **SERVICEWEIGHT**: The dynamic weight is the sum of the number of services bound to the GSLB service (2), and the cumulative weight is the product of the dynamic weight (2) and the weight of the GSLB service (3), which is 6.

Note: Dynamic weights are not applicable when content switching virtual servers are configured.

To configure a GSLB virtual server to use dynamic weights by using the command line interface

At the command prompt, type:

set gslb vserver <name> -dynamicWeight SERVICECOUNT | SERVICEWEIGHT

Example

set gslb vserver vserver-GSLB-1 -dynamicWeight SERVICECOUNT

To set GSLB virtual server to use dynamic weights by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the GSLB Virtual Servers pane, select the GSLB virtual server for which you want to set dynamic weights (for example, vserver-GSLB-1).
3. Click Open.
4. On the Method and Persistence tab, under Method, select SERVICECOUNT or SERVICEWEIGHT from the Dynamic Weight list.
5. Click OK.

Monitoring GSLB Services

When you bind a remote service to a GSLB virtual server, the GSLB sites exchange metric information, including network metric Information, which is the round-trip-time and persistence Information.

If a metric exchange connection is momentarily lost between any of the participating sites, the remote site is marked as DOWN and load balancing is performed on the remaining sites that are UP. When metric exchange for a site is DOWN, the remote services belonging to the site are marked DOWN as well.

The NetScaler appliance periodically evaluates the state of the remote GSLB services by using either MEP or monitors that are explicitly bound to the remote services. Binding explicit monitors to local services is not required, because the state of the local GSLB service is updated by default using the MEP. However, you can bind explicit monitors to a remote service. When monitors are explicitly bound, the state of the remote service is not controlled by the metric exchange.

By default, when you bind a monitor to a remote GSLB service, the NetScaler appliance uses the state of the service reported by the monitor. However, you can configure the NetScaler appliance to use monitors to evaluate services in the following situations:

- Always use monitors (default setting).
- Use monitors when MEP is DOWN.
- Use monitors when remote services and MEP are DOWN.

The second and third of the above settings enable the NetScaler to stop monitoring when MEP is UP. For example, in a hierarchical GSLB setup, a GSLB site provides the MEP information about its child sites to its parent site. Such an intermediate site may evaluate the state of the child site as DOWN because of network issues, though the actual state of the site is UP. In this case, you can bind monitors to the services of the parent site and disable MEP to determine the actual state of the remote service. This option enables you to control the manner in which the states of the remote services are determined.

To use monitors, first create them, and then bind them to GSLB services.

Adding or Removing Monitors

To add a monitor, you specify the type and the port. You cannot remove a monitor that is bound to a service. You must first unbind the monitor from the service.

To add a monitor by using the command line interface

At the command prompt, type the following commands to create a monitor and verify the configuration:

- add lb monitor <monitorName> -type <monitorType> -destPort <portNumber>
- show lb monitor <monitorName>

Example

```
add lb monitor monitor-HTTP-1 -type HTTP -destPort 80
show lb monitor monitor-HTTP-1
```

To remove a monitor by using the command line interface

At the command prompt, type:

rm lb monitor <monitorName>

Parameters for adding a monitor

name

The name of the monitor being created. This alphanumeric string is required and cannot be changed after the monitor is created. The name must not exceed 31 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

type

The type of monitor being configured. The following are valid monitor types:

- **TCP** - The NetScaler appliance establishes a TCP connection with the monitor destination and then closes the connection. If the NetScaler observes TCP traffic to the destination, it does not send TCP monitoring requests. This occurs if LRTM is disabled. By default, LRTM is disabled on this monitor. This is done only for UDP, and the service goes down immediately.

- **TCP-ECV** - The NetScaler appliance establishes a TCP connection with the monitor destination. When the connection is established, the appliance sends specific data to the service by using the -send parameter, and the appliance and expects a specific response through the -receive parameter.

- **HTTP** - the NetScaler establishes a TCP connection with the monitor destination. After the connection is established, the NetScaler sends HTTP requests and compares the response code, in the response from the service, with the configured set of response codes.

- **HTTP-ECV** - the NetScaler establishes a TCP connection with the monitor destination. When the connection is established, the NetScaler sends the HTTP data specified by the -send parameter to the service and expects the HTTP response that the -receive parameter specifies. (HTTP body part, not including HTTP headers.) Empty response data matches any response. Expected data may be anywhere in the first 24K bytes of the HTTP body of the response.

- **PING** - the NetScaler sends an ICMP echo request to the destination of the monitor and expects an ICMP echo response.

Note: The NetScaler also supports FTP, UDP, DNS, UDP-ECV, TCPS, HTTPS, TCPS-ECV, HTTPS-ECV, LDNS-PING, LDNS-TCP, and LDNS-DNS monitors.

For more information about monitors, see Load Balancing.

destPort

Destination TCP/UDP port of the probe (the port of the dispatcher to which the probe is sent). The port can be different from the server port to which the monitor is bound. The value 0 (zero) directs the probes to the bound server's port. This parameter has no effect on PING type monitors.

To add a monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing and click Monitors.
2. In the details pane, click Add.
3. In the Create Monitor dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for adding a monitor” as shown:
   - Name*—name
   - Type*—type

   * A required parameter
4. On the Standard Parameters tab, in the Destination Port text box, type the destination port number (see “destPort” in the above parameter list).
5. Click Create, and then click Close.

Binding Monitors to a GSLB Service

Once you create monitors, you must bind them to GSLB services. When binding monitors to the services, you can specify a weight for the monitor. After binding one or more weighted monitors, you can configure a monitor threshold for the service. This threshold takes the service down if the sum of the bound monitor weights falls below the threshold value.

Note: In the configuration utility, you can set both the weight and the monitoring threshold at the same time that you bind the monitor. When using the command line, you must issue a separate command to set the service's monitoring threshold.

To bind the monitor to the GSLB service by using the command line interface

At the command prompt, type:

bind monitor <name> <serviceName> [-state (**Enabled** | **Disabled**)] -weight <positiveInteger>

Example

bind monitor monitor-HTTP-1 service-GSLB-1 -state enabled -weight 2

To set the monitoring threshold for a GSLB service by using the command line interface

At the command prompt, type:

set gslb service <ServiceName> -monThreshold <PositiveInteger>

Example

set gslb service service-GSLB-1 -monThreshold 9

Parameters for binding a monitor to a GSLB service

name

The name of the monitor to be bound to the service.

serviceName

The name of the service to which to bind the monitor.

weight

The weight to assign to the service. Minimum value: 1. Maximum value: 100. Default: 1.

monThreshold

The monitoring threshold for the service. Minimum value: 0. Maximum value: 65535.

To bind the monitor to the GSLB service by using the configuration utility

1. In the navigation pane, expand GSLB and click Services.
2. The details pane, select the service to which you want to bind the monitor (for example, select service-GSLB-1).
3. Click Open.
4. In the Configure GSLB Service dialog box, on the Monitors tab, select the monitor that you want to bind to the service (for example, monitor-HTTP-1).
5. Click Add.
6. In the Configured table, you can select the newly assigned monitor and enter a new weight value.
7. To enable the monitor, make sure the State check box is selected.
8. Repeat the preceding steps to add additional monitors.
9. In the Monitor Threshold text box, you can enter a threshold value.
10. Click OK.

Monitoring GSLB Sites

The NetScaler appliance uses MEP or monitors to determine the state of the GSLB sites. You can configure a GSLB site to always use monitors (the default), use monitors when MEP is down, or use monitors when both the remote service and MEP are down. In the latter two cases, the NetScaler appliance stops monitoring when MEP returns to the UP state.

To configure monitor triggering by using the command line interface

At the command prompt, type:

set gslb site <siteName> -triggerMonitor (ALWAYS | MEPDOWN | MEPDOWN_SVCDOWN)

Example

```
> set gslb site Site-GSLB-North-America –triggerMonitor Always
 Done
```

To configure monitor triggering by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Sites.
2. In the details pane, select the site, and then click Open.
3. In the Configure GSLB Site dialog box, in the Trigger Monitors drop-down list, select an option for when to trigger monitoring.
4. Click OK.

Protecting the GSLB Setup Against Failure

You can protect your GSLB setup against failure of a GSLB site or a GSLB virtual server by configuring a backup GSLB virtual server, configuring the NetScaler appliance to respond with multiple IP addresses, or configuring a Backup IP address for a GSLB domain. You can also divert excess traffic to a backup virtual server by using spillover.

Configuring a Backup GSLB Virtual Server

Configuring a backup entity for a GSLB virtual server ensures that DNS traffic to a site is not interrupted if the GSLB virtual server goes down. The backup entity can be another GSLB virtual server, or it can be a backup IP address. With a backup entity configured, if the primary GSLB virtual server goes down, the backup entity handles DNS requests. To specify what should happen when the primary GSLB virtual server comes back up again, you can configure the backup entity to continue handling traffic until you manually enable the primary virtual server to take over (using the disablePrimaryOnDown option), or you can configure a timeout period after which the primary takes over.

If you configure both the timeout and the disablePrimaryOnDown option for the backup entity, the backup session time-out takes precedence over the disablePrimaryOnDown setting.

To configure a backup GSLB virtual server by using the command line interface

At the command prompt, type the following commands to configure a GSLB virtual server as a backup virtual server and verify the configuration:

- set gslb vserver <name> -backupVServer <name> [-backupSessionTimeout <timeoutValue>] [-disablePrimaryOnDown (ENABLED | DISABLED)]
- show gslb vserver <name>

Example

```
set gslb vserver vserver-GSLB-1 -backupVServer vserver-GSLB-2 -backupSessionTimeout 3 -disablePrimaryOnD
show gslb vserver vserver-GSLB-1
```

Parameters for configuring a backup GSLB virtual server

name

The name of the GSLB virtual server for which you are configuring a backup.

backupVServer

The name of the GSLB virtual server being configured as a backup.

backupSessionTimeout

The time, in minutes, after which the former primary GSLB virtual becomes primary again after returning to the UP state.

disablePrimaryOnDown

Require manual intervention to return the former primary GSLB virtual server to primary status.

To set GSLB virtual server as a backup virtual server by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the GSLB Virtual Servers pane, select the GSLB virtual server for which you want to configure a backup virtual server (for example, vserver-GSLB-1).
3. Click Open.
4. On the Advanced tab, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a backup GSLB virtual server” as shown:
   - Backup VServer—backupVServer
   - Backup Session Time-out (mins)—backupSessionTimeout
   - Disable Primary When Down—disablePrimaryOnDown
5. Click OK.

Configuring a GSLB Setup to Respond with Multiple IP Addresses

A typical DNS response contains the IP address of the best performing GSLB service. However, if you enable multiple IP response (MIR), the NetScaler appliance sends the best GSLB service as the first record in the response and adds the remaining active services as additional records. If MIR is disabled (the default), the NetScaler appliance sends the best service as the only record in the response.

To configure a GSLB virtual server for multiple IP responses by using the command line interface

At the command prompt, type the following commands to configure a GSLB virtual server for multiple IP responses and verify the configuration:

- set gslb vserver<name> -MIR (ENABLED | DISABLED)
- show gslb vserver <name>

Example

```
set gslb vserver vserver-GSLB-1 -MIR ENABLED
 show gslb vserver <vserverName>
```

To set a GSLB virtual server for multiple IP responses by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the GSLB Virtual Servers pane, select the GSLB virtual server for which you want to configure a backup virtual server (for example, vserver-GSLB-1).
3. Click Open.
4. On the Advanced tab, under When this VServer is “UP,” select the Send all “active” service IP in response (MIR) check box.
5. Click OK.

Configuring a GSLB Virtual Server to Respond with an Empty Address Record When DOWN

A DNS response can contain either the IP address of the requested domain or an answer stating that the IP address for the domain is not known by the DNS server, in which case the query is forwarded to another name server. These are the only possible responses to a DNS query.

When a GSLB virtual server is disabled or in a DOWN state, the response to a DNS query for the GSLB domain bound to that virtual server contains the IP addresses of all the services bound to the virtual server. However, you can configure the GSLB virtual server to in this case send an empty down response (EDR). When this option is set, a DNS response from a GSLB virtual server that is in a DOWN state does not contain IP address records, but the response code is successful. This prevents clients from attempting to connect to GSLB sites that are down.

Note: You must configure this setting for each virtual server to which you want it to apply.

To configure a GSLB virtual server for empty down responses by using the command line interface

At the command prompt, type:

set gslb vserver<name> -EDR (ENABLED | DISABLED)

Example

```
> set gslb vserver vserver-GSLB-1 -EDR ENABLED
 Done
```

To set a GSLB virtual server for empty down responses by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the GSLB Virtual Servers pane, select the GSLB virtual server for which you want to configure a backup virtual server (for example, vserver-GSLB-1).
3. Click Open.
4. On the Advanced tab, under When this VServer is “Down,” select the Do not send any service’s IP address in response (EDR) check box.
5. Click OK.

Configuring a Backup IP Address for a GSLB Domain

You can configure a backup site for your GSLB configuration. With this configuration in place, if all of the primary sites go DOWN, the IP address of the backup site is provided in the DNS response.

Typically, if a GSLB virtual server is active, that virtual server sends a DNS response with one of the active site IP addresses as selected by the configured GSLB method. If all the configured primary sites in the GSLB virtual server are inactive (in the DOWN state), the authoritative domain name system (ADNS) server or DNS server sends a DNS response with the backup site's IP address.

Note: When a backup IP address is sent, persistence is not honored.

To set a backup IP address for a domain by using the command line interface

At the command prompt, type the following commands to set a backup IP address and verify the configuration:

- set gslb vserver <name> -domainName <string> -backupIP <IPAddress>
- show gslb vserver <name>

Example

set gslb vserver vserver-GSLB-1 -domainName www.abc.com -backupIP 10.102.29.66
show gslb vserver vserver-GSLB-1

Parameters for configuring a backup IP address for a domain

vserverName

The name of the GSLB virtual server to which the domain you are configuring a backup IP address for is bound.

domainName

The name of the domain for which a backup IP address is being configured.

backupIP

The IP address of the backup service. This IP address is used when all services bound to the domain are down, or when the backup chain is down.

To set a backup IP address for a domain by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the GSLB Virtual Servers pane, select the GSLB virtual server to which you want to bind the backup domain (for example, vserver-GSLB-1).
3. Click Open.
4. On the Domains tab, select a domain and click Open.
5. In the Configure GSLB Domain dialog box, in the Backup IP text box, type the IP address of the backup domain.
6. Click OK.

Diverting Excess Traffic to a Backup Virtual Server

Once the number of connections to a primary GSLB virtual server exceeds the configured threshold value, you can use the spillover option to divert new connections to a backup GSLB virtual server. This threshold value can be calculated dynamically or set manually. Once the number of connections to the primary virtual server drops below the threshold, the primary GSLB virtual server resumes serving client requests.

You can configure persistence with spillover. When persistence is configured, new clients are diverted to the backup virtual server if that client is not already connected to a primary virtual server. When persistence is configured, connections that were diverted to the backup virtual server are not moved back to the primary virtual server after the number of connections to the primary virtual server drops below the threshold. Instead, the backup virtual server continues to process those connections until they are terminated by the user. Meanwhile, the primary virtual server accepts new clients.

The threshold can be measured either by the number of connections or by the bandwidth.

If the backup virtual server reaches the configured threshold and is unable to take any additional load, the primary virtual server diverts all requests to the designated redirect URL. If a redirect URL is not configured on the primary virtual server, subsequent requests are dropped.

The spillover feature prevents the remote backup GSLB service (backup GSLB site) from getting flooded with client requests when the primary GSLB virtual server fails. This occurs when a monitor is bound to a remote GSLB service, and the service experiences a failure that causes its state to go DOWN. The monitor continues to keep the state of the remote GSLB service UP, however, because of the spillover feature.

As part of the resolution to this problem, two states are maintained for a GSLB service, the primary state and effective state. The primary state is the state of the primary virtual server and the effective state is the cumulative state of the virtual servers (primary and backup chain). The effective state is set to UP if any of the virtual servers in the chain of virtual servers is UP. A flag that indicates that the primary VIP has reached the threshold is also provided. The threshold can be measured by either the number of connections or the bandwidth.

A service is considered for GSLB only if its primary state is UP. Traffic is directed to the backup GSLB service only when all the primary virtual servers are DOWN. Typically, such deployments will have only one backup GSLB service.

Adding primary and effective states to a GSLB service has the following effects:

- When source IP persistence is configured, the local DNS is directed to the previously selected site only if the primary virtual server on the selected site is UP and below threshold. Persistence can be ignored in the round robin mode.
- If cookie-based persistence is configured, client requests are redirected only when the primary virtual server on the selected site is UP.

- If the primary virtual server has reached its saturation and the backup VIP(s) is absent or down, the effective state is set to DOWN.
- If external monitors are bound to an HTTP-HTTPS virtual server, the monitor decides the primary state.
- If there is no backup virtual server to the primary virtual server and the primary virtual server has reached its threshold, the effective state is set to DOWN.

To configure a backup GSLB virtual server by using the command line interface

At the command prompt, type the following commands to configure a backup GSLB virtual server and verify the configuration:

- set gslb vserver <name> -soMethod <method> -soThreshold <threshold> -soPersistence (**ENABLED** | **DISABLED**) -soPersistenceTimeout <timeout>
- show gslb vserver <name>

Example

```
set gslb vserver Vserver-GSLB-1 -soMethod CONNECTION -soThreshold 1000 -soPersistence ENABLED -soPersis
show gslb vserver Vserver-GSLB-1
```

Parameters for configuring a backup GSLB virtual server

name

The name of the GSLB virtual server for which a backup virtual server is being configured.

soMethod

The type of spillover used to divert traffic to the backup GSLB virtual server when the primary virtual server reaches the threshold. Possible values:

- **CONNECTION**. Spillover based on number of connections exceeding the threshold.
- **DYNAMICCONNECTION**. Spillover based on the combined number of connections exceeding the threshold.
- **BANDWIDTH**. Spillover based on combined incoming and outgoing bandwidth.
- **HEALTH**. Spillover occurs if bound and active services and service groups fall below a threshold relative to all bound elements.
- **NONE**.

soThreshold

The threshold value that decides when traffic must spill over to the backup virtual server. The following threshold values are supported:

- For the **CONNECTION** (or) **DYNAMICCONNECTION** spillover type, the threshold value is the maximum number of connections that the sites under the primary GSLB virtual server will handle before spillover occurs.
- For the **BANDWIDTH** spillover type, the threshold value is the amount of incoming and outgoing traffic (in kilobits per second) that the GSLB virtual server will handle before spillover occurs. Minimum value: 1. Maximum value: 4,294,967,294.
- For **HEALTH**, the threshold value is a positive integer from 1 through 99. This integer represents a percentage of the sum of the binding weights of all of the enabled, bound, and active GSLB services and service groups relative to the sum of the binding weights of all enabled and bound services and service groups (active and inactive).

soPersistence

The configured spillover persistence state. If you enable spillover persistence, the NetScaler appliance maintains source-IP based persistence over the primary virtual server and backup virtual servers. Possible values: ENABLED, DISABLED. Default: DISABLED.

soPersistenceTimeout

The configured time-out value, in minutes, for spillover persistence. Minimum value: 2. Maximum value: 1440. Default: 2.

backupVServer

The name of the GSLB virtual server being configured as a backup.

backupSessionTimeout

The time, in minutes, after which the former primary GSLB virtual becomes primary again after returning to the UP state.

To configure a backup GSLB virtual server by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to configure as a backup (for example, Vserver-LB-1), and then click Open.
3. On the Advanced tab, under Spillover, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a backup GSLB virtual server” as shown:
   - Method— soMethod
   - Threshold— soThreshold
   - Persistence Time-out (min) — soPersistenceTimeout
4. Select the Persistence check box.
5. Click OK.

Managing Client Connections

To facilitate management of client connections, you can enable delayed cleanup of connections to the virtual server. You can then manage local DNS traffic by configuring DNS policies.

Enabling Delayed Cleanup of Virtual Server Connections

The state of a virtual server depends on the states of the services bound to it, and the state of each service depends on the monitors bound to it. If a server is slow or down, the monitoring probes time out and the service that represents the server is marked as DOWN. A virtual server is marked as DOWN only when all services bound to it are marked as DOWN. You can configure services and virtual servers to either terminate all connections when they go down, or allow the connections to go through. The latter setting is for situations in which a service is marked as DOWN because of a slow server.

When you configure the down state flush option, the NetScaler appliance performs a delayed cleanup of connections to a GSLB service that is down.

To enable delayed cleanup of virtual server connections by using the command line interface

At the command prompt, type the following commands to configure delayed connection cleanup and verify the configuration:

- set gslb service <name> -downStateFlush (ENABLED | DISABLED)
- show gslb service <name>

Example

```
> set gslb service Service-GSLB-1 -downStateFlush ENABLED
 Done
> show gslb service Service-GSLB-1
 Done
```

Parameters for delayed connection cleanup

name

The name of the GSLB service for which delayed connection cleanup is being configured.

downStateFlush

Enables or disables delayed cleanup of connections to the GSLB service. Possible Values: ENABLED or DISABLED.

To enable delayed cleanup of virtual server connections by using the configuration utility

1. In the navigation pane, expand GSLB and click Services.
2. In the GSLB Services pane, select the service (for example, service-GSLB-1), and then click Open.
3. On the Advanced tab, select the Down state flush check box.
4. Click OK.

Managing Local DNS Traffic by Using DNS Policies

You can use DNS policies to implement site affinity by directing traffic from the IP address of a local DNS resolver or network to a predefined target GSLB site. This is configured by creating DNS policies with DNS expressions and binding the policies globally on the NetScaler appliance.

DNS Expressions

The NetScaler appliance provides certain predefined DNS expressions that can be used for configuring actions specific to a domain. Such actions can, for example, drop certain requests, select a specific view for a specific domain, or redirect certain requests to a specific location.

These DNS expressions (also called *rules*) are combined to create DNS policies that are then bound globally on the NetScaler appliance.

Following is the list of predefined DNS qualifiers available on the NetScaler appliance:

- `CLIENT.UDP.DNS.DOMAIN.EQ("domainname")`
- `CLIENT.UDP.DNS.IS_AREC`
- `CLIENT.UDP.DNS.IS_AAAAREC`
- `CLIENT.UDP.DNS.IS_SRVREC`
- `CLIENT.UDP.DNS.IS_MXREC`
- `CLIENT.UDP.DNS.IS_SOAREC`
- `CLIENT.UDP.DNS.IS_PTRREC`
- `CLIENT.UDP.DNS.IS_CNAME`
- `CLIENT.UDP.DNS.IS_NSREC`
- `CLIENT.UDP.DNS.IS_ANYREC`

The `CLIENT.UDP.DNS.DOMAIN` DNS expression can be used with string expressions. If you are using domain names as part of the expression, they must end with a period (.). For example, `CLIENT.UDP.DNS.DOMAIN.ENDSWITH("abc.com.")`

To create an expression by using the configuration utility

1. Click the icon next to the Expression text box. Click Add. (Leave the Flow Type and Protocol drop-down list boxes empty.) Follow these steps to create a rule.
2. In the Qualifier box, select a qualifier (for example, LOCATION).
3. In the Operator box, select an operator (for example, ==).
4. In the Value box, type a value (for example, Asia, Japan....).
5. Click OK. Click Create and click Close. The rule is created.
6. Click OK.

Configuring DNS Actions

A DNS policy includes the name of a DNS action to be performed when the policy rule evaluates to TRUE. A DNS action can do one of the following:

- Send the client an IP address for which you have configured a DNS view. For more information about DNS views, see Adding DNS Views.
- Send the client the IP address of a GSLB service after referring to a list of preferred locations that overrides static proximity behavior. For more information about preferred locations, see Overriding Static Proximity Behavior by Configuring Preferred Locations.
- Send the client a specific IP address as determined by the evaluation of the DNS query or response (DNS response rewrite).
- Forward a request to the name server without performing a lookup in the appliance's DNS cache.
- Drop a request.

You cannot create a DNS action for dropping a DNS request or for bypassing the DNS cache on the appliance. If you want to drop a DNS request, use the built-in action, `dns_default_act_Drop`. If you want to bypass the DNS cache, use the built-in action, `dns_default_act_Cachebypass`. Both actions are available along with custom actions in the Create DNS Policy and the Configure DNS Policy dialog boxes. These built-in actions cannot be modified or removed.

To configure a DNS action by using the command line interface

At the command prompt, type the following commands to configure a DNS action and verify the configuration:

- add dns action <actionName> <actionType> (-IPAddress <ip_addr | ipv6_addr> ... | -viewName <string> | -preferredLocList <string> ...) [-TTL <secs>]
- show dns action [<actionName>]

Examples

Example 1: Configuring DNS Response Rewrite. The following DNS action sends the client a preconfigured IP address when the policy to which the action is bound evaluates to true:

```
> add dns action dns_act_response_rewrite Rewrite_Response -IPAddress 192.0.2.20 192.0.2.56 198.51.100.1
 Done
> show dns action dns_act_response_rewrite
```

```
1)  ActionName:  dns_act_response_rewrite ActionType:  Rewrite_Response TTL:  3600          IPAddress:
 Done
```

Example 2: Configuring a DNS-View Based Response. The following DNS action sends the client an IP address for which you have configured a DNS view:

```
> add dns action send_ip_from_view_internal_ip ViewName -viewName view_internal_ip
 Done
> show dns action send_ip_from_view_internal_ip
1)  ActionName:  send_ip_from_view_internal_ip ActionType:  ViewName    ViewName:  view_internal_ip
 Done
```

Example 3: Configuring a Response Based on a Preferred Location List. The following DNS action sends the client the IP address that corresponds to the preferred location that it selects from the specified list of locations:

```
> add dns action send_preferred_location GslbPrefLoc -preferredLocList NA.tx.ns1.*.*.* NA.tx.ns2.*.*.* NA.tx
 Done
> show dns action  send_preferred_location
1)  ActionName:  send_preferred_location ActionType:  GslbPrefLoc PreferredLocList:  "NA.tx.ns1.*.*.*" "NA.t
 Done
```

Parameters for configuring a DNS action

actionName (Action Name)

The name of the DNS action. Maximum length: 127 characters. Must begin with a letter, a number, or the underscore character (_). Additional characters allowed, after the first character, are the number sign (#), period (.), space ( ), colon (:), at sign (@), equal sign (=) and hyphen (-). If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, `"dns action 1"` or `'dns action 1'`).

actionType (Type)

The type of DNS action that you want to configure. Possible values: viewName, GslbPrefLoc, Rewrite_Response.

Use the viewName option if you want to specify the name of a DNS view. When you specify a DNS view, the appliance sends clients the IP address for which the view was created. The viewName option must be followed by the viewName parameter.

Use the GslbPrefLoc option if you want to specify a list of preferred locations for requests that match the DNS policy. The GslbPrefLoc option must be followed by the preferredLocList parameter.

Use the Rewrite_Response option if you want to specify a list of IP addresses with which you want to rewrite DNS responses. The Rewrite_Response option must be followed by

the IPAddress parameter.

IPAddress (IP Address)

The list of IP addresses for the `Rewrite_Response` action type. The list can contain up to 25 IPv4 addresses and up to 5 IPv6 addresses. Use spaces as separators between the address entries. If invalid or duplicate IP addresses are included in the list, the add dns action command succeeds, but the invalid/duplicate IP addresses are not included in the IP address list.

TTL

The time to live, in seconds, for the address records. Minimum value: 0. Maximum value: 2147483647. Default: 3600.

viewName (View Name)

The name of the view that is associated with the IP address that you want to send the client.

preferredLocList (Preferred Location)

The list of preferred locations to choose from when a DNS policy rule evaluates to `TRUE`. When a policy matches, the preferred location list is given priority over the static proximity database. Locations must be provided in the descending order of priority. If the policy evaluates to `TRUE`, the NetScaler appliance uses an algorithm to select one or more GSLB services that correspond to the preferred locations. If only one service is found and the service is up, the appliance returns the IP address of the service to the client in the DNS response. If multiple GSLB services are found, the appliance load balances the services that are up. The appliance implements site affinity by directing all subsequent requests from the same source location to the selected preferred location.

You can add up to a maximum of 8 preferred locations. Maximum length: 1583.

To configure a DNS action by using the NetScaler configuration utility

1. In the navigation pane, expand DNS, and then click Actions.
2. In the details pane, do one of the following:
   - To create a DNS action, click Add.
   - To modify a DNS action, select the DNS action that you want to modify, and then click Open.
3. In the Create DNS Action or Configure DNS Action dialog box, set the following parameters:
   - Action Name (cannot be changed for an existing DNS action)
   - Type (cannot be changed for an existing DNS action)

     To set the Type parameter, do one of the following:
     - To create a DNS action that is associated with a DNS view, select View Name. Then, from the View Name list, select the DNS view that you want to use in the action.
     - To create a DNS action with a preferred location list, select Preferred Location List. In Preferred Location, enter a location, and then click Add. Add as many DNS locations as you want.
     - To configure a DNS action for rewriting a DNS response on the basis of policy evaluation, select Rewrite Response. In IP Address, enter an IP address, and then click Add. Add as many IP addresses as you want.
   - TTL (applicable only to the Rewrite Response action type)

Configuring DNS Policies

DNS policies operate on a location database that uses static and custom IP addresses. The attributes of the incoming local DNS request are defined as part of an expression, and the target site is defined as part of a DNS policy. While defining actions and expressions, you can use a pair of single quotation marks (‘’) as a wildcard qualifier to specify more than one location. When a DNS policy is configured and a GSLB request is received, the custom IP address database is first queried for an entry that defines the location attributes for the source:

- When a DNS query comes from an LDNS, the characteristics of the LDNS are evaluated against the configured policies. If they match, an appropriate action (site affinity) is executed. If the LDNS characteristics match more than one site, the request is load balanced between the sites that match the LDNS characteristics.
- If the entry is not found in the custom database, the static IP address database is queried for an entry, and if there is a match, the above policy evaluation is repeated.
- If the entry is not found in either the custom or static databases, the best site is selected and sent in the DNS response on the basis of the configured load balancing method.

The following restrictions apply to DNS policies created on the NetScaler appliance.

- A maximum of 64 policies are supported.
- DNS policies are global to the NetScaler and cannot be applied to a specific virtual server or domain.
- Domain or virtual server specific binding of policy is not supported.

You can use DNS policies to direct clients that match a certain IP address range to a specific site. For example, if you have a GSLB setup with multiple GSLB sites that are separated geographically, you can direct all clients whose IP address is within a specific range to a particular data center.

Both TCP-based and UDP-based DNS traffic can be evaluated. Policy expressions are available for UDP-based DNS traffic on the server and for both UDP-based DNS traffic and TCP-based DNS traffic on the client side. Additionally, you can configure expressions to evaluate queries and responses that involve only the following DNS question types (or QTYPE values):

- A
- AAAA
- NS
- SRV
- PTR

- CNAME
- SOA
- MX
- ANY

The following response codes (RCODE values) are also supported:

- NOERROR - No error
- FORMERR - Format error
- SERVFAIL - Server failure
- NXDOMAIN - Non-existent domain
- NOTIMP - Query type not implemented
- REFUSED - Query refused

You can configure expressions to evaluate DNS traffic. A DNS expression begins with the `DNS.REQ` or `DNS.RES` prefixes. Functions are available for evaluating the queried domain, the query type, and the carrier protocol. For more information about DNS expressions, see "Expressions for Evaluating a DNS Message and Identifying Its Carrier Protocol" in "Policy Configuration and Reference".

To add a DNS policy by using the command line interface

At the command prompt, type the following commands to create a DNS policy and verify the configuration:

- add dns policy <name> <rule> <actionName>
- show dns policy <name>

Example

```
> add dns policy policy-GSLB-1 'CLIENT.UDP.DNS.DOMAIN.EQ(\"domainname\")' my_dns_action
 Done
> show dns policy policy-GSLB-1
   Name: policy-GSLB-1
   Rule: CLIENT.UDP.DNS.DOMAIN.EQ("domainname")
   Action Name: my_dns_action
   Hits: 0
   Undef Hits: 0

 Done
```

To remove a configured DNS policy by using the command line interface

At the command prompt, type:

rm dns policy <name>

Parameters for configuring a DNS policy

name

The name of the DNS policy being created.

rule

Expression to be used by the dns policy.

actionName (Action)

The name of the DNS action that you want to trigger if the policy evaluates to TRUE. The following built-in DNS actions are available, along with any custom actions that you have created:

- **dns_default_act_Drop.** Drops the DNS request.
- **dns_default_act_Cachebypass.** Bypasses the DNS cache and forwards the request to the name server.

To configure a DNS policy by using the NetScaler configuration utility

1. In the navigation pane, expand DNS, and then click Policies.
2. In the details pane, do one of the following:
   - To create a DNS policy, click Add.
   - To modify a DNS policy, select the DNS policy, and then click OK.
3. In the Create DNS Policy or Configure DNS Policy dialog box, set the following parameters:
   - Policy Name (cannot be changed for an existing policy)
   - Action
   - Expression

     To specify an expression, do the following:

     a. Click Add, and then, in the drop-down box that appears, select the expression element with which you want to begin the expression. A second list appears. The list contains a set of expression elements that you can use immediately after the firs expression element.

     b. In the second list, select the expression element that you want, and then enter a period.

     c. After each selection, if you enter a period, the next set of valid expression elements appear in a list. Select expression elements and fill in arguments to functions until you have the expression you want.
4. Click Create or OK, and then click Close.

Binding DNS Policies

DNS policies are bound globally on the NetScaler appliance and are available for all configured GSLB virtual servers. Even though DNS policies are globally bound, policy execution can be limited to a specific GSLB virtual server by specifying the domain in the expression.

Note: Even though the bind dns global command accepts `REQ_OVERRIDE` and `RES_OVERRIDE` as valid bind points, those bind points are redundant, because DNS policies can be bound only globally. Bind your DNS policies only to the `REQ_DEFAULT` and `RES_DEFAULT` bind points.

To bind a DNS policy globally by using the command line interface

At the command prompt, type the following commands to bind a DNS policy globally and verify the configuration:

- bind dns global <policyName> <priority> [-gotoPriorityExpression <string>] [-type <type>]
- show dns global -type <type>

Example

```
> bind dns global policy-GSLB-1 10 -gotoPriorityExpression END
 Done
> show dns global -type REQ_DEFAULT
1)  Policy Name: policy-GSLB-1
    Priority: 10
    GotoPriorityExpression: END

 Done
```

To bind a DNS policy globally by using the configuration utility

1. In the navigation pane, expand DNS and click Policies.
2. In the details pane, click Global Bindings.
3. In the Bind/Unbind DNS Policy(s) to Global dialog box, click Insert Policy.
4. In the Policy Name column, select, from the list, the policy that you want to bind. Alternatively, in the list, click New Policy, and then create a DNS policy by setting parameters in the Create DNS Policy dialog box.
5. To modify a policy that is already bound globally, click the name of the policy, and then click Modify Policy. Then, in the Configure DNS Policy dialog box, modify the policy, and then click OK.
6. To unbind a policy, click the name of the policy, and then click Unbind Policy.
7. To modify the priority assigned to a policy, double-click the priority value, and then enter a new value.
8. To regenerate assigned priorities, click Regenerate Priorities. The priority values are modified to begin at 100, with increments of 10, without affecting the order of evaluation.
9. Click OK.

To view the global bindings of a DNS policy by using the command line interface

At the command prompt, type:

show dns global

To view the global bindings of a DNS policy by using the configuration utility

1. In the navigation pane, expand DNS and click Policies.
2. In the details pane, click Global Bindings. The global bindings of all DNS policies appear in this dialog box.

Adding DNS Views

You can configure DNS views to identify various types of clients and provide an appropriate IP address to a group of clients who query for the same GSLB domain. DNS views are configured by using DNS policies that select the IP addresses sent back to the client.

For example, if you have configured GSLB for your company's domain and have the server hosted in your company's network, clients querying for the domain from within your company's internal network can be provided with the server's internal IP address instead of the public IP address. Clients that query DNS for the domain from the Internet, on the other hand, can be provided the domain's public IP address.

To add a DNS view, you assign it a name of up to 31 characters. The leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ). After adding the view, you configure a policy to associate it with clients and a part of the network, and you bind the policy globally. To configure and bind a DNS policy, see Configuring DNS Policies and Binding DNS Policies.

To add a DNS view by using the command line interface

At the command prompt, type the following commands to create a DNS view and verify the configuration:

- add dns view <viewName>
- show dns view <viewName>

Example

```
add dns view PrivateSubnet
show dns view PrivateSubnet
```

To remove a DNS view by using the command line interface

At the command prompt, type:

rm dns view <viewName>

To add a DNS view by using the configuration utility

1. In the navigation pane, expand DNS and click Views.
2. In the details pane, click Add.
3. In the Create DNS view dialog box, in the Name text box, enter the name of the DNS view.
4. Click Create, and then click Close. The DNS view that you created appears in the Views pane.

For details on how to create a DNS policy, see Configuring DNS Policies and for details on how to bind DNS policies globally, see Binding DNS Policies.

Configuring GSLB for Commonly Used Deployment Scenarios

GSLB is commonly used in the following deployment scenarios:

- GSLB for disaster recovery
- GSLB based on proximity
- GSLB based on scalability
- GSLB based on the number of Access Gateway users
- GSLB for XenDesktop

Configuring GSLB for Disaster Recovery

Disaster recovery capability is critical, because downtime is costly. A NetScaler appliance configured for GSLB forwards traffic to the least-loaded or the best-performing data center. This configuration, referred to as an active-active setup, not only improves performance, but also provides immediate disaster recovery by routing traffic to other data centers if a data center that is part of the setup goes down. Alternatively, you can configure an active-standby GSLB setup for disaster recovery only.

Configuring GSLB for Disaster Recovery in an Active-Standby Data Center Setup

A conventional disaster recovery setup includes an active data center and a standby data center. The standby data center is a remote site. When a failover occurs as a result of a disaster event that causes the primary active data center to be inactive, the standby data center becomes operational.

Configuring disaster recovery in an active-standby data-center setup consists of the following tasks.

- Create the active data center.
    - Add a local GSLB site.
    - Add a GSLB vserver, which represents the active data center.
    - Bind the domain to the GSLB virtual server.
    - Add gslb services and bind the services to active GSLB virtual server.
- Create the standby data center.
    - Add a remote gslb site.
    - Add a gslb vserver, which represents standby data center.
    - Add gslb services which represents standby data center and bind the services to the standby gslb vserver.
    - Designate the standby data center by configuring the standby GSLB virtual server as the backup virtual server for the active GSLB virtual server.

Once you have configured the primary data center, replicate the configuration for the backup data center and designate it as the standby GSLB site by designating a GSLB virtual server at that site as the backup virtual server.

For details on how to configure a basic GSLB setup, see Configuring Global Server Load Balancing (GSLB).

To designate the standby GSLB site by using the command line interface

At both the active site and the remote site, at the command prompt, type:

set gslb vserver <name> -backupVserver <string>

Example

```
set gslb vserver vserver-GSLB-1 -backupVServer vserver-GSLB-2
```

To configure the standby site by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. Select the GSLB virtual server for the primary site and click Open.
3. In the Configure GSLB Virtual Server dialog box, on the Advanced tab, in the Backup VServer drop-down list box, select a backup virtual server.
4. Click OK.

By default, once the primary virtual server becomes active, it starts receiving traffic. However, if you want the traffic to be directed to the backup virtual server even after the primary virtual server becomes active, use the ‘disable primary on down’ option.

Configuring for Disaster Recovery in an Active-Active Data Center Setup

An active-active GSLB deployment, in which both GSLB sites are active, removes any risk that may arise in having a standby data center. With such a setup, web or application content can be mirrored in geographically separate locations. This ensures that data is consistently available at each distributed data center.

To configure GSLB for disaster recovery in an active-active data center set up, you must first configure the basic GSLB setup on the first data center and then configure all other data centers.

First create at least two GSLB sites. Then, for the local site, create GSLB a virtual server and GSLB services and bind the services to the virtual servers. Then create ADNS services and bind the domain for which you are configuring GSLB to the GSLB virtual server in the local site. Finally, at the local site, create a load balancing virtual server with the same virtual server IP address as the GSLB service.

Once you have configured the first data center, replicate the configuration for other data centers part of the setup.

For details on how to configure a basic GSLB setup, see Configuring Global Server Load Balancing (GSLB).

Configuring for Disaster Recovery with Weighted Round Robin

When you configure GSLB to use the weighted round robin method, weights are added to the GSLB services and the configured percentage of incoming traffic is sent to each GSLB site. For example, you can configure your GSLB setup to forward 80 percent of the traffic to one site and 20 percent of the traffic to another. After you do this, the NetScaler appliance will send four requests to the first site for each request that it sends to the second.

To set up the weighted round robin method, first create two GSLB sites, local and remote. Next, for the local site create a GSLB virtual server and GSLB services, and bind the services to the virtual servers. Configure the GSLB method as round robin. Next, create ADNS services and bind the domain for which you are configuring GSLB to the GSLB virtual server. Finally, create a load balancing virtual server with the same virtual server IP address as the GSLB service.

Each service that represents a physical server in the network has weights associated with it. Therefore the GSLB service is assigned a dynamic weight that is the sum of weights of all services bound to it. Traffic is then split between the GSLB services based on the ratio of the dynamic weight of the particular service to the total weight. You can also configure individual weights for each GSLB service instead of the dynamic weight.

If the services do not have weights associated with them, you can configure the GSLB virtual server to use the number of services bound to it to calculate the weight dynamically.

For details on how to configure a basic GSLB setup, see Configuring Global Server Load Balancing (GSLB).

Once you configure a basic GSLB setup, you must configure the weighted round robin method such that the traffic is split between the configured GSLB sites according to the weights configured for the individual services.

To configure a virtual server to assign weights to services by using the command line interface

At the command prompt, type one of the following commands, depending upon whether you want to create a new load balancing virtual server or configure an existing one:

- add lb vserver <name>@ -weight <WeightValue> <ServiceName>
- set lb vserver <name>@ -weight <WeightValue> <ServiceName>

Example

```
add lb vserver Vserver-LB-1 -weight 4 Service-HTTP-1
set lb vserver Vserver-LB-1 -weight 4 Service-HTTP-1
```

To set dynamic weight by using the command line interface

At the command prompt, type:

set gslb vserver <name> -dynamicWeight DynamicWeightType

Example

set gslb vserver Vserver-GSLB-1 -dynamicWeight ServiceWeight

To add weights to the GSLB services by using the command line interface

At the command prompt, type:

set gslb vserver <name> -serviceName GSLBServiceName -weight WeightValue

Example

set gslb vserver Vserver-GSLB-1 -serviceName Service-GSLB-1 -weight 1

Parameters for configuring a backup GSLB virtual server

lbVserverName

The name of the load balancing virtual server whose services you are configuring weights for.

serviceName

The name of the service whose weights you are configuring.

weight

The weight associated with the service. Minimum Value: 1, Maximum Value: 100.

dynamicWeight

Configures the GSLB virtual server to use either the service count or the cumulative service weights as its dynamic weight. Possible Values: SERVICECOUNT, SERVICEWEIGHT, DISABLED Default Value: DISABLED.

To configure a virtual server to assign weights to services by using the configuration utility

1. In the navigation pane, expand Load Balancing and click Virtual Servers.
2. Select the virtual server (for example, Vserver-LB-1) and click Open.
3. On the Services tab, in the Weights spin box, type or select the weight of a service (for example, 4) next to Service-HTTP-1).
4. Click OK.

To add weights to the GSLB services by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. Select the virtual server (for example vserver-GSLB-1) and click Open.
3. On the Services tab, in the Weight spin box, type or select the weight of a service (for example, next to service-GSLB-1, type 1).
4. Click OK.

To set dynamic weight by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. Select the virtual server (for example vserver-GSLB-1) and click Open.
3. On the Method and Persistence tab, under Method, in Dynamic Weight drop-down list, select SERVICEWEIGHT.
4. Click OK.

Configuring for Disaster Recovery with Data Center Persistence

Data center persistence is required for web applications that require maintaining a connection with the same server instead of having the requests load balanced. For example, in an e-commerce portal, maintaining a connection between the client and the same server is critical. For such applications, HTTP redirect persistence can be configured in an active-active setup.

To configure GSLB for disaster recovery with data center persistence, you must first configure the basic GSLB set up and then configure HTTP redirect persistence.

First create two GSLB sites, local and remote. Next, for the local site, create a GSLB virtual server and GSLB services and bind the services to the virtual server. Next, create ADNS services and bind the domain for which you are configuring GSLB to the GSLB virtual server at the local site. Next, create a load balancing virtual server with the same virtual server IP address as the GSLB service. Finally, duplicate the previous steps for the remote configuration, or configure the NetScaler appliance to autosynchronize your GSLB configuration.

For details on how to configure a basic GSLB setup, see Configuring Global Server Load Balancing (GSLB).

Once you have configured a basic GSLB setup, configure HTTP redirect precedence to enable data center persistence.

To configure HTTP redirect by using the command line interface

At the command prompt, type the following commands to configure HTTP redirect and verify the configuration:

- set gslb service <serviceName> -sitePersistence <sitePersistence> -sitePrefix <string>
- show gslb service <serviceName>

Example

set gslb service Service-GSLB-1 -sitePersistence HTTPRedirect -sitePrefix vserver-GSLB-1
show gslb service Service-GSLB-1

Parameters for configuring HTTP redirect

serviceName

The name of the GSLB service for which you are configuring site persistence.

sitePersistence

The type of site persistence being configured. Possible Values: ConnectionProxy, HTTPRedirect, None.

sitePrefix

When a service is bound to a GSLB virtual server, for each bound service-domain pair, a GSLB site domain is generated internally by concatenating the service's siteprefix and the domain name. If a special string, "NONE," is specified, the siteprefix string is not set.

To configure HTTP redirect by using the configuration utility

1. In the navigation pane, expand GSLB and click Services.
2. Select the GSLB service to be configured and click Open.
3. On the Advanced tab, under Site Persistence options, select the HTTPRedirect option.
4. In the Site Prefix text box, enter the site prefix (for example, vserver-GSLB-1).
5. Click OK.

Configuring GSLB for Proximity

When you configure GSLB for proximity, client requests are forwarded to the closest data center. The main benefit of the proximity-based GSLB method is faster response times resulting from the selection of the closest available data center. Such a deployment is critical for applications that require fast access to large volumes of data.

You can configure GSLB for proximity based on the round trip time (RTT), static proximity, or a combination of the two.

Configuring Dynamic Method (RTT)

Dynamic round trip time (RTT) is a measure of time or delay in the network between the client's local DNS server and a data resource. To measure dynamic RTT, the NetScaler appliance probes the client's local DNS server and gathers RTT metric information. The NetScaler then uses this metric to make its load balancing decision. Global server load balancing monitors the real-time status of the network and dynamically directs the client request to the data center with the lowest RTT value

To configure GSLB for proximity with dynamic method, you must first configure the basic GSLB set up and then configure dynamic RTT.

First create two GSLB sites, local and remote. Then, for the local site, create a GSLB virtual server and GSLB services and bind the services to the virtual server. Then create ADNS services and bind the domain for which you are configuring GSLB to the GSLB virtual server at the local site. Finally, create a load balancing virtual server with the same virtual server IP address as the GSLB service.

For details on how to configure a basic GSLB setup, see Configuring Global Server Load Balancing (GSLB).

Once you have configured a basic GSLB setup, configure the dynamic RTT method.

For details on how to configure the GSLB virtual server to use the dynamic RTT method for load balancing, see Configuring Dynamic RTT.

Configuring Static Proximity

The static proximity method for GSLB uses an IP address-based static proximity database to determine the proximity between the client's local DNS server and the GSLB sites. The NetScaler appliance responds with the IP address of a site that best matches the proximity criteria.

If two or more GSLB sites at different geographic locations serve the same content, the NetScaler appliance maintains a database of IP address ranges and uses the database for decisions about the GSLB sites to which to direct incoming client requests.

To configure GSLB for proximity with static proximity, you must first configure the basic GSLB set up and then configure static proximity.

First create two GSLB sites, local and remote. Then, for the local site, create a GSLB virtual server and GSLB services and bind the services to the virtual server. Then create ADNS services and bind the domain for which you are configuring GSLB to the GSLB virtual server at the local site. Finally, create a load balancing virtual server with the same virtual server IP address as the GSLB service.

For details on how to configure a basic GSLB setup, see Configuring Global Server Load Balancing (GSLB).

Once you have configured a basic GSLB setup, configure static proximity.

For details on how to configure the GSLB virtual server to use static proximity for load balancing, see Configuring Static Proximity.

Configuring Static Proximity and Dynamic RTT

You can configure the GSLB virtual server to use a combination of static proximity and dynamic RTT when you have some clients coming from an internal network like a branch office. You can configure GSLB such that the clients coming from the branch office or any other internal network are directed to a particular GSLB site that is geographically close to the client network. For all other requests, you can use dynamic RTT.

First create two GSLB sites, local and remote. Then, for the local site, create a GSLB virtual server and GSLB services and bind the services to the virtual server. Then create ADNS services and bind the domain for which you are configuring GSLB to the GSLB virtual server at the local site. Finally, create a load balancing virtual server with the same virtual server IP address as the GSLB service.

For details on how to configure a basic GSLB setup, see Configuring Global Server Load Balancing (GSLB).

Once you have configured a basic GSLB setup, configure the GSLB virtual server to use static proximity for all traffic originating from an internal network and then use dynamic RTT for all other traffic.

For details on how to configure static proximity, see Configuring Static Proximity and for details on how to configure dynamic RTT, see Configuring Dynamic RTT.

Configuring Parent-Child Topology

NetScaler appliances configured for global server load balancing (GSLB) provide for disaster recovery and ensure continuous availability of applications by protecting against points of failure in a wide area network (WAN). GSLB can balance the load across data centers by directing client requests to the closest or best performing data center, or to surviving data centers in the event of an outage.

There are three fundamental entities that must be configured for GSLB:

- **Site**: A GSLB site represents a NetScaler or a high availability (HA) pair of NetScaler appliances that maintain GSLB state information and provide information about how the NetScaler nodes should communicate. A site can also represent a data center.

- **GSLB virtual server**: A GSLB virtual server represents a group of resources to which users can be directed, and the logic used to select one resource verses another.

- **GSLB service**: A GSLB service represents a target resource and is bound to a GSLB virtual server. The target resource might be a load balancing virtual server on a NetScaler, or it could represent a third party server.

Sites and services are inherently linked to indicate proximity between the two. That is, all services must belong to a site, and are assumed to be in the same location as the GSLB site for proximity purposes. Likewise, services and virtual servers are linked, so that the logic is linked to the resources that are available.

Relationships among GSLB Sites

The concept of sites is central to NetScaler GSLB implementations. Unless otherwise specified, sites form a peer relationship among themselves. This relationship is used first to exchange health information and then to distribute load as determined by the selected algorithm. In many situations, however, a peer relationship among all GSLB sites is not desirable. Reasons for not having an all-peer implementation could be

1. To clearly separate GSLB sites. For example, to separate sites that participate in resolving DNS queries from the traffic management sites.

2. To reduce the volume of Metric Exchange Protocol (MEP) traffic, which increases exponentially with an increasing number of peer sites.

These goals can be achieved by using parent and child GSLB sites. Parent-child relationships can be used to build a two-level hierarchical GSLB design with the following characteristics:

- At the top level are parent sites that have peer relationships with other parents.

- Each parent can have multiple children, but each child can have only one parent.

- Each parent site exchanges health information with its children and with other parent sites.

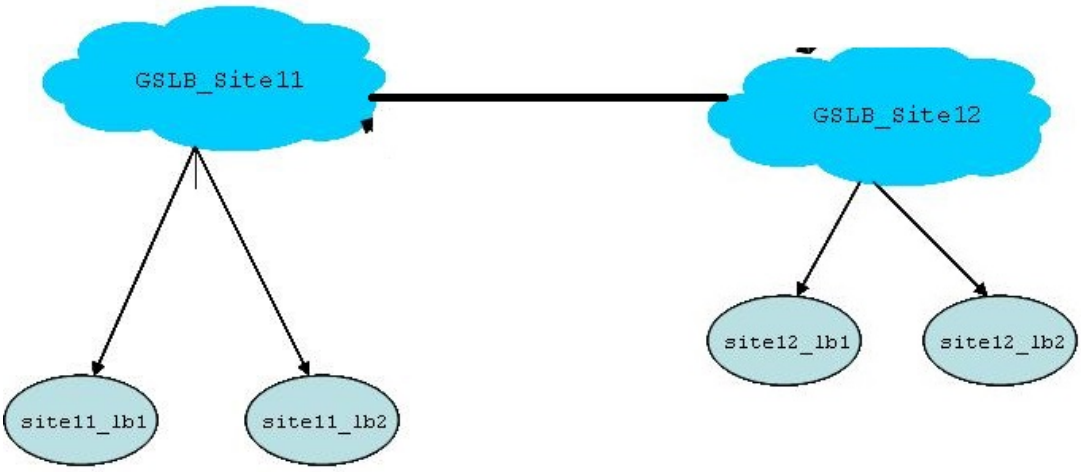
- A child communicates only with its parent.

Note: In a parent-child relationship for GSLB, only the parent site does the GSLB resolution. The child sites act as normal load balancing sites.

Limitations of GSLB Parent-Child site configuration:

- You can configure 32 Parent sites and 1024 Child sites for each Parent site.
- On the Child site, by default, the nwmetricExchange and sessionExchange options are disabled.
- Round Trip Time (RTT) GSLB method is not recommended for GSLB Parent-Child site configuration.
- ADNS service or DNS load balancing virtual servers should be configured only in the Parent site.

Setting Up a Parent-Child Configuration for Global Server Load Balancing



If you have a firewall configured at a GSLB site, make sure that port 3011 is open. Follow the procedures at the following location to create services and virtual servers: Configuring Global Server Load Balancing (GSLB) Figure 1. GSLB Parent-Child Topology

In the above figure:

- GSLB_Site11 and GSLB_Site12 are parent sites in a peer relationship.
- site11_lb1 and site11_lb2 are the child sites of GSLB_Site11, while site12_lb1 and site_lb2 are the child sites of GSLB_Site12.

The configuration of each parent site includes the information about all the child sites associated with it, but the configuration of each child site pertains only to that child and its parent. A child site is not aware about any other parent site or other child sites in the configuration. For example, in the above figure, the configuration of child site site11_lb1 would include only information about its parent site, GSLB_Site11.

Note: GSLB auto sync syncs only the GSLB configuration across the parent sites. It does not sync any configuration to the child sites.

To set up a parent-child configuration for GSLB by using the NetScaler command line

1. On each parent site, enter the following command: add gslb site<siteName><siteIPAddress> [-publicIP<ip_addr|ipv6_addr|*>] [-parentSite<string>] For example: `# add gslb site gslb_site11 1.1.1.1 -publicIP 1.1.1.1`

   ```
   # add gslb site site11_lb1 1.1.1.2 -publicIP 1.1.1.2 -parentSite
   gslb_site11

   # add gslb site site11_lb2 1.1.1.3 -publicIP 1.1.1.3 -parentSite
   gslb_site11

   # add gslb site gslb_site12 3.3.3.1 -publicIP 3.3.3.1

   # add gslb site site12_lb1 3.3.3.2 -publicIP 3.3.3.2 -parentSite
   gslb_site12

   # add gslb site site12_lb2 3.3.3.3 -publicIP 3.3.3.3 -parentSite
   gslb_site12
   ```

   The above command makes the parent site aware of its child sites as well as of the other parent site in the configuration.

2. On each child site, enter the following command: add gslb site<siteName><siteIPAddress> [-publicIP<ip_addr|ipv6_addr|*>] [-parentSite<string>] For example: `# add gslb site site11_lb1 1.1.1.1 -publicIP 1.1.1.1`

   ```
   # add gslb site site11_lb1 1.1.1.2 -publicIP 1.1.1.2 -parentSite
   gslb_site11
   ```

   The above command creates the child site and adds the parent-site information to child site's configuration.

   Network metrics, such as RTT and persistence session information, are synced only across the parent sites. Therefore, parameters like `nwMetric` and `sessionExchange` are disabled by default on all the child sites.

To verify correct parent-child configuration, check the states of all the GSLB services bound to the parent sites.

Note: If you want to use different private and public IP address for GSLB services, add the corresponding GSLB-service related configuration to the child site in a separate procedure, not as part of the GSLB site configuration.

Link Load Balancing

Link load balancing (LLB) balances outbound traffic across multiple Internet connections provided by different service providers. LLB enables the Citrix® NetScaler® appliance to monitor and control traffic so that packets are transmitted seamlessly over the best possible link. Unlike with server load balancing, where a service represents a server, with LLB, a service represents a router or the next hop. A link is a connection between the NetScaler and the router.

To configure link load balancing, many users begin by configuring a basic setup with default settings. Configuring a basic setup involves configuring services, virtual servers, monitors, routes, an LLB method, and, optionally, configuring persistence. Once a basic setup is operational, you can customize it for your environment.

Load balancing methods that are applicable to LLB are round robin, destination IP hash, least bandwidth, and least packets. You can optionally configure persistence for connections to be sustained on a specific link. The available persistence types are source IP address-based, destination IP address-based, and source IP and destination IP address-based. PING is the default monitor but configuring a transparent monitor is recommended.

You can customize your setup by configuring reverse NAT (RNAT) and backup links.

Configuring a Basic LLB Setup

To configure LLB, you first create services representing each router to the Internet Service Providers (ISPs). A PING monitor is bound by default to each service. Binding a transparent monitor is optional but recommended. Then, you create a virtual server, bind the services to the virtual server, and configure a route for the virtual server. The route identifies the virtual server as the gateway to the physical routers represented by the services. The virtual server selects a router by using the load balancing method that you specify. Optionally, you can configure persistence to make sure that all traffic for a particular session is sent over a specific link.

A default monitor (PING) is automatically bound to a service type of ANY when the service is created, but you can replace the default monitor with a transparent monitor, as described in "Creating and Binding a Transparent Monitor."

To create a service by using the command line interface

At the command prompt, type:

- add service <name> <IP> <serviceType> <port>
- show service <name>

Example

```
add service ISP1R_svc_any 10.10.10.254 any *
show service ISP1R_svc_any
      ISP1R_svc_any (10.10.10.254:*) - ANY
      State: DOWN
      Last state change was at Tue Aug 31 04:31:13 2010
      Time since last state change: 2 days, 05:34:18.600
      Server Name: 10.10.10.254
      Server ID : 0   Monitor Threshold : 0
      Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
      Use Source IP: NO
      Client Keepalive(CKA): NO
      Access Down Service: NO
      TCP Buffering(TCPB): YES
      HTTP Compression(CMP): NO
      Idle timeout: Client: 120 sec   Server: 120 sec
      Client IP: DISABLED
      Cacheable: NO
      SC: OFF
      SP: OFF
      Down state flush: ENABLED

1)     Monitor Name: ping
            State: UP       Weight: 1
            Probes: 244705  Failed [Total: 0 Current: 0]
            Last response: Success - ICMP echo reply received.
            Response Time: 1.322 millisec
 Done
```

Parameters for creating a service

name

The name of the service. Maximum length: 127

IP

The IP address of the physical router for which a service will be added.

serviceType

The type of connections that the service will handle. Specify a service type of ANY.

port

Port on which the service listens. Specify an asterisk (*) as the port number.

To create services by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating a service, as shown:
   - Service Name*—name
   - Server—IP
   - Protocol*—serviceType (Select ANY from the drop-down list.)
   - Port*—port

   * A required parameter
4. Click Create.
5. Repeat Steps 2-4 to create another service.
6. Click Close.
7. In the Services pane, select the services that you just configured and verify that the settings displayed at the bottom of the screen are correct.

Configuring an LLB Virtual Server and Binding a Service

After you create a service, create a virtual server and bind services to the virtual server. The default LB method of least connections is not supported in LLB. For information about changing the LB method, see "Configuring the LLB Method and Persistence."

To create a link load balancing virtual server and bind a service by using the command line interface

At the command prompt, type:

- add lb vserver <name> <serviceType>
- bind lb vserver < name> <serviceName>
- show lb vserver < name>

Example

```
add lb vserver Router1-vip any
bind lb vserver Router-vip ISP1R_svc_any
sh lb vserver router-vip
        Router-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: DOWN
        Last state change was at Thu Sep  2 10:51:32 2010
        Time since last state change: 0 days, 17:51:46.770
        Effective State: DOWN
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: ROUNDROBIN
        Mode: IP
        Persistence: NONE
        Connection Failover: DISABLED

1) ISP1R_svc_any (10.10.10.254: *) - ANY State: DOWN    Weight: 1
 Done
```

Parameters for creating an LLB virtual server

name

The name of the load balancing virtual server being added. Maximum length: 127

serviceType

The service type. Possible value: ANY.

Parameters for binding the service

name

The virtual server name to which the service is bound. Maximum length: 127

serviceName

The name of the service that is bound. Maximum Length: 127

To create a link load balancing virtual server and bind a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the Load Balancing Virtual Servers pane, click Add.
3. In the Create Virtual Servers (Load Balancing) dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating an LLB virtual server, as shown:
   - Name*—name
   - Protocol*—serviceType (Select ANY.)

   * A required parameter

   Note: Make sure Directly Addressable is unchecked.
4. Under the Services tab, in the Active column, select the check box for the service that you want to bind to the virtual server.
5. Click Create, and then click Close.
6. In the Load Balancing Virtual Servers tab, select the virtual server that you just created, and verify that the settings displayed in the Details pane are correct.

Configuring the LLB Method and Persistence

By default, the NetScaler appliance uses the least connections method to select the service for redirecting each client request, but you should set the LLB method to one of the supported methods. You can also configure persistence, so that different transmissions from the same client are directed to the same server.

To configure the LLB method and/or persistence by using the command line interface

At the command prompt, type the following command:

- set lb vserver <name> -lbMethod <lbMethod> -persistenceType <persistenceType>
- show lb vserver <name>

Example

```
set lb vserver router-vip -lbmethod ROUNDROBIN -persistencetype SOURCEIP

show lb vserver Router-vip
        Router-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: DOWN
        Last state change was at Fri Sep  3 04:46:48 2010
        Time since last state change: 0 days, 00:52:21.200
        Effective State: DOWN
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: ROUNDROBIN
        Mode: IP
        Persistence: SOURCEIP
    Persistence Mask: 255.255.255.255       Persistence v6MaskLength: 128   Persistence Timeout: 2 min
        Connection Failover: DISABLED
```

Parameters for configuring the LLB method and persistence

name

The name of the load balancing virtual server. Maximum Length: 127

lbMethod

The load balancing method. Possible values:

- ROUNDROBIN: Rotates the outgoing packets among the available links. This method distributes packets equally among the links, even if they operate at different speeds. Therefore, it can result in retransmissions or out-of-order packets.
- DESTINATIONHASH: Uses the hashed value of the destination IP address to select a link. You can mask the destination IP address to specify which part of it to use in the hash value calculation, so that requests that are from different networks but destined for the same subnet are all directed to the same link.
- LEASTBANDWIDTH: Selects the link that is currently serving the least amount of traffic, measured in megabits per second (Mbps).
- LEASTPACKETS: Selects the link that has received the fewest packets in the last 14 seconds.

persistenceType

Persistence type for the virtual server. Possible values:

- SOURCEIP: Persistence based on the source IP address of inbound packets. After the load balancing method selects a link for transmission of the first packet, the NetScaler directs all subsequent packets sent from the same source IP address to the same link.
- DESTIP: Persistence based on the destination IP address of outbound packets. After the load balancing method selects a link for transmission of the first packet, the NetScaler directs all subsequent packets for the same destination IP address to the same link.
- SRCIPDESTIP: Persistence based on the source IP address of inbound packets and destination IP address of outbound packets. After the load balancing method selects a link for transmission of the first packet, the NetScaler directs all subsequent requests from the same source IP address and to the same destination IP address to the same link.

To configure the link load balancing method and/or persistence by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure the Load Balancing method and/or persistence settings, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, on the Method and Persistence tab, specify values for some or all of the following parameters, which correspond to parameters described in "Parameters for configuring the LLB method and persistence" as shown:
   - Method—lbMethod
   - Persistence—persistenceType
4. Click OK.
5. In the Load Balancing Virtual Servers pane, select the virtual server that you just configured and verify that the settings displayed in the Details pane are correct.

Configuring an LLB Route

After configuring the IPv4 or IPv6 services, virtual servers, LLB methods, and persistence, you configure an IPv4 or IPv6 LLB route for the network specifying the virtual server as the gateway. A route is a collection of links that are load balanced. Requests are sent to the virtual server IP address that acts as the gateway for all outbound traffic and selects the router based on the LLB method configured.

To configure an IPv4 LLB route by using the command line interface

At the command prompt, type:

- add lb route <network> <netmask> <gatewayName>
- show lb route [<network> <netmask>]

Example

```
add lb route 0.0.0.0 0.0.0.0 Router-vip
show lb route 0.0.0.0 0.0.0.0
     Network         Netmask       Gateway/VIP           Flags
    -----------     -------------  --------------        --------
1)    0.0.0.0         0.0.0.0       Router-vip             UP
```

To configure an IPv6 LLB route by using the command line interface

At the command prompt, type:

- add lb route6 <network> <gatewayName>
- show lb route6

```
add lb route6 ::/0 llb6_vs
show lb route6
     Network          VIP            Flags
    -----------      ---------       --------
1)    ::/0             llb6_vs          UP
```

Example

Parameters for configuring the LLB route

network (Network)

The IPv4 or IPv6 address of the network to which the route belongs.

netmask (Netmask)

The mask specifying the subnet to which the route belongs. This is required for IPv4 routes.

gatewayName (Gateway Name)

The name of the virtual server. Maximum Length: 127

To configure an LLB route by using the configuration utility

1. In the navigation pane, expand Network, and then click Routes.
2. In the details pane, select one of the following:
   - Click LLB to configure an IPv4 route.
   - Click LLBV6 to configure an IPv4 route.
3. In the Create LB Route or Create LB IPV6 Routedialog box, set the following parameters:
   - Network*
   - Netmask*—Required for IPV4 routes.
   - Gateway Name*—gatewayName

   * A required parameter
4. Click Create, and then click Close. The route that you just created appears on the LLB or the LLB6 tab in the Routes pane.

The following diagram shows a basic LLB setup. A service is configured for each of the two links (ISPs) and PING monitors are bound by default to these services. A link is selected based on the LLB method configured.

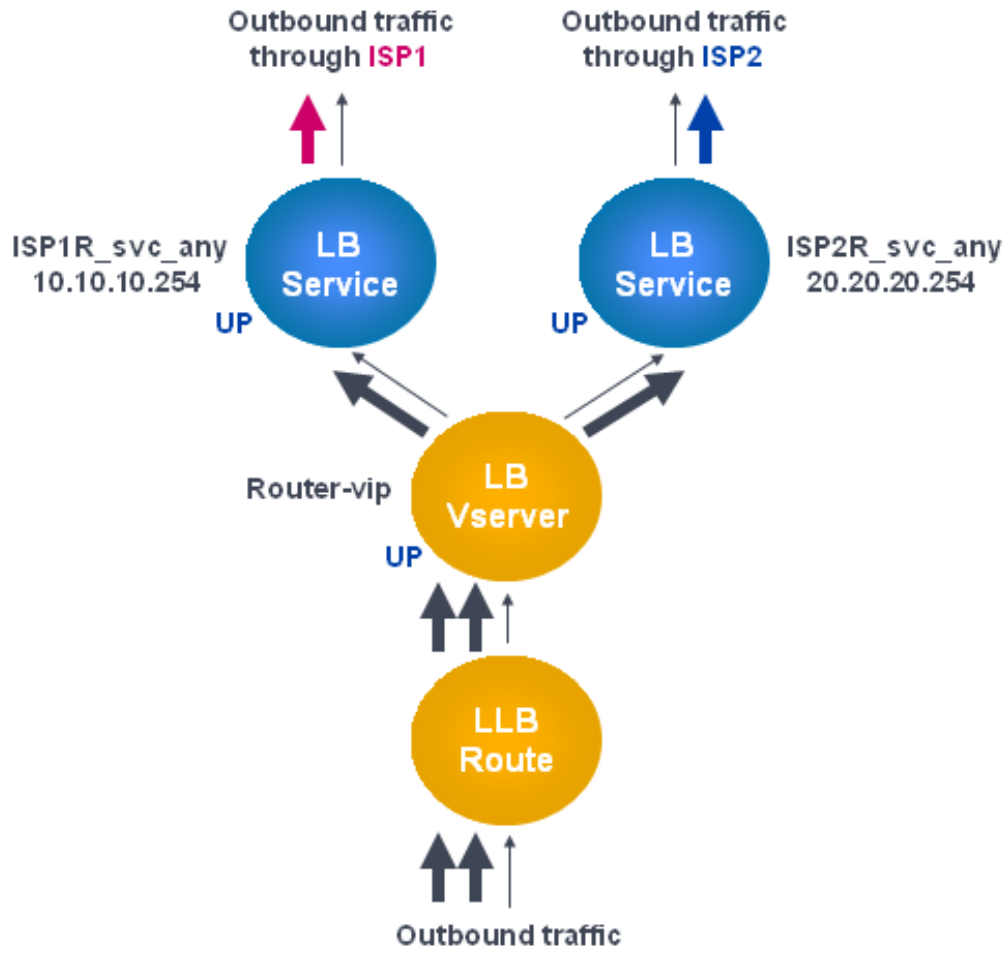


Figure 1. Basic LLB Setup

Note: If your Internet service provider has provided an IPv6 address, replace the IPv4 service with an IPv6 service in the above figure.

Creating and Binding a Transparent Monitor

You create a transparent monitor to monitor the health of upstream devices, such as routers. You can then bind the transparent monitor to services. The default PING monitor monitors the connectivity only between the NetScaler appliance and the upstream device. The transparent monitor monitors all the devices existing in the path from the appliance to the device that owns the destination IP address specified in the monitor. If a transparent monitor is not configured and the status of the router is UP but one of the next hop devices from that router is down, the appliance includes the router while performing load balancing and forwards the packet to the router. However, the packet is not delivered to the final destination because one of the next hop devices is down. By binding a transparent monitor, if any of the devices (including the router) are down, the service is marked as DOWN and the router is not included when the appliance performs link load balancing.

To create a transparent monitor by using the command line interface

At the command prompt, type:

- add lb monitor <monitorName> <type> -destIP <ip_addr|*> -transparent YES
- show lb monitor [<monitorName>]

Example

```
add lb monitor monitor-1 PING -destIP 10.10.10.11 -transparent YES
> show lb monitor monitor-1
1)   Name.......: monitor-1  Type......:     PING   State....:   ENABLED
Standard parameters:
  Interval.........:          5 sec   Retries...........:             3
  Response timeout.:          2 sec   Down time.........:         30 sec
  Reverse..........:             NO   Transparent.......:           YES
  Secure...........:             NO   LRTM..............:       ENABLED
  Action...........:   Not applicable   Deviation.........:         0 sec
  Destination IP...:      10.10.10.11
  Destination port.:    Bound service
  Iptunnel.........:             NO
  TOS..............:             NO   TOS ID............:             0
  SNMP Alert Retries:             0     Success Retries..:             1
  Failure Retries..:             0
```

Parameters for creating a transparent monitor

monitorName (Name)

The name of the monitor. Maximum Length: 31 characters.

type (Type)

The type of monitor.

destIP (Destination IP)

The IP address to which the probe is sent. If the destination IP address is set to 0, the destination IP address is that of the server to which the monitor is bound. Default value: 0.

transparent (Transparent)

The state of the monitor for transparent devices, such as firewalls, based on the responsiveness of the services behind them. If the monitoring of transparent devices is enabled, the destination IP address should be specified. The probe is sent to the specified destination IP address by using the MAC address of the transparent device. Possible values: YES, NO. Default value: NO.

To create a transparent monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. In the Monitors pane, click Add.
3. In the Create Monitor dialog box, set the following parameters:
   - Name*
   - Type*
   - Destination IP
   - Transparent

   * A required parameter
4. Click Create, and then click Close.
5. In the Monitors pane, select the monitor that you just configured and verify that the settings displayed in the Details pane are correct.

To bind a monitor to a service by using the command line interface

At the command prompt, type:

- bind lb monitor <monitorName> <serviceName>
- show service <name>

Example

```
bind lb monitor monitor-HTTP-1 isp1R_svc_any
 Done
> show service isP1R_svc_any
        ISP1R_svc_any (10.10.10.254:*) - ANY
        State: UP
        Last state change was at Thu Sep  2 10:51:07 2010
        Time since last state change: 0 days, 18:41:55.130
        Server Name: 10.10.10.254
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
              State: UP  Weight: 1
              Probes: 1256       Failed [Total: 0 Current: 0]
              Last response: Success - ICMP echo reply received.
              Response Time: 1.322 millisec
 Done
```

Parameters for binding a monitor

monitorName

The name of the monitor to be bound. Maximum Length: 31 characters.

serviceName

The name of the service or a service group to which the monitor is to be bound. Maximum Length: 127 characters.

To bind a monitor to a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select a service to which you want to bind a monitor, and then click Open.
3. In the Configure Service dialog box, on the Monitors tab, under Available, select the monitor that you want to bind to the service, and then click Add.
4. Click OK.
5. In the Services pane, select the service that you just configured and verify that the settings displayed in the Details pane are correct.

Configuring RNAT with LLB

You can configure an LLB setup for reverse network address translation (RNAT) for outbound traffic. This ensures that the return network traffic for a specific flow is routed through the same path. First configure basic LLB, as described in "Configuring a Basic LLB Setup", and then configure RNAT. You must then enable use subnet IP (USNIP) mode.

To configure RNAT by using the command line interface

At the command prompt, type:

- set rnat <network> <netmask>
- show rnat

Example

```
set rnat 10.102.29.0 255.255.255.0
> show rnat
1)      Network: 10.102.29.0    Netmask: 255.255.255.0
        NatIP: *
```

Parameters for configuring RNAT

network

The network or subnet from which the traffic is flowing.

netmask

The subnet mask for the network.

To configure RNAT by using the configuration utility

1. In the navigation pane, expand Network, and then click Routes.
2. In the detailspane, on the RNAT tab, click Configure RNAT.
3. In the Configure RNAT dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring RNAT" as shown:
   - Network*—network
   - Netmask*—netmask

   * A required parameter
4. Click Create, and then click Close. The RNAT route that you just created appears in the on the RNAT tab in the Routes pane.

To enable Use Subnet IP mode by using the command line interface

At the command prompt, type:

- enable ns mode USNIP
- show ns mode

Example

```
enable ns mode USNIP
> show ns mode
      Mode                  Acronym          Status
      -------               -------          ------
 1)   Fast Ramp               FR               ON
 2)   ....
 8)   Use Subnet IP           USNIP            ON
 9)   …
```

To enable Use Subnet IP mode by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In details pane, under Modes and Features, click Configure modes.
3. In the Configure Modes dialog box, select Use Subnet IP, and then click OK.
4. In the Enable/Disable Mode(s) message box, click Yes.

Configuring a Backup Route

To prevent disruption in services when the primary route is down, you can configure a backup route. Once the backup route is configured, the NetScaler appliance automatically uses it when the primary route fails. First create a primary virtual server as described in "Configuring an LLB Virtual Server and Binding a Service." To configure a backup route, create a secondary virtual server similar to a primary virtual server and then designate this virtual server as a backup virtual server (route).

In the following diagram, **Router-vip** is the primary virtual server, and **Backup_Router-vip** is the secondary virtual server designated as the backup virtual server.

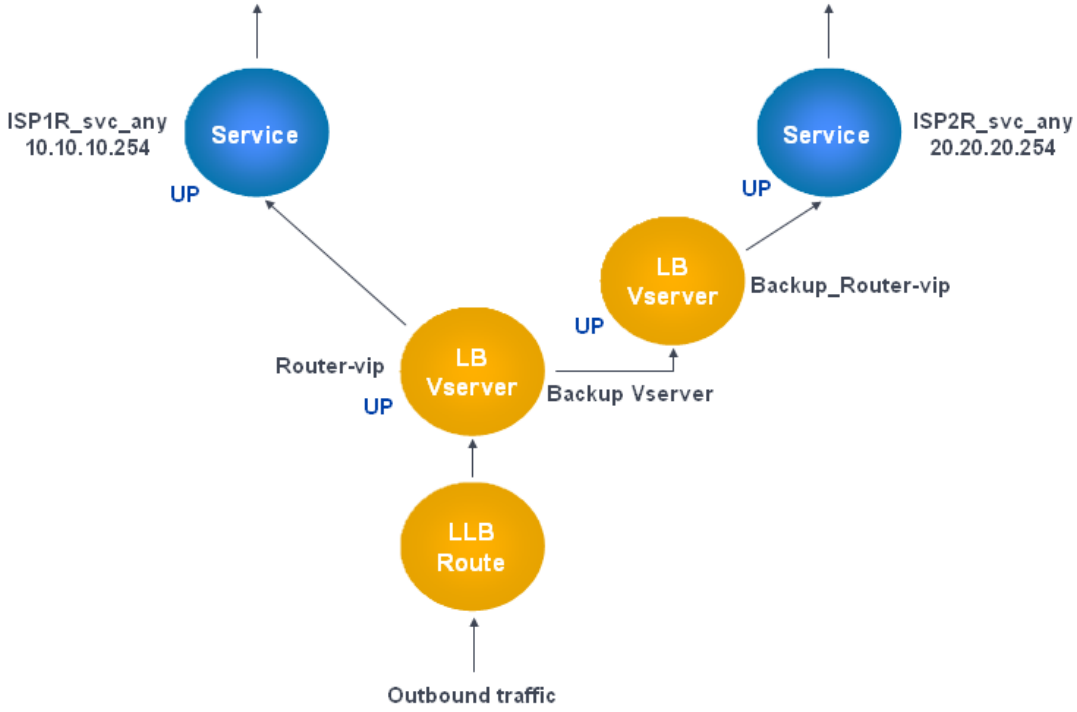


Figure 1. Backup Route Setup

Note: If your Internet service provider has provided an IPv6 address, replace the IPv4 service with an IPv6 service in the above figure.

By default, all traffic is sent through the primary route. However, when the primary route fails, all traffic is diverted to the backup route as shown in the following diagram.

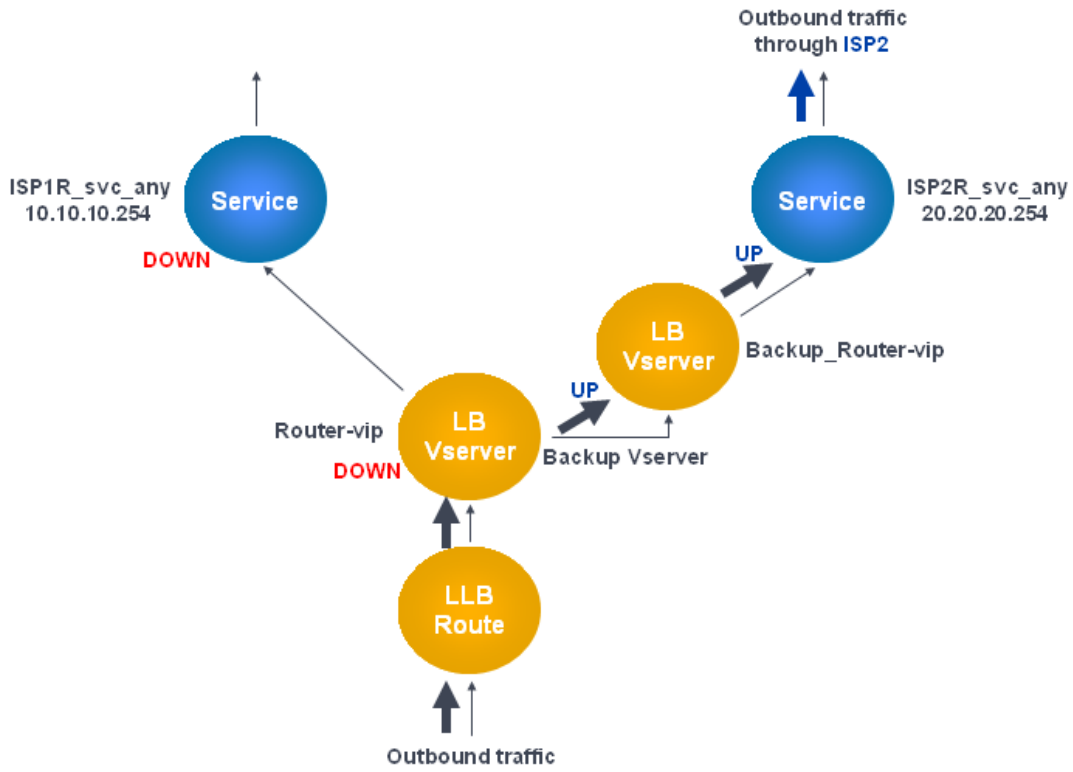


Figure 2. Backup Routing in Operation

Note: If your Internet service provider has provided an IPv6 address, replace the IPv4 service with an IPv6 service in the above figure.

To set the secondary virtual server as the backup virtual server by using the command line interface

At the command prompt, type:

set lb vserver <name> -backupVserver <string>

Example

```
set lb vserver Router-vip -backupVServer Backup_Router-vip
> show lb vserver Router-vip
        Router-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Fri Sep  3 04:46:48 2010
        Time since last state change: 0 days, 03:09:45.600
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       1 (Active)
```

```
    Configured Method: ROUNDROBIN
    Mode: IP
    Persistence: DESTIP    Persistence Mask: 255.255.255.255    Persistence v6MaskLength: 128    Persiste
    Backup: Router2-vip
    Connection Failover: DISABLED
Done
```

Parameters for setting up the secondary virtual server as the backup virtual server

name

The name of the load balancing virtual server for which you are configuring a backup. Maximum Length: 127 characters.

backupVServer

The name of the backup virtual server. Maximum Length: 127 characters.

To set the secondary virtual server as the backup virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the secondary virtual server for which you want to configure the backup virtual server, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, click the Advanced tab.
4. In the Backup Virtual Server drop-down list, select the secondary backup virtual server, and then click OK.

Resilient LLB Deployment Scenario

In the following diagram, there are two networks: 30.30.30.0 and 30.30.31.0. Link load balancing is configured based on the destination IP address. Two routes are configured with gateways **Router1-vip** and **Router2-vip**, respectively. **Router1-vip** is configured as a backup to **Router2-vip** and vice versa. All traffic with the destination IP specified as 30.30.30.30 is sent through **Router1-vip** and traffic with the destination IP specified as 30.30.31.31 is sent through **Router2-vip**.

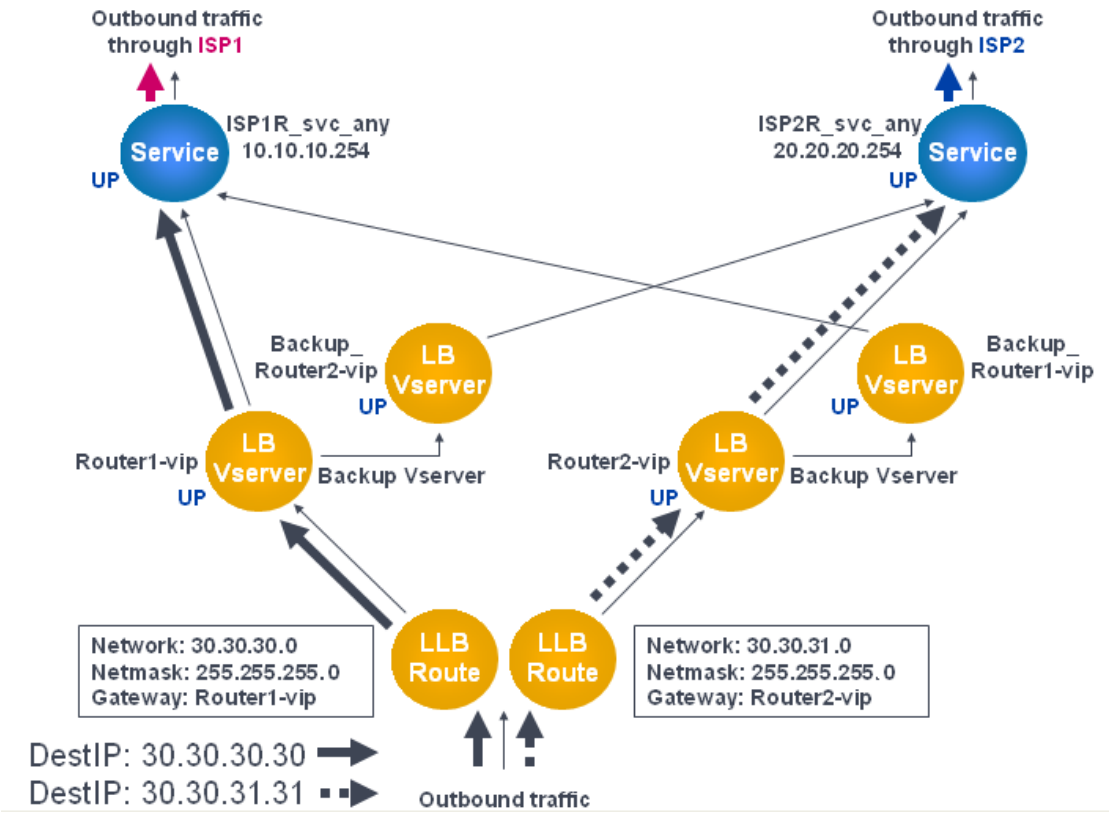


Figure 1. Resilient LLB Deployment Setup

Note: If your Internet service provider has provided an IPv6 address, replace the IPv4 service with an IPv6 service in the above figure.

However, if any one of the gateways (**Router1-vip** or **Router2-vip**) is DOWN, traffic is routed through the backup router. In the following diagram, **Router1-vip** for ISP1 is DOWN, so all traffic with the destination IP specified as 30.30.30.30 is also sent through ISP2.

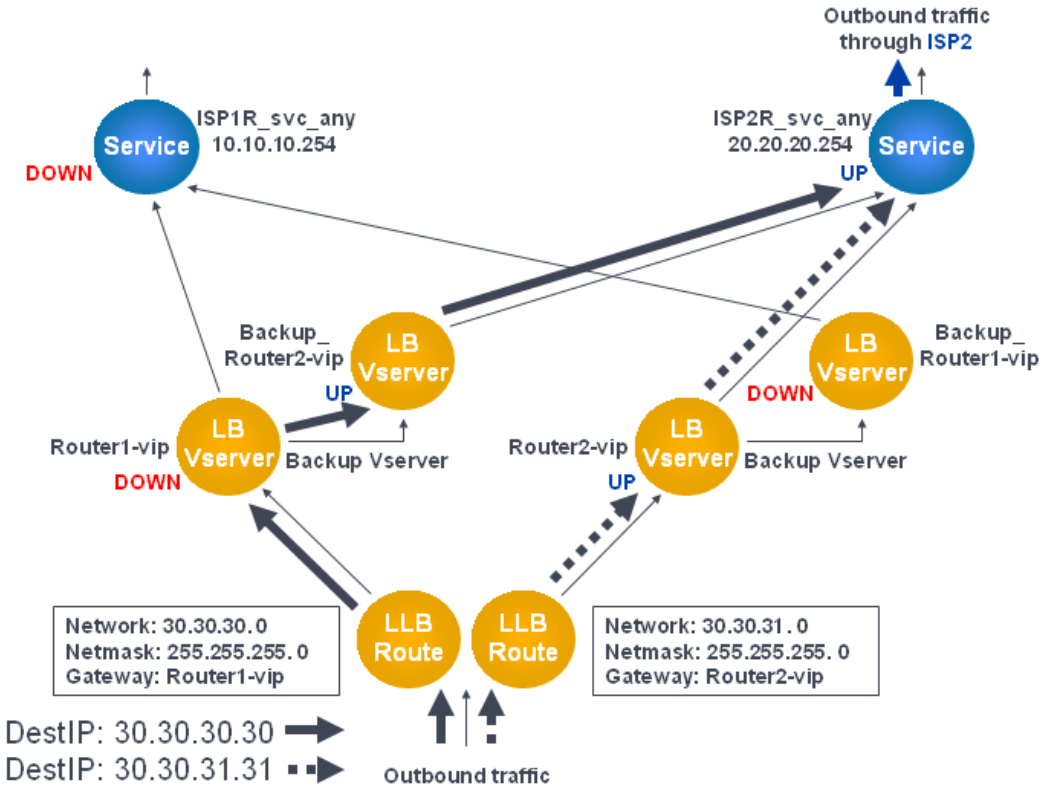


Figure 2. Resilient LLB Deployment Scenario

Note: If your Internet service provider has provided an IPv6 address, replace the IPv4 service with an IPv6 service in the above figure.

Monitoring an LLB Setup

After the configuration is up and running, you should view the statistics for each service and virtual server to check for possible problems.

Viewing the Statistics of a Virtual Server

To evaluate the performance of virtual servers or to troubleshoot problems, you can display details of the virtual servers configured on the NetScaler appliance. You can display a summary of statistics for all the virtual servers, or you can specify the name of a virtual server to display the statistics only for that virtual server. You can display the following details:

- Name
- IP address
- Port
- Protocol
- State of the virtual server
- Rate of requests received
- Rate of hits

To display virtual server statistics by using the command line interface

To display a summary of the statistics for all the virtual servers currently configured on the NetScaler, or for a single virtual server, at the command prompt, type:

stat lb vserver [-detail] [<name>]

Example

```
>stat lb vserver -detail
Virtual Server(s) Summary
                  vsvrIP  port     Protocol       State    Req/s   Hits/s
One                    *    80         HTTP          UP      5/s      0/s
Two                    *     0          TCP        DOWN      0/s      0/s
Three                  *  2598          TCP        DOWN      0/s      0/s
dnsVirtualNS    10.102.29.90    53          DNS        DOWN      0/s      0/s
BRVSERV          10.10.1.1    80         HTTP        DOWN      0/s      0/s
LBVIP         10.102.29.66    80         HTTP          UP      0/s      0/s
 Done
```

Parameters for displaying statistics

detail

Include the statistics for hits per second and the total number of hits.

name

Name of the virtual server whose statistics are displayed.

To display virtual server statistics by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. If you want to display the statistics for only one virtual server, in the details pane, select the virtual server whose statistics you want to display.
3. In the details pane, click Statistics.

Viewing the Statistics of a Service

You can view the rate of requests, responses, request bytes, response bytes, current client connections, requests in surge queue, current server connections, and so forth using the service statistics.

To view the statistics of a service by using the command line interface

At the command prompt, type:

stat service <name>

Example

stat service Service-HTTP-1

To view the statistics of a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service whose statistics you want to view (for example, Service-HTTP-1).
3. Click Statistics. The statistics appear in a new window.

Load Balancing

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

You can configure the load balancing feature to:

- Distribute all requests for a specific protected website, application, or resource between two or more identically-configured servers.
- Use any of several different algorithms to determine which server should receive each incoming user request, basing the decision on different factors, such as which server has the fewest current user connections or which server has the lightest load.

The load balancing feature is a core feature of the NetScaler appliance. Most users first set up a working basic configuration and then customize various settings, including persistence for connections. In addition, you can configure features for protecting the configuration against failure, managing client traffic, managing and monitoring servers, and managing a large scale deployment.

How Load Balancing Works

In a basic load balancing setup, clients send their requests to the IP address of a virtual server configured on the NetScaler appliance. The virtual server distributes them to the load-balanced application servers according to a preset pattern, called the load balancing algorithm. In some cases, you might want to assign the load balancing virtual server a wildcard address instead of a specific IP address. For instructions about specifying a global HTTP port on the appliance, see Global HTTP Ports.

Load Balancing Basics

A load balancing setup includes a load-balancing virtual server and multiple load-balanced application servers. The virtual server receives incoming client requests, uses the load balancing algorithm to select an application server, and forwards the requests to the selected application server. The following conceptual drawing illustrates a typical load balancing deployment. Another variation involves assigning a global HTTP port.

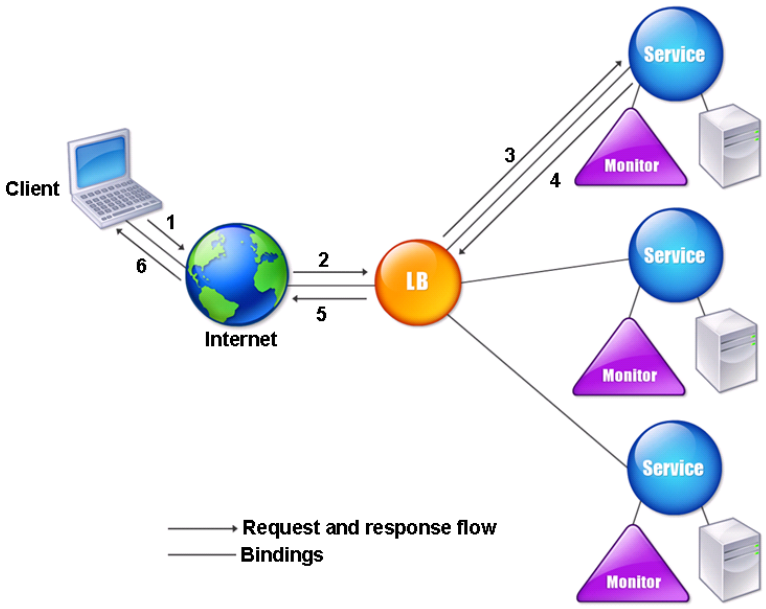


Figure 1. Load Balancing Architecture

The load balancing virtual server can use any of a number of algorithms (or methods) to determine how to distribute load among the load-balanced servers that it manages. The default load balancing method is the least connection method, in which the NetScaler appliance forwards each incoming client connection to whichever load-balanced application server currently has the fewest active user connections.

The entities that you configure in a typical NetScaler load balancing setup are:

- **Load balancing virtual server.** The IP address, port, and protocol combination to which a client sends connection requests for a particular load-balanced website or application. If the application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address.

- **Service.** The IP address, port, and protocol combination used to route requests to a specific load-balanced application server. A service can be a logical representation of the application server itself, or of an application running on a server that hosts multiple applications. After creating a service, you bind it to a load balancing virtual server.

- **Server object.** A virtual entity that enables you to assign a name to a physical server instead of identifying the server by its IP address. If you create a server object, you can specify its name instead of the server's IP address when you create a service. Otherwise, you must specify the server's IP address when you create a service, and the IP address becomes the name of the server.

- **Monitor.** An entity on the NetScaler appliance that tracks a service and ensures that it is operating correctly. The monitor periodically probes (or performs a health check on) each service to which you assign it. If the service does not respond within the time specified by the time-out, and a specified number of health checks fail, that service is marked DOWN. The NetScaler appliance then skips that service when performing load balancing, until the issues that caused the service to quit responding are fixed.

The virtual server, services, and load balanced application servers in a load balancing setup can use either Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) IP addresses. You can mix IPv4 and IPv6 addresses in a single load balancing setup.

For variations in the load balancing setup, see the following use cases:

- Configuring Load Balancing in Direct Server Return Mode
- Configuring LINUX Servers in DSR Mode
- Configuring DSR Mode When Using TOS
- Configuring Load Balancing in DSR Mode by Using IP Over IP
- Configuring Load Balancing in One-arm Mode
- Configuring Load Balancing in the Inline Mode
- Load Balancing of Intrusion Detection System Servers
- Load Balancing RDP services

Understanding the Topology

In a load balancing setup, the load balancing server is logically located between the client and the server farm, and manages traffic flow to the servers in the server farm. On the NetScaler appliance, the application servers are represented by virtual entities called services. The following diagram shows the topology of a basic load balancing configuration.

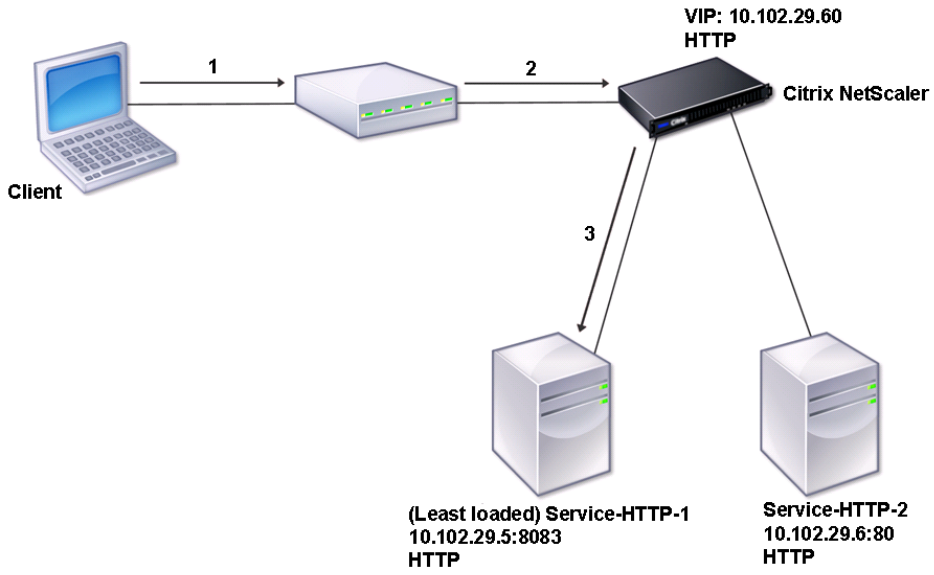


Figure 1. Basic Load Balancing Topology

In the diagram, load balancing is used to manage traffic flow to the servers. The virtual server selects the service and assigns it to serve client requests. Consider a scenario where the services Service-HTTP-1 and Service-HTTP-2 are created and bound to the virtual server named Vserver-LB-1. Vserver-LB-1 forwards the client request to either Service-HTTP-1 or Service-HTTP-2. The NetScaler appliance uses the least connection load balancing method to select the service for each request. The following table lists the names and values of the basic entities that must be configured on the appliance.

Entity	Mandatory Parameters and Sample Values			
	Name	IP Address	Port	Protocol
Virtual server	Vserver-LB-1	10.102.29.60	80	HTTP
Services	Service-HTTP-1	10.102.29.5	8083	HTTP
	Service-HTTP-2	10.102.29.6	80	HTTP
Monitors	Default	None	None	None

The following diagram shows the load balancing sample values and mandatory parameters that are described in the preceding table.

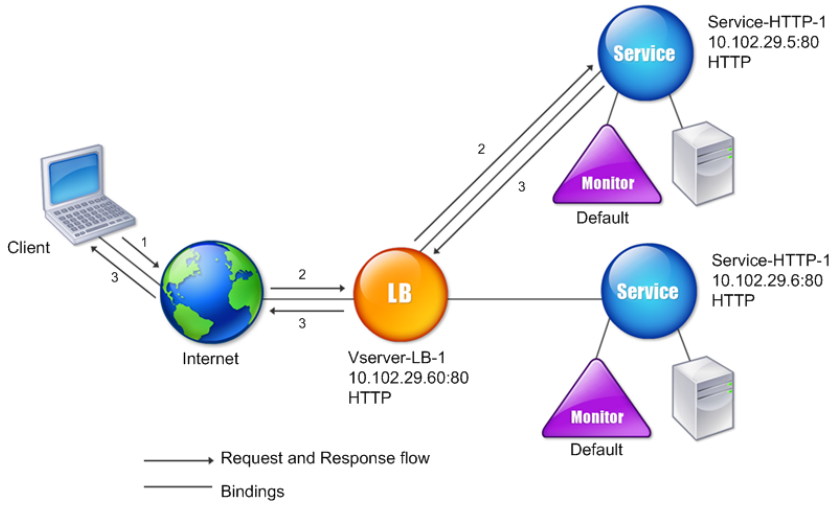


Figure 2. Load Balancing Entity Model

Use of Wildcards Instead of IP Addresses and Ports

In some cases you might need to use a wildcard for the IP address or the port of a virtual server or for the port of a service. The following cases may require using a wildcard:

- If the NetScaler appliance is configured as a transparent pass through, which must accept all traffic that is sent to it regardless of the IP or port to which it is sent.
- If one or more services listen on ports that are not well known.
- If one or more services, over time, change the ports that they listen on.
- If you reach the limit for the number of IP addresses and ports that you can configure on a single NetScaler appliance.
- If you want to create virtual servers that listen for all traffic on a specific virtual LAN.

When a wildcard-configured virtual server or service receives traffic, the NetScaler appliance determines the actual IP address or port and creates new records for the service and associated load balanced application server. These dynamically created records are called dynamically learned server and service records.

For example, a firewall load balancing configuration can use wildcards for both the IP address and port. If you bind a wildcard TCP service to this type of load balancing virtual server, the virtual server receives and processes all TCP traffic that does not match any other service or virtual server.

The following table describes some of the different types of wildcard configurations and when each should be used.

IP	Port	Protocol	Description
*	*	TCP	A general wildcard virtual server that accepts traffic sent to any IP address and port on the NetScaler appliance. When using a wildcarded virtual server, the appliance dynamically learns the IP and port of each service and creates the necessary records as it processes traffic.

*	*	TCP	A firewall load balancing virtual server. You can bind firewall services to this virtual server, and the NetScaler appliance passes traffic through the firewall to the destination.
IP Address	*	TCP,UDP, and ANY	A virtual server that accepts all traffic that is sent to the specified IP address, regardless of the port. You must explicitly bind to this type of virtual server the services to which it will redirect traffic. It will not dynamically learn them. **Note:** You do not configure services or virtual servers for a global HTTP port. In this case, you configure a specific port as a global HTTP port (for example, `set ns param -httpPort 80`). The appliance then accepts all traffic that matches the port number, and processes it as HTTP traffic. The appliance dynamically learns and creates services for this traffic.

*	port	SSL, SSL_TCP	A virtual server that accepts all traffic sent to any IP address on a specific port. Used for global transparent SSL offloading. All SSL, HTTP, and TCP processing that usually is performed for a service of the same protocol type is applied to traffic that is directed to this specific port. The appliance uses the port to dynamically learn the IP of the service it should use. If `-cleartext` is not specified, the NetScaler appliance uses end-to-end SSL.
*	port	Not applicable	All other virtual servers that can accept traffic to the port. You do not bind services to these virtual servers; the NetScaler appliance learns them dynamically.

Note: If you have configured your NetScaler appliance as a transparent pass through that makes use of global (wildcard) ports, you may want to turn on Edge mode. For more information, see "Configuring Edge Mode."

The NetScaler appliance attempts to locate virtual servers and services by first attempting an exact match. If none is found, it continues to search for a match based on wildcards, in the following order:

1. Specific IP address and specific port number
2. Specific IP address and a * (wildcard) port
3. * (wildcard) IP address and a specific port
4. * (wildcard) IP address and a * (wildcard) port

If the appliance is unable to select a virtual server by IP address or port number, it searches for a virtual server on the basis of the protocol used in the request, in the following order:

1. HTTP
2. TCP
3. ANY

Configuring Global HTTP Ports

You do not configure services or virtual servers for a global HTTP port. Instead, you configure a specific port by using the `set ns param` command. After configuring this port, the NetScaler appliance accepts all traffic that matches the port number, and processes it as HTTP traffic, dynamically learning and creating services for that traffic.

You can configure more than one port number as a global HTTP port. If you are specifying more than one port number in a single `set ns param` command, separate the port numbers by a single white space. If one or more ports have already been specified as global HTTP ports, and you want to add one or more ports without removing the ports that are currently configured, you must specify all the port numbers, current and new, in the command. Before you add port numbers, use the `show ns param` command to view the ports that are currently configured.

To configure a global HTTP port by using the command line interface

At the command prompt, type the following commands to configure a global HTTP port and verify the configuration:

- set ns param –httpPort <port>
- show ns param

Example 1: Configuring a port as a global HTTP port

In this example, port 80 is configured as a global HTTP port.

```
> set ns param -httpPort 80
 Done
> show ns param
        Global configuration settings:
                     HTTP port(s): 80
                  Max connections: 0
          Max requests per connection: 0
                Client IP insertion: DISABLED
                    Cookie version: 0
       Persistence Cookie Secure Flag: ENABLED
       ...
       ...
```

Example 2: Adding ports when one or more global HTTP ports are already configured

In this example, port 8888 is added to the global HTTP port list. Port 80 is already configured as a global HTTP port.

```
> show ns param

        Global configuration settings:
                        HTTP port(s): 80
                    Max connections: 0
          Max requests per connection: 0
                 Client IP insertion: DISABLED
                     Cookie version: 0
        Persistence Cookie Secure Flag: ENABLED
                        Min Path MTU: 576
        ...
        ...
 Done
> set ns param -httpPort 80 8888
 Done
>  show ns param

        Global configuration settings:
                        HTTP port(s): 80,8888
                    Max connections: 0
          Max requests per connection: 0
                 Client IP insertion: DISABLED
                     Cookie version: 0
        Persistence Cookie Secure Flag: ENABLED
                        Min Path MTU: 576

        ...
        ...
 Done
>
```

Parameters for configuring a global HTTP port

httpPort

The HTTP ports on the web server. This setting allows the system to perform connection off-load for any client request that has a destination port matching one of the configured ports. Minimum value: 1.

To configure a global HTTP port by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Settings, click Change HTTP parameters.
3. In the Configure HTTP Parameters dialog box, in the HTTP Port area, do the following:
   - To add a port, enter the port number, and then click Add.
   - To remove a port that has already been configured, click the port number, and then click Remove.
4. Click OK.

Setting Up Basic Load Balancing

Before configuring your initial load balancing setup, enable the load balancing feature. Then begin by creating at least one service for each server in the load balancing group. With the services configured, you are ready to create a load balancing virtual server, and bind each service to the virtual server. That completes the initial setup. Before proceeding with further configuration, verify your configuration to make sure that each element was configured properly and is operating as expected.

Enabling Load Balancing

You can configure load balancing entities such as services and virtual servers when the load balancing feature is disabled, but they will not function until you enable the feature.

To enable load balancing by using the command line interface

At the command prompt, type the following command to enable load balancing and verify the configuration:

- enable ns feature LB
- show ns feature

Example

```
> enable ns feature LoadBalancing
 Done
> show ns feature

      Feature                Acronym          Status
      -------                -------          ------
1)    Web Logging              WL               OFF
2)    Surge Protection         SP               ON
3)    Load Balancing           LB               ON
.
.
.
24)   NetScaler Push           push             OFF
Done
```

To enable load balancing by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features, click Change basic features.
3. In the Configure Basic Features dialog box, select the Load Balancing check box, and then click OK.
4. In the Enable/Disable Feature(s)? message box, click Yes.

Configuring Services

After you enable the load balancing feature, you must create at least one service for each application server that is to be included in your load balancing setup. The services that you configure provide the connections between the NetScaler appliance and the load balanced servers. Each service has a name and specifies an IP address, a port, and the type of data that is served.

If you create a service without first creating a server object, the IP address of the service is also the name of the server that hosts the service. If you prefer to identify servers by name rather than IP address, you can create server objects and then specify a server's name instead of its IP address when you create a service.

When you create a service that uses UDP as the transport layer protocol, a ping monitor is automatically bound to the service. A ping monitor is the most basic of the built-in monitors. When you create a service that uses TCP as the transport layer protocol, a TCP_default monitor is automatically bound to the service. When you develop a strategy for managing your load balancing setup, you might decide to bind a different type of monitor, or multiple monitors, to the service.

Adding a Server

If you add a server to the list of servers before creating a service to represent that server, you can assign a name to the server. You can then specify the server's name instead of its IP address when you create a service. If you create a service from the configuration utility, you can select the server from the drop-down list. When adding the server to the list, you might want to assign it a name that helps identify the kind of services that you will create with it. You can also specify its state and add a comment.

When adding a server, you must identify it by specifying its IP address or domain name. If you specify the domain name, you can later change the IP address of the physical server without having to modify the server's entry in the list of servers on the appliance. The domain name is resolved to an IP address that is specified in an address record on the DNS.

During hardware maintenance or software upgrades, you may have to make the server DOWN. If the server is domain based, to override the IP address resolved by the DNS, you can configure an IP address mask and a translation IP address on the NetScaler appliance. For more information, see "Translating the IP Address of a Domain Based Server."

You can add a range of servers from a single CLI command or the same dialog box. The names in the range vary by a number used as a suffix or prefix. For example, server1, server2, and so on. From the configuration utility, you can specify a range only in the last octet of the IP address, which is the fourth in case of an IPv4 address and the eighth in case of an IPv6 address. From the command line, you can specify the range in any octet of the IP address. For more information, see "Creating a Range of Virtual Servers."

To add a server by using the command line interface

At the command prompt, type:

add server <name> (<ipAddress> | (<domain> [-ipv6Address (YES | NO)]) [-state (ENABLED | DISABLED)] [-comment <string>]

Examples

```
add server myserver www.example.net -state DISABLED -comment "Web server for example.net"
Done
> show server myserver
   Name:          myserver      State:DISABLED
   Domain: www.example.net      Resolve Retry: 0 Secs
   Translation IP:        0.0.0.0  Translation Mask:        0.0.0.0
   Comment: "Web server for example.net"
 Done
>
```

Parameters for configuring a server

name

The name assigned to the server. This alphanumeric string is required. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

ipAddress

IP address of the server, in either IPv4 or IPv6 format.

If the server is not reachable from the appliance or is not active, the service is marked as DOWN.

domain

Domain name that resolves to the IP address that represents the server.

ipv6Address

Resolve the domain name to an IPv6 address. Possible values: YES, NO. Default: NO.

state

The initial state of the server. Possible values: ENABLED, DISABLED. Default: ENABLED.

comment

A comment to help identify the server. Maximum length: 255 characters. To include spaces in a comment that you type on the command line, enclose the entire comment inside quotation marks. The quotation marks become part of the comment. They are not required if you use the configuration utility.

To add a server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Servers.
2. In the details pane, click Add.
3. In the Create Server dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring a server" as shown above:
   - Server Name—name
   - IP Address—ipAddress (Select IP Address and type the address. Before typing an IPv6 address, select the **IPv6** check box.)
   - Domain Name—domain (For a domain-name based server, select Domain Name and type the name of the server's domain.)
   - Enable after Creating—state
   - Comment—comment
4. If you specify the domain name of the server and you want the domain name to be resolved to an IPv6 address, select the IPv6 Domain check box.
5. Click Create, and then click Close. The server you named appears in the Servers pane.

Creating a Service

Before you create a service, you need to understand the different service types and how each is used. The following list describes the types of services supported on the NetScaler appliance.

HTTP

Used for load-balanced servers that accept HTTP traffic, such as standard web sites and web applications. The HTTP service type enables the NetScaler appliance to provide compression, content filtering, caching, and client keep-alive support for your Layer 7 web servers. This service type also supports virtual server IP port insertion, redirect port rewriting, Web 2.0 Push, and URL redirection support.

Because HTTP is a TCP-based application protocol, you can also use the TCP service type for web servers. If you do so, however, the NetScaler appliance is able to perform only Layer 4 load balancing. It cannot provide any of the Layer 7 support described earlier.

SSL

Used for servers that accept HTTPS traffic, such as ecommerce web sites and shopping cart applications. The SSL service type enables the NetScaler appliance to encrypt and decrypt SSL traffic (perform SSL offloading) for your secure web applications. It also supports HTTP persistence, content switching, rewrite, virtual server IP port insertion, Web 2.0 Push, and URL redirection.

You can also use the SSL_BRIDGE, SSL_TCP, or TCP service types. If you do so, however, the NetScaler performs only Layer 4 load balancing. It cannot provide SSL offloading or any of the Layer 7 support described above

FTP

Used for servers that accept FTP traffic. The FTP service type enables the NetScaler appliance to support specific details of the FTP protocol.

You can also use TCP or ANY service types for FTP servers.

TCP

Used for servers that accept many different types of TCP traffic, or that accept a type of TCP traffic for which a more specific type of service is not available.

You can also use the ANY service type for these servers.

SSL_TCP

Used for servers that accept non-HTTP-based SSL traffic, to support SSL offloading.

You can also use the TCP service type for these services. If you do so, the NetScaler appliance performs both the Layer 4 load balancing and SSL offloading.

UDP

Used for servers that accept UDP traffic. You can also use the ANY service type.

SSL_BRIDGE

Used for servers that accept SSL traffic when you do not want the NetScaler appliance to perform SSL offloading. Alternatively, you can use the SSL_TCP service type.

NNTP

Used for servers that accept Network News Transfer Protocol (NNTP) traffic, typically Usenet sites.

DNS

Used for servers that accept DNS traffic, typically nameservers. With the DNS service type, the NetScaler appliance validates the packet format of each DNS request and response. It can also cache DNS responses. You can apply DNS policies to DNS services.

You can also use the UDP service type for these services. If you do, however, the NetScaler appliance can only perform Layer 4 load balancing. It cannot provide support for DNS-specific features.

ANY

Used for servers that accept any type of TCP, UDP, or ICMP traffic. The ANY parameter is used primarily with firewall load balancing and link load balancing.

SIP-UDP

Used for servers that accept UDP-based Session Initiation Protocol (SIP) traffic. SIP initiates, manages, and terminates multimedia communications sessions, and has emerged as the standard for Internet telephony (VoIP).

You can also use the UDP service type for these services. If you do, however, the NetScaler appliance performs only Layer 4 load balancing. It cannot provide support for SIP-specific features.

DNS-TCP

Used for servers that accept DNS traffic, where the NetScaler appliance acts as a proxy for TCP traffic sent to DNS servers. With services of the DNS-TCP service type, the NetScaler appliance validates the packet format of each DNS request and response and can cache DNS responses, just as with the DNS service type.

You can also use the TCP service type for these services. If you do, however, the NetScaler appliance only performs Layer 4 load balancing of external DNS name servers. It cannot provide support for any DNS-specific features.

RTSP

Used for servers that accept Real Time Streaming Protocol (RTSP) traffic. RTSP provides delivery of multimedia and other streaming data. Select this type to support audio, video, and other types of streamed media.

You can also use the TCP service type for these services. If you do, however, the NetScaler appliance performs only Layer 4 load balancing. It cannot parse the RTSP stream or provide support for RTSPID persistence or RTSP NATting.

DHCPRA

Used for servers that accept DHCP traffic. The DHCPRA service type can be used to relay DHCP requests and responses between VLANs.

DIAMETER

Used for load balancing Diameter traffic among multiple Diameter servers. Diameter uses message-based load balancing.

SSL_DIAMETER

Used for load balancing Diameter traffic over SSL.

Services are designated as DISABLED until the NetScaler appliance connects to the associated load-balanced server and verifies that it is operational. At that point, the service is designated as ENABLED. Thereafter, the NetScaler appliance periodically monitors the status of the servers, and places any that fail to respond to monitoring probes (called health checks) back in the DISABLED state until they respond.

Note: You can create a range of services from a single CLI command or the same dialog box. The names in the range vary by a number used as a suffix/prefix. For example, service1, service2, and so on. From the configuration utility, you can specify a range only in the last octet of the IP address, which is the fourth in case of an IPv4 address and the eighth in case of an IPv6 address. From the command line, you can specify the range in any octet of the IP address.

To create a service by using the command line interface

At the command prompt, type:

add service <name> <serverName> <serviceType> <port>

Example

add service Service-HTTP-1 192.0.2.5 HTTP 80

Parameters for configuring a service

name

Name of the service. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serverName

Either the name of a previously created server object, or the IP address of the load-balanced server that hosts this service, in either IPv4 or IPv6 format. When you provide the IP address of the service, a server object is created with this IP address as its name. You can also create a server object manually, and then select the server name instead of an IP address from the drop-down menu that is associated with this field.

If the server is not reachable from the NetScaler or is not active, the service is designated as DOWN.

serviceType

The type of connections that the service will handle. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, DNS_TCP, ADNS_TCP, RADIUS, MYSQL, MSSQL, and RDPHTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, and SSL_DIAMETER. Default: HTTP.

port

Port on which the service listens. The port number must be a positive number not greater than 65534.

Note: For more information about the SSL and SSL_TCP service types, see SSL Offload and Acceleration.

To create a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating a service” as shown:
   - Service Name—name
   - Server—serverName
   - Protocol—serviceType
   - Port—port
4. Click Create, and then click Close. The service you created appears in the Services pane.

Troubleshooting

When binding a service group to a load balancing virtual server, the appliance displays the following error message:

```
Operation not permitted error
```

Are there any recommended settings that can resolve this issue?

Resolution: When creating a service, you must enable the Health Monitoring option. To resolve this issue, edit the service and select the Health Monitoring option.

Creating a Virtual Server

After you create your services, you must create a virtual server to accept traffic for the load balanced Web sites, applications, or servers. Once load balancing is configured, users connect to the load-balanced Web site, application, or server through the virtual server's IP address or FQDN.

Note: The virtual server is designated as DOWN until you bind the services that you created to it, and until the NetScaler appliance connects to those services and verifies that they are operational. Only then is the virtual server designated as UP.

To create a virtual server by using the command line interface

At the command prompt, type:

add lb vserver <name> <serviceType> <ip> <port>

Example

add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80

Parameters for creating a virtual server

name

Name of the virtual server. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( )

IPAddress

IP address of the virtual server. This IP address can be an IPv4 or IPv6 address, and is usually a public IP address. Clients send connection requests to this IP address.

serviceType

The type of services to which the virtual server distributes requests. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, and MSSQLHTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, and SSL_DIAMETER. Default: HTTP

port

Port on which the virtual server listens for client connections. The port number must be between 0-65535.

To create a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Load Balancing) dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating a virtual server” as shown:
   - Name—name
   - IP Address—IPAddress

     Note: If the virtual server uses IPv6, select the IPv6 check box and enter the address in IPv6 format (for example, `1000:0000:0000:0000:0005:0600:700a:888b`).
   - Protocol—serviceType
   - Port—port
4. Click Create, and then click Close. The virtual server you created appears in the Load Balancing Virtual Servers pane.

Binding Services to the Virtual Server

After you have created services and a virtual server, you must bind the services to the virtual server. In most cases, services are bound to virtual servers of the same type, but you can bind certain types of services to certain different types of virtual servers, as shown below.

Virtual Server Type	Service Type	Comment
HTTP	SSL	You would normally bind an SSL service to an HTTP virtual server to do encryption.
SSL	HTTP	You would normally bind an HTTP service to an SSL virtual server to do SSL offloading.
SSL_TCP	TCP	You would normally bind a TCP service to an SSL_TCP virtual server to do SSL offloading for other TCP (SSL decryption without content awareness).

The state of the services bound to a virtual server determines the state of the virtual server: if all of the bound services are DOWN, the virtual server is marked DOWN, and if any of the bound services is UP or OUT OF SERVICE, the state of the virtual server is UP.

To bind a service to a load balancing virtual server by using the command line interface

At the command prompt, type:

bind lb vserver <name> <serviceName>

Example

bind lb vserver Vserver-LB-1 Service-HTTP-1

To bind a service to a load balancing virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.

2. In the details pane, select the virtual server for which you want to bind the service.
3. Click Open.
4. In the Configure Virtual Server (Load Balancing) dialog box, on the Services tab, select the Active check box next to the service that you want to bind to the virtual server.
5. Click OK.

Note: You can bind a service to multiple virtual servers.

Verifying the Configuration

After finishing your basic configuration, you should view the properties of each service and load balancing virtual server in your load balancing setup to verify that each is configured correctly. After the configuration is up and running, you should view the statistics for each service and load balancing virtual server to check for possible problems.

Viewing the Properties of a Server Object

You can view properties such as the name, state, and IP address of any server object in your NetScaler appliance configuration.

To view the properties of server objects by using the command line interface

At the command prompt, type:

show server <serverName>

Example

show server server-1

To view the properties of server objects by using the configuration utility

In the navigation pane, expand Load Balancing, and then click Servers. The parameter values of the available servers appear in the details pane.

Viewing the Properties of a Virtual Server

You can view properties such as the name, state, effective state, IP address, port, protocol, method, and number of bound services for your virtual servers. If you have configured more than the basic load balancing settings, you can view the persistence settings for your virtual servers, any policies that are bound to them, and any cache redirection and content switching virtual servers that have been bound to the virtual servers.

To view the properties of a load balancing virtual server by using the command line interface

At the command prompt, type:

show lb vserver <name>

Example

show lb vserver Vserver-LB-1

To view the properties of a load balancing virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click a virtual server to display its properties at the bottom of the details pane.
3. To view cache redirection and content switching virtual servers that are bound to this virtual server, click Show CS/CR Bindings.

Viewing the Properties of a Service

You can view the name, state, IP address, port, protocol, maximum client connection, maximum requests per connection, and server type of the configured services, and use this information to troubleshoot any mistake in the service configuration.

To view the properties of services by using the command line interface

At the command prompt, type:

show service <name>

Example

show service Service-HTTP-1

To view the properties of services by using the configuration utility

In the navigation pane, expand Load Balancing, and then click Services. The details of the available services appear on the Services pane.

Viewing the Bindings of a Service

You can view the list of virtual servers to which the service is bound. The binding information also provides the name, IP address, port and state of the virtual servers to which the services are bound. You can use the binding information to troubleshoot any problem with binding the services to virtual servers.

To view the bindings of a service by using the command line

At the command prompt, type:

show service bindings <name>

Example

show service bindings Service-HTTP-1

To view the bindings of a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service whose binding information you want to view.
3. Click Show Bindings. The bindings of the service you selected appear in the Binding details for Service: ServiceName dialog box.

Viewing the Statistics of a Virtual Server

To evaluate the performance of virtual servers or to troubleshoot problems, you can display details of the virtual servers configured on the NetScaler appliance. You can display a summary of statistics for all the virtual servers, or you can specify the name of a virtual server to display the statistics only for that virtual server. You can display the following details:

- Name
- IP address
- Port
- Protocol
- State of the virtual server
- Rate of requests received
- Rate of hits

To display virtual server statistics by using the command line interface

To display a summary of the statistics for all the virtual servers currently configured on the NetScaler, or for a single virtual server, at the command prompt, type:

stat lb vserver [-detail] [<name>]

Example

```
>stat lb vserver -detail
Virtual Server(s) Summary
                vsvrIP  port    Protocol      State   Req/s  Hits/s
One                  *    80        HTTP         UP     5/s     0/s
Two                  *     0         TCP       DOWN     0/s     0/s
Three                *  2598         TCP       DOWN     0/s     0/s
dnsVirtualNS  10.102.29.90    53         DNS       DOWN     0/s     0/s
BRVSERV        10.10.1.1    80        HTTP       DOWN     0/s     0/s
LBVIP       10.102.29.66    80        HTTP         UP     0/s     0/s
 Done
```

Parameters for displaying statistics

detail

Include the statistics for hits per second and the total number of hits.

name

Name of the virtual server whose statistics are displayed.

To display virtual server statistics by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. If you want to display the statistics for only one virtual server, in the details pane, select the virtual server whose statistics you want to display.
3. In the details pane, click Statistics.

Viewing the Statistics of a Service

You can view the rate of requests, responses, request bytes, response bytes, current client connections, requests in surge queue, current server connections, and so forth using the service statistics.

To view the statistics of a service by using the command line interface

At the command prompt, type:

stat service <name>

Example

stat service Service-HTTP-1

To view the statistics of a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service whose statistics you want to view (for example, Service-HTTP-1).
3. Click Statistics. The statistics appear in a new window.

Customizing a Load Balancing Configuration

After you configure a basic load balancing setup, you can make a number of modifications to it so that it distributes load exactly as you need. The load balancing feature is complex. You can modify the basic elements by changing the load balancing algorithm, configuring load balancing groups and using them to create your load balancing configuration, configuring persistent client-server connections, configuring the redirection mode, and assigning different weights to different services that have different capacities.

The default load balancing algorithm on the NetScaler appliance is the least connection method, which configures the appliance to send each incoming connection to the service that is currently handling the fewest connections. You can specify different load balancing algorithms, each of which is suited to different conditions.

To accommodate applications such as shopping carts, which require that all requests from the same user be directed to the same server, you can configure the appliance to maintain persistent connections between clients and servers. You can also specify persistence for a group of virtual servers, causing the appliance to direct individual client requests to the same service regardless of which virtual server in the group receives the client request.

You can enable and configure the redirection mode that the appliance uses when redirecting user requests, choosing between IP-based and MAC-based forwarding. You can assign weights to different services, specifying what percentage of incoming load should be directed to each service, so that you can include servers with different capacities in the same load balancing setup without overloading the lower-capacity servers or allowing the higher-capacity servers to sit idle.

Load Balancing Algorithms

The load balancing algorithm defines the criteria that the NetScaler appliance uses to select the service to which to redirect each client request. Different load balancing algorithms use different criteria. For example, the least connection algorithm selects the service with the fewest active connections, while the round robin algorithm maintains a running queue of active services, distributes each connection to the next service in the queue, and then sends that service to the end of the queue.

Some load balancing algorithms are best suited to handling traffic on websites, others to managing traffic to DNS servers, and others to handling complex web applications used in e-commerce or on company LANs or WANs. The following table lists each load balancing algorithm that the NetScaler appliance supports, with a brief description of how each operates.

Name	Server Selection Based On
LEASTCONNECTION	Which service currently has the fewest client connections. This is the default load balancing algorithm.
ROUNDROBIN	Which service is at the top of a list of services. After that service is selected for a connection, it moves to the bottom of the list.
LEASTRESPONSETIME	Which load balanced server currently has the quickest response time.
URLHASH	A hash of the destination URL.
DOMAINHASH	A hash of the destination domain.
DESTINATIONIPHASH	A hash of the destination IP address.
SOURCEIPHASH	A hash of the source IP address.
SRCIPDESTIPHASH	A hash of the source and destination IP addresses.
CALLIDHASH	A hash of the call ID in the SIP header.
SRCIPSRCPORTHASH	A hash of the client's IP address and port.
LEASTBANDWIDTH	Which service currently has the fewest bandwidth constraints.
LEASTPACKETS	Which service currently is receiving the fewest packets.
CUSTOMLOAD	Data from a load monitor.
TOKEN	The configured token.
LRTM	Fewest active connections and the lowest average response time.

Depending on the protocol of the service that it is load balancing, the NetScaler appliance sets up each connection between client and server to last for a different time interval. This

is called load balancing granularity, of which are three types: request-based, connection-based, and time-based granularity. The following table describes each type of granularity and when each is used.

Granularity	Types of Load Balanced Service	Specifies
Request -based	HTTP or HTTPS	A new service is chosen for each HTTP request, independent of TCP connections. As with all HTTP requests, after the Web server fulfills the request, the connection is closed.
Connection-based	TCP and TCP-based protocols other than HTTP	A service is chosen for every new TCP connection. The connection persists until terminated by either the service or the client.
Time-based	UDP and other IP protocols	A new service is chosen for each UDP packet. Upon selection of a service, a session is created between the service and a client for a specified period of time. When the time expires, the session is deleted and a new service is chosen for any additional packets, even if those packets come from the same client.

During startup of a virtual server, or whenever the state of a virtual server changes, the virtual server can initially use the round robin method to distribute the client requests among the physical servers. This type of distribution, referred to as *startup round robin,* helps prevent unnecessary load on a single server as the initial requests are served. After using the round robin method at the startup, the virtual server switches to the load balancing method specified on the virtual server.

The Startup RR Factor works in the following manner:

- If the Startup RR Factor is set to zero, the NetScaler switches to the specified load balancing method depending on the request rate.
- If the Startup RR Factor is any number other than zero, NetScaler uses the round robin method for the specified number of requests before switching to the specified load balancing method.
- By default, the Startup RR Factor is set to zero.

Note: You cannot set the startup RR Factor for an individual virtual server. The value you specify applies to all the virtual servers on the NetScaler appliance.

To set the startup round-robin factor by using the command line interface

At the command prompt, type:

set lb parameter -startupRRFactor <positive_integer>

Example

```
set lb parameter -startupRRFactor 25000
```

Parameter for setting the startup round-robin factor

startupRRFactor

The number of requests for which the virtual server is to apply the round robin load balancing method (slow start mode) before switching to the load balancing method configured on the virtual server. Minimum value: 0, Maximum value: 4294967295. Default: 0.

To set the startup round-robin factor by using the configuration utility

1. In the navigation pane, click Load Balancing.
2. Under Settings, click Configure Load Balancing Parameters.
3. In the Configure Load Balancing Parameters dialog box, for Startup RR Factor type a value.
4. Click OK.

The Least Connection Method

When a virtual server is configured to use the least connection load balancing algorithm (or method), it selects the service with the fewest active connections. This is the default method, because, in most circumstances, it provides the best performance.

For TCP, HTTP, HTTPS, and SSL_TCP services, the NetScaler appliance includes the following connection types in its list of existing connections:

- **Active connections to a service.** Connections representing requests that a client has sent to the virtual server and that the virtual server has forwarded to a service. For HTTP and HTTPS services, active connections represent only those HTTP or HTTPS requests that have not yet received a response.
- **Waiting connections in the surge queue.** Any connections to the virtual server that are waiting in a surge queue and have not yet been forwarded to a service. Connections can build up in the surge queue at any time, for any of the following reasons:
  - Your services have connection limits, and all services in your load balancing configuration are at that limit.
  - The surge protection feature is configured and has been activated by a surge in requests to the virtual server.
  - The load-balanced server has reached an internal limit and therefore does not open any new connections. (For example, an Apache server's connection limit is reached.)

  When a virtual server uses the least connection method, it considers the waiting connections as belonging to the specific service. Therefore, it does not open new connections to those services.

For UDP services, the connections that the least connection algorithm considers include all sessions between the client and a service. These sessions are logical, time-based entities. When the first UDP packet in a session arrives, the NetScaler appliance creates a session between the source IP address and port and the destination IP address and port.

For Real-Time Streaming Protocol (RTSP) connections, the NetScaler appliance uses the number of active control connections to determine the lowest number of connections to an RTSP service.

The following example shows how a virtual server selects a service for load balancing by using the least connection method. Consider the following three services:

- Service-HTTP-1 is handling 3 active transactions.
- Service-HTTP-2 is handling 15 active transactions.
- Service-HTTP-3 is not handling any active transactions.

The following diagram illustrates how the NetScaler appliance forwards incoming requests when using the least connection method.

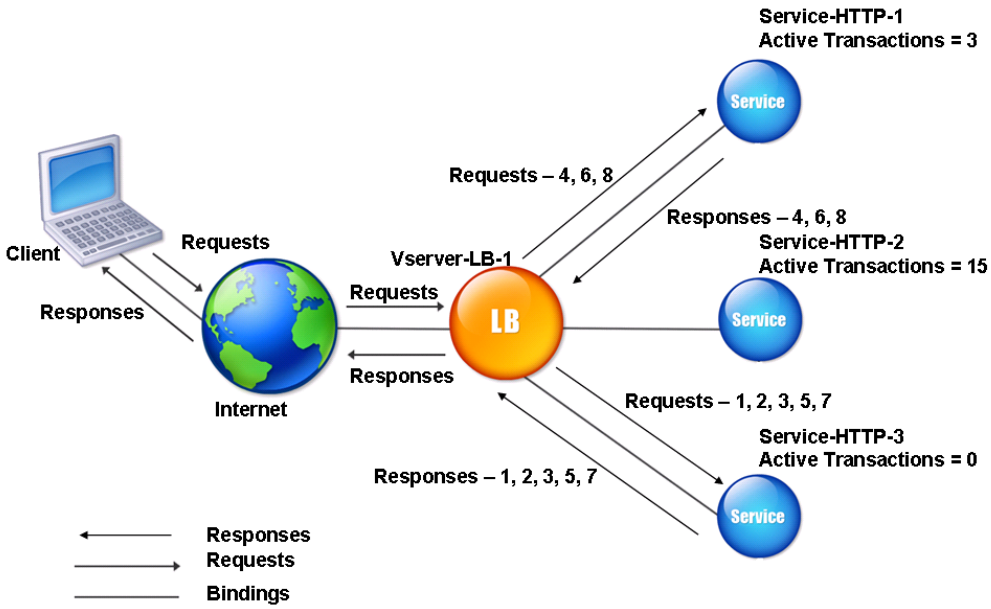


Figure 1. Mechanism of the Least Connections Load Balancing Method

In this diagram, the virtual server selects the service for each incoming connection by choosing the server with the fewest active transactions.

Connections are forwarded as follows:

- Service-HTTP-3 receives the first request, because it is not handling any active transactions.

  Note: The service with no active transaction is selected first.

- Service-HTTP-3 receives the second and third requests because the service has the next least number of active transactions.

- Service-HTTP-1 receives the fourth request Because Service-HTTP-1 and Service-HTTP-3 have same number of active transactions, the virtual server uses the round robin method to choose between them.

- Service-HTTP-3 receives the fifth request.

- Service-HTTP-1 receives the sixth request, and so on, until both Service-HTTP-1 and Service-HTTP-3 are handling the same number of requests as Service-HTTP-2. At that time, the NetScaler appliance starts forwarding requests to Service-HTTP-2 when it is the least loaded service or its turn comes up in the round robin queue.

  Note: If connections to Service-HTTP-2 close, it might get new connections before each of the other two services has 15 active transactions.

The following table explains how connections are distributed in the three-service load balancing setup described above.

Incoming Connection	Service Selected	Current Number of Active Connections	Remarks
Request-1	Service-HTTP-3 (N = 0)	1	Service-HTTP-3 has the fewest active connections.
Request-2	Service-HTTP-3 (N = 1)	2	
Request-3	Service-HTTP-3 (N = 2)	3	
Request-4	Service-HTTP-1 (N = 3)	4	Service-HTTP-1 and Service-HTTP-3 have the same number of active connections.
Request-5	Service-HTTP-3 (N = 3)	4	
Request-6	Service-HTTP-1 (N = 4)	5	
Request-7	Service-HTTP-3 (N = 4)	5	
Request-8	Service-HTTP-1 (N = 5)	6	
Service-HTTP-2 is selected for load balancing when it completes its active transactions and the current connections to it close, or when the other services (Service-HTTP-1 and Service-HTTP-3) have 15 or more connections each.			

The NetScaler appliance can also use the least connection method when weights are assigned to services. It selects a service by using the value (Nw) of the following expression:

*Nw = (Number of active transactions) * (10000 / weight)*

The following example shows how the NetScaler appliance selects a service for load balancing by using the least connection method when weights are assigned to services. In the preceding example, suppose Service-HTTP-1 is assigned a weight of 2, Service-HTTP-2 is assigned a weight of 3, and Service-HTTP-3 is assigned a weight of 4. Connections are forwarded as follows:

- Service-HTTP-3 receives the first because the service is not handling any active transactions.

  Note: If services are not handling any active transactions, the NetScaler appliance uses the round robin method regardless of the weights assigned to each of the services.

- Service-HTTP-3 receives the second, third, fourth, fifth, sixth, and seventh requests because the service has lowest Nw value.

- Service-HTTP-1 receives the eighth request. Because Service-HTTP-1 and Service-HTTP-3 now have same Nw value, the NetScaler performs load balancing in a round robin manner. Therefore, Service-HTTP-3 receives the ninth request.

The following table explains how connections are distributed on the three-service load balancing setup that is described above.

Request Received	Service Selected	Current Nw (Number of active transactions) * (10000 / weight) value	Remarks
Request-1	Service-HTTP-3 (Nw = 0)	Nw = 2500	Service-HTTP-3 has the lowest Nw value.
Request-2	Service-HTTP-3 (Nw = 2500)	Nw = 5000	
Request-3	Service-HTTP-3 (Nw = 5000)	Nw = 7500	
Request-4	Service-HTTP-3 (Nw = 7500)	Nw = 10000	
Request-5	Service-HTTP-3 (Nw = 10000)	Nw = 12500	
Request-6	Service-HTTP-3 (Nw = 12500)	Nw = 15000	
Request-7	Service-HTTP-1 (Nw = 15000)	Nw = 20000	Service-HTTP-1 and Service-HTTP-3 have the same Nw values
Request-8	Service-HTTP-3 (Nw = 15000)	Nw = 17500	
Service-HTTP-2 is selected for load balancing when it completes its active transactions or when the Nw value of other services (Service-HTTP-1 and Service-HTTP-3) is equal to 50000.			

The following diagram illustrates how the NetScaler appliance uses the least connection method when weights are assigned to the services.

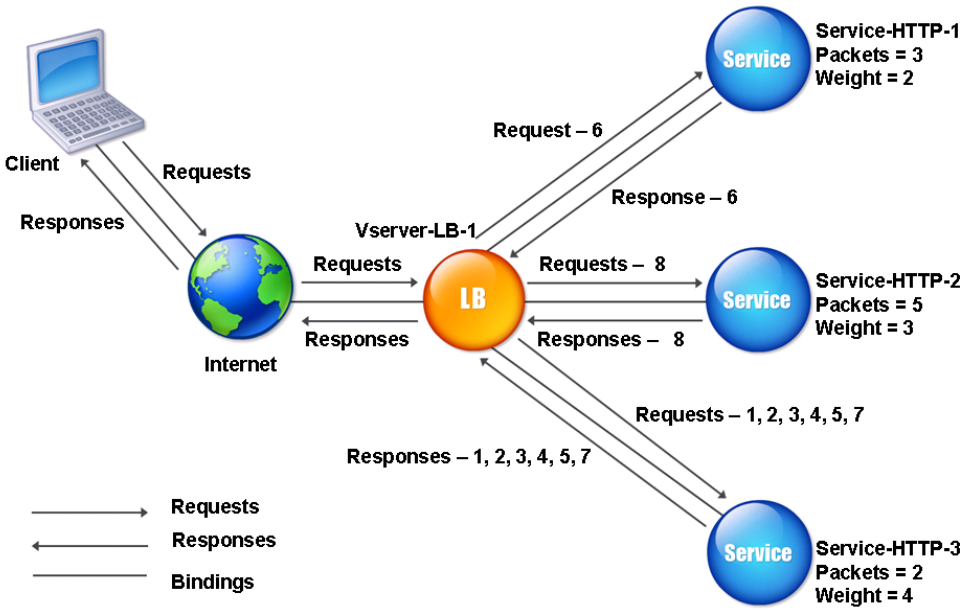


Figure 2. Mechanism of the Least Connections Load Balancing Method when Weights are Assigned

To configure the least connection method, see Configuring a Load Balancing Method that Does Not Include a Policy.

The Round Robin Method

When a load balancing virtual server is configured to use the round robin method, it continuously rotates a list of the services that are bound to it. When the virtual server receives a request, it assigns the connection to the first service in the list, and then moves that service to the bottom of the list.

The following diagram illustrates how the NetScaler appliance uses the round robin method with a load balancing setup that contains three load-balanced servers and their associated services.

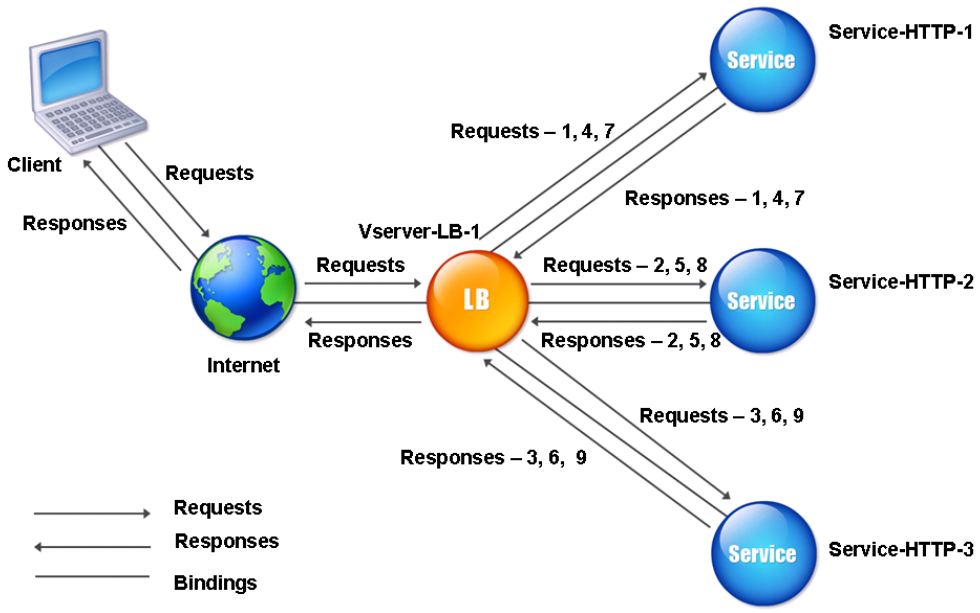


Figure 1. How the Round Robin Load Balancing Method Works

If you assign a different weight to each service, the NetScaler appliance performs weighted round robin distribution of incoming connections. It does this by skipping the lower-weighted services at appropriate intervals.

For example, assume that you have a load balancing setup with three services. You set Service-HTTP-1 to a weight of 2, Service-HTTP-2 to a weight of 3, and Service-HTTP-3 to a weight of 4. The services are bound to Vserver-LB-1, which is configured to use the round robin method. With this setup, incoming requests are delivered as follows:

- Service-HTTP-1 receives the first request.
- Service-HTTP-2 receives the second request.

- Service-HTTP-3 receives the third request.
- Service-HTTP-1 receives the fourth request.
- Service-HTTP-2 receives the fifth request.
- Service-HTTP-3 receives the sixth request.
- Service-HTTP-2 receives the seventh request.
- Service-HTTP-3 receives both the eighth and the ninth requests.

Note: You can also configure weights on services to prevent multiple services from using the same server and overloading the server.

A new cycle then begins, using the same pattern.

The following diagram illustrates the weighted round robin method.

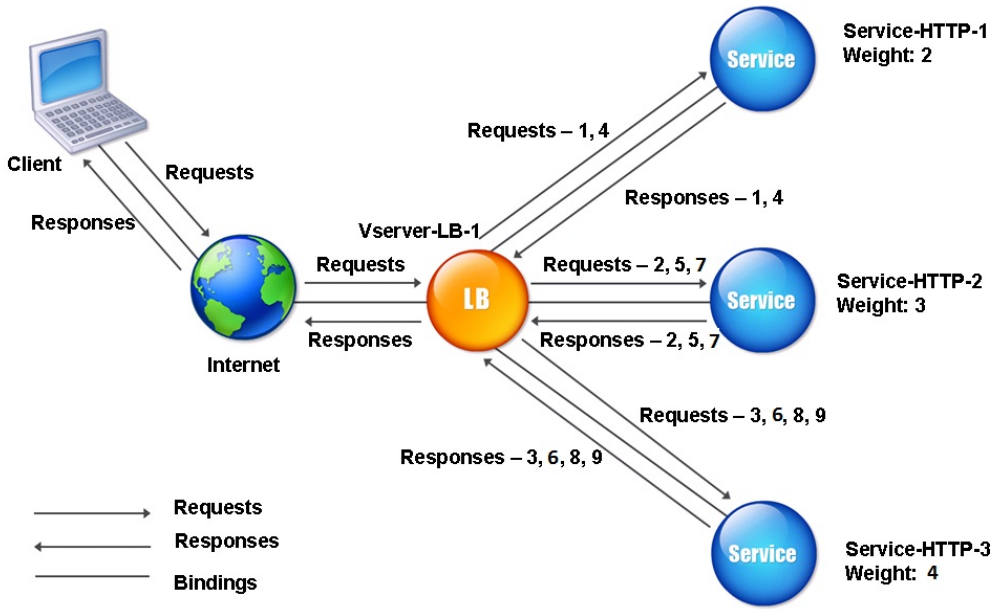


Figure 2. How the Round Robin Load Balancing Method Works with Weighted Services

To configure the round robin method, see Configuring a Load Balancing Method that Does Not Include a Policy.

The Least Response Time Method

When the load balancing virtual server is configured to use the least response time method, it selects the service with the fewest active connections and the lowest average response time. You can configure this method for HTTP and Secure Sockets Layer (SSL) services only. The response time (also called Time to First Byte, or TTFB) is the time interval between sending a request packet to a service and receiving the first response packet from the service. The NetScaler appliance uses response code 200 to calculate TTFB.

The following example shows how a virtual server selects a service for load balancing by using the least response time method. Consider the following three services:

- Service-HTTP-1 is handling three active transactions and TTFB is two seconds.
- Service-HTTP-2 is handling seven active transactions and TTFB is one second.
- Service-HTTP-3 is not handling any active transactions and TTFB is two seconds.

The following diagram illustrates how the NetScaler appliance uses the least response time method to forward the connections.

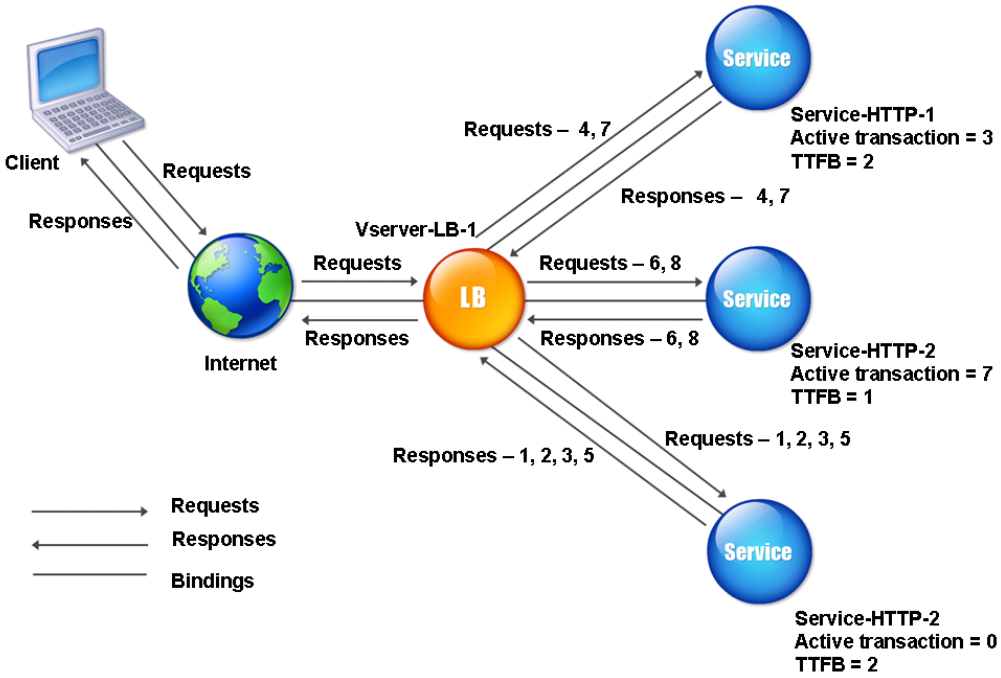


Figure 1. How the Least Response Time Load Balancing Method Works

The virtual server selects a service by multiplying the number of active transactions by the TTFB for each service and then selecting the service with the lowest result. For the example shown above, the virtual server forwards requests as follows:

- Service-HTTP-3 receives the first request, because the service is not handling any active transactions.
- Service-HTTP-3 also receives the second and third requests, because the result is lowest of the three services.
- Service-HTTP-1 receives the fourth request. Since Service-HTTP-1 and Service-HTTP-3 have the same result, the NetScaler appliance chooses between them by applying the Round Robin method.
- Service-HTTP-3 receives the fifth request.
- Service-HTTP-2 receives the sixth request, because at this point it has the lowest result.
- Because Service-HTTP-1, Service-HTTP-2, and Service-HTTP-3 all have the same result at this point, the NetScaler switches to the round robin method, and continues to distribute connections using that method.

The following table explains how connections are distributed in the three-service load balancing setup described above.

Request Received	Service Selected	Current N Value (Number of Active Transactions * TTFB)	Remarks
Request-1	Service-HTTP-3 (N = 0)	N = 2	Service-HTTP-3 has the lowest N value.
Request-2	Service-HTTP-3 (N = 2)	N = 4	
Request-3	Service-HTTP-3 (N = 3)	N = 6	
Request-4	Service-HTTP-1 (N = 6)	N = 8	Service-HTTP-1 and Service-HTTP-3 have the same N values.
Request-5	Service-HTTP-3 (N = 6)	N = 8	
Request-6	Service-HTTP-2 (N = 7)	N = 8	Service-HTTP-2 has the lowest N value.
Request-7	Service-HTTP-1 (N = 8)	N = 15	Service-HTTP-1, Service-HTTP-2, and Service-HTTP-3 have the same N values.
Request-8	Service-HTTP-2 (N = 8)	N = 9	

The virtual server selects a service by using the value (Nw) in the following expression:

*Nw = (N) * (10000 / weight)*

Suppose Service-HTTP-1 is assigned a weight of 2, Service-HTTP-2 is assigned weight of 3, and Service-HTTP-3 is assigned weight of 4.

The NetScaler appliance distributes requests as follows:

- Service-HTTP-3 receives the first request, because it is not handling any active transactions.

  If services are not handling any active transactions, the NetScaler selects them regardless of the weights assigned to them.

- Service-HTTP-3 receives the second, third, fourth, and fifth requests, because this service has the lowest Nw value.

- Service-HTTP-2 receives the sixth request, because this service has the lowest Nw value.

- Service-HTTP-3 receives the seventh request, because this service has the lowest Nw value.

- Service-HTTP-2 receives the eighth request, because this service has the lowest Nw value.

Service-HTTP-1 has the lowest weight and therefore the highest Nw value, so the virtual server does not select it for load balancing.

The following table explains how connections are distributed in the three-service load balancing setup described above.

Request Received	Service Selected	Current Nw Value (Number of Active Transactions) * (10000 / Weight)	Remarks
Request-1	Service-HTTP-3 (Nw = 0)	Nw = 2500	Service-HTTP-3 has the lowest Nw value.
Request-2	Service-HTTP-3 (Nw = 2500	Nw = 5000	
Request-3	Service-HTTP-3 (Nw = 5000)	Nw = 15000	
Request-4	Service-HTTP-3 (Nw = 15000)	Nw = 20000	
Request-5	Service-HTTP-3 (Nw = 20000)	Nw = 25000	

Request-6	Service-HTTP-2 (Nw = 23333.34)	Nw = 26666.67	Service-HTTP-2 has the lowest Nw value.
Request-7	Service-HTTP-3 (Nw = 25000)	Nw= 30000	Service-HTTP-3 has the lowest Nw value.
Request-8	Service-HTTP-2 (Nw = 26666.67)	Nw = 33333.34	Service-HTTP-2 has the lowest Nw value.
Service-HTTP-1 is selected for load balancing when it completes its active transactions or when the Nw values of other services (Service-HTTP-2 and Service-HTTP-3) are equal to 105000.			

The following diagram illustrates how the NetScaler appliance uses the least response time method when weights are assigned.

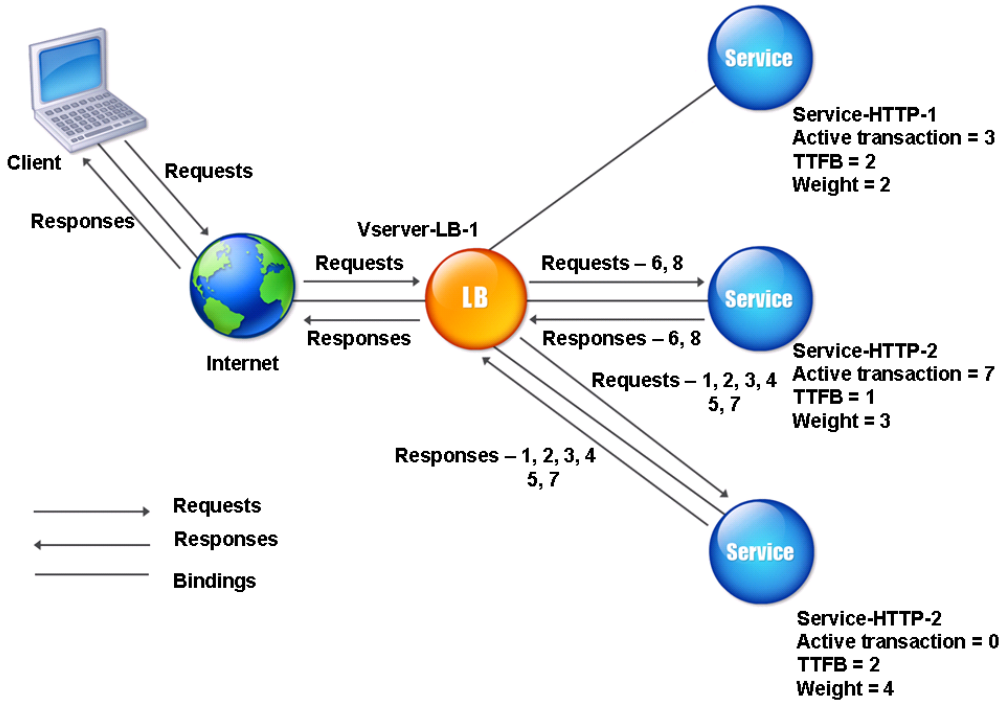


Figure 2. How the Least Response Time Load Balancing Method Works When Weights Are Assigned

To configure the least response time method, see Configuring a Load Balancing Method that Does Not Include a Policy.

When a load balancing virtual server is configured to use the least response time method with monitors, it uses the existing monitoring infrastructure to select the service with the smallest number of active transactions and the fastest average response time. Before you use the least response time method with monitoring, you must bind application-specific monitors to each service and enable least response time method mode on these monitors. The NetScaler appliance then makes load balancing decisions based on the response times it calculates from monitoring probes. For more information about configuring monitors, see

Configuring Monitors in a Load Balancing Setup.

You can use the least response time method with monitors to select non-HTTP and non-HTTPS services. You can also use this method when several monitors are bound to a service. Each monitor determines the response time by using the protocol that it measures for the service that it is bound to. The virtual server then calculates an average response time for that service by averaging the results.

The following table summarizes how response times are calculated for various monitors.

Monitor	Response Time Calculation
PING	Time difference between the ICMP ECHO request and the ICMP ECHO response.
TCP	Time difference between the SYN request and the SYN+ACK response.
HTTP	Time difference between the HTTP request (after the TCP connection is established) and the HTTP response.
TCP-ECV	Time difference between the time the data send string is sent and the data receive string is returned. A tcp-ecv monitor without the send and receive strings is considered to have an incorrect configuration.
HTTP-ECV	Time difference between the HTTP request and the HTTP response.
UDP-ECV	Time difference between the UDP send string and the UDP receive string. A udp-ecv monitor without the receive string is considered to have an incorrect configuration.
DNS	Time difference between a DNS query and the DNS response.
TCPS	Time difference between a SYN request and the SSL handshake completion.
FTP	Time difference between the sending of the user name and the completion of user authentication.
HTTPS (monitors HTTPS requests)	Time difference is same as for the HTTP monitor.
HTTPS-ECV (monitors HTTPS requests)	Time difference is same as for the HTTP-ECV monitor
USER	Time difference between the time when a request is sent to the dispatcher and the time when the dispatcher response is received.

The following example shows how the NetScaler appliance selects a service for load balancing by using the least response time method with monitors. Consider the following three services:

- Service-HTTP-1 is handling 3 active transactions and the response time is five seconds.
- Service-HTTP-2 is handling 7 active transactions and the response time is one second.
- Service-HTTP-3 is not handling any active transactions and the response time is two seconds.

The following diagram illustrates the process that the NetScaler appliance follows when it forwards requests.

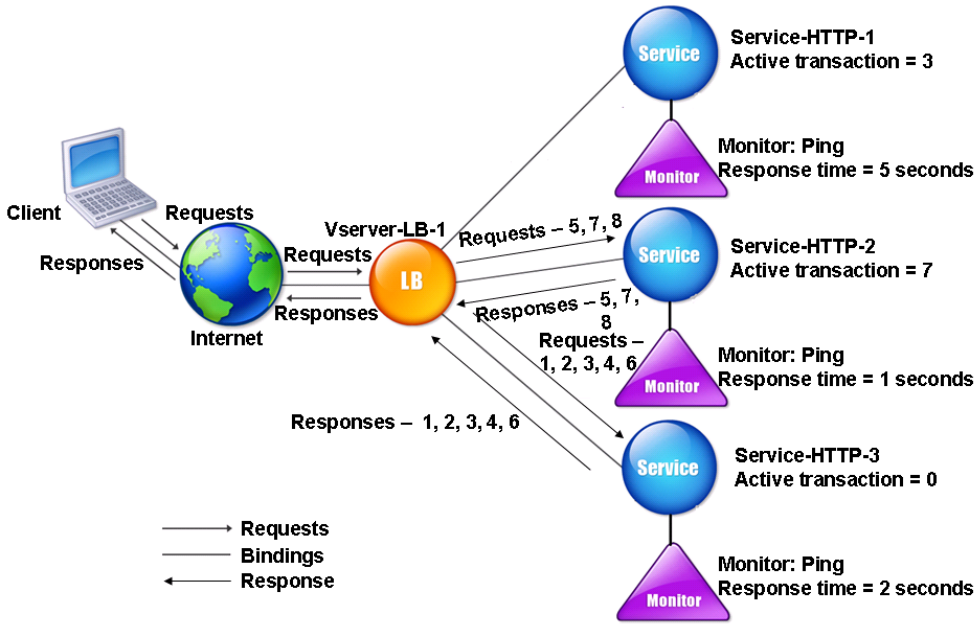


Figure 3. How the Least Response Time Load Balancing Method Works When Using Monitors

The virtual server selects a service by using the value (N) in the following expression:

*N = Number of active transactions * Response time that is determined by the monitor*

The virtual server delivers requests as follows:

- Service-HTTP-3 receives the first request, because this service is not handling any active transaction.
- Service-HTTP-3 receives the second, third, and fourth requests, because this service has the lowest N value.
- Service-HTTP-2 receives the fifth request, because this service has the lowest N value.

- Since both Service-HTTP-2 and Service-HTTP-3 currently have the same N value, the NetScaler appliance switches to the round robin method Therefore, Service-HTTP-3 receives the sixth request.

- Service-HTTP-2 receives the seventh and eighth requests, because this service has the lowest N value.

Service-HTTP-1 is not considered for load balancing, because it is more heavily loaded (has the highest N value) when compared to the other two services. However, if Service-HTTP-1 completes its active transactions, the NetScaler appliance again considers that service for load balancing.

The following table summarizes how N is calculated for the services.

Request Received	Service Selected	Current N Value (Number of Active Transactions)	Remarks
Request-1	Service-HTTP-3 (N = 0)	N = 2	Service-HTTP-3 has the lowest N value.
Request-2	Service-HTTP-3 (N = 2)	N = 4	
Request-3	Service-HTTP-3 (N = 4)	N = 6	
Request-4	Service-HTTP-3 (N = 6)	N = 8	
Request-5	Service-HTTP-2 (N = 7)	N = 8	Service-HTTP-1 and Service-HTTP-3 have the same N values.
Request-6	Service-HTTP-3 (N = 8)	N = 10	
Request-7	Service-HTTP-2 (N = 8)	N = 9	Service-HTTP-2 has the lowest N value.
Request-8	Service-HTTP-1 (N = 9)	N = 10	
Service-HTTP-1 is again selected for load balancing when it completes its active transactions or when the N value of the other services (Service-HTTP-2 and Service-HTTP-3) is equal to 15.			

The NetScaler appliance also performs load balancing by using the number of active transactions, response time, and weights if different weights are assigned to services. The NetScaler appliance selects the service by using the value (Nw) in the following expression:

*Nw = (N) * (10000 / weight)*

As in the preceding example, suppose Service-HTTP-1 is assigned a weight of 2, Service-HTTP-2 is assigned a weight of 3, and Service-HTTP-3 is assigned a weight of 4.

The NetScaler appliance delivers requests as follows:

- Service-HTTP-3 receives the first request, because it is not handling any active transactions.
- Service-HTTP-3 receives the second, third, and fourth requests, because this service has the lowest Nw value.
- Service-HTTP-2 receives the fifth request, because this service has the lowest Nw value.
- Service-HTTP-3 receives the sixth request, because this service has the lowest Nw value.
- Service-HTTP-2 receives the seventh and the eighth requests, because this service has the lowest Nw value.

Service-HTTP-1 has the lowest weight and the highest Nw value, so the NetScaler appliance does not select it for load balancing.

The following table summarizes how Nw is calculated for various monitors.

Request Received	Service Selected	Current Nw Value (Number of Active Transactions) * (10000 / Weight)	Remarks
Request-1	Service-HTTP-3 (Nw = 0)	Nw = 5000	Service-HTTP-3 has the lowest Nw value.
Request-2	Service-HTTP-3 (Nw = 5000	Nw = 10000	
Request-3	Service-HTTP-3 (Nw = 15000)	Nw = 20000	
Request-4	Service-HTTP-3 (Nw = 20000)	Nw = 25000	
Request-5	Service-HTTP-2 (Nw = 23333.34)	Nw = 26666.67	Service-HTTP-2 has the lowest Nw value.
Request-6	Service-HTTP-3 (Nw = 25000)	Nw = 30000	Service-HTTP-3 has the lowest Nw value.
Request-7	Service-HTTP-2 (Nw = 23333.34)	Nw= 26666.67	Service-HTTP-2 has the lowest Nw value.

Request-8	Service-HTTP-2 (Nw =25000)	Nw = 30000	Service-HTTP-2 has the lowest Nw value.
Service-HTTP-1 is selected for load balancing when it completes its active transactions or when the Nw value of the other services (Service-HTTP-2 and Service-HTTP-3) is equal to 75000.			

The following diagram illustrates how the virtual server uses the least response time method when weights are assigned.

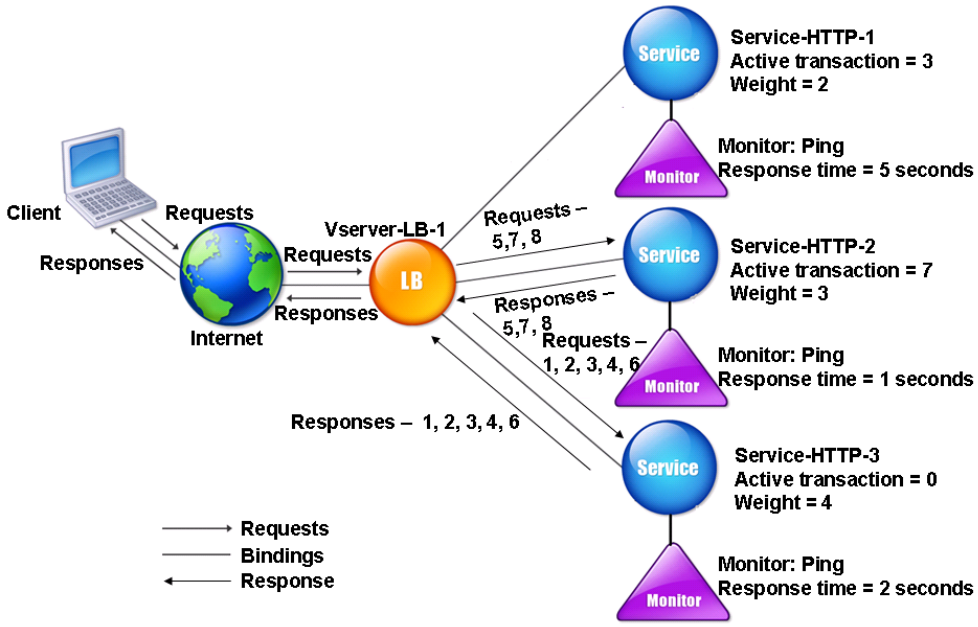


Figure 4. How the Least Response Time Load Balancing Method with Monitors Works When Weights Are Assigned

To configure the least response time method using monitors, see Configuring a Load Balancing Method that Does Not Include a Policy.

About Hashing Methods

Load balancing methods based on hashes of certain connection information or header information constitute the majority of the NetScaler appliance's load balancing methods. Hashes are shorter and easier to use than the information that they are based on, while retaining enough information to ensure that no two different pieces of information generate the same hash and are therefore confused with one another.

You can use the hashing load balancing methods in an environment where a cache serves a wide range of content from the Internet or specified origin servers. Caching requests reduces request and response latency, and ensures better resource (CPU) utilization, making caching popular on heavily used Web sites and application servers. Since these sites also benefit from load balancing, hashing load balancing methods are widely useful.

The NetScaler provides the following hashing methods:

- URL hash method
- Domain hash method
- Destination IP hash method
- Source IP hash method
- Source IP Destination IP hash method
- Source IP Source Port hash method
- Call ID hash method
- Token method

These hashing algorithms ensure minimal disruption when services are added to or deleted from your load balancing setup. Most of them calculate two hash values:

- A hash of the service's IP address and port.
- A hash of the incoming URL, the domain name, the source IP address, the destination IP address, or the source and destination IP addresses, depending on the configured hash method.

The NetScaler appliance then generates a new hash value by using both of those hash values. Finally, it forwards the request to the service with highest hash value. As the appliance computes a hash value for each request and selects the service that will process the request, it populates a cache. Subsequent requests with the same hash value are sent to the same service. The following flow chart illustrates this process.

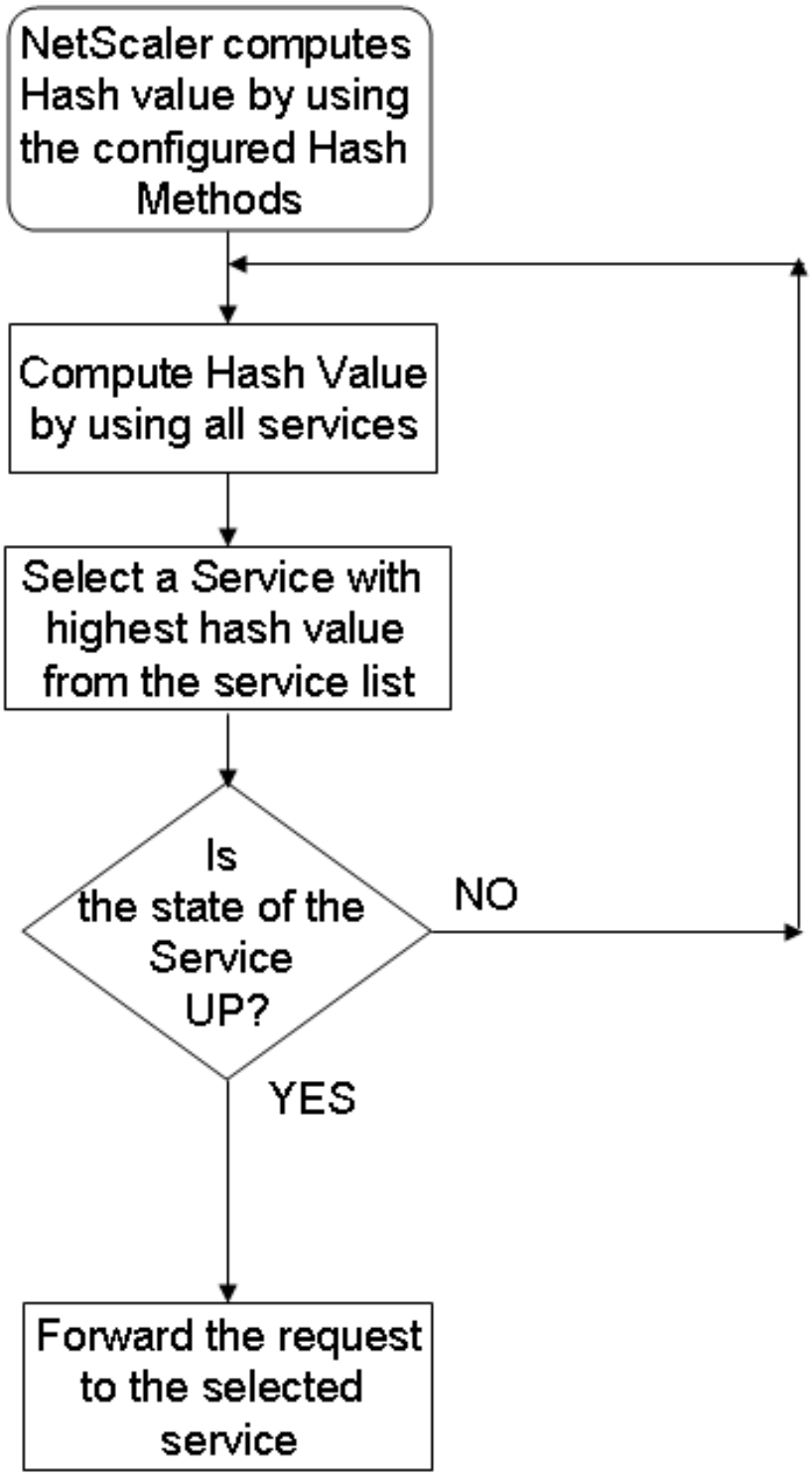


Figure 1. How the Hashing Methods Distribute Requests

Hashing methods can be applied to IPv4 and IPv6 addresses.

Consider a scenario where three services (Service-HTTP-1, Service-HTTP-2, and Service-HTTP-3) are bound to a virtual server, any hash method is configured, and the hash value is Hash1. When the configured services are UP, the request is sent to Service-HTTP-1. If Service-HTTP-1 is down, the NetScaler appliance calculates the hash value for the last log

of the number of services. The NetScaler then selects the service with the highest hash value, such as Service-HTTP-2. The following diagram illustrates this process.

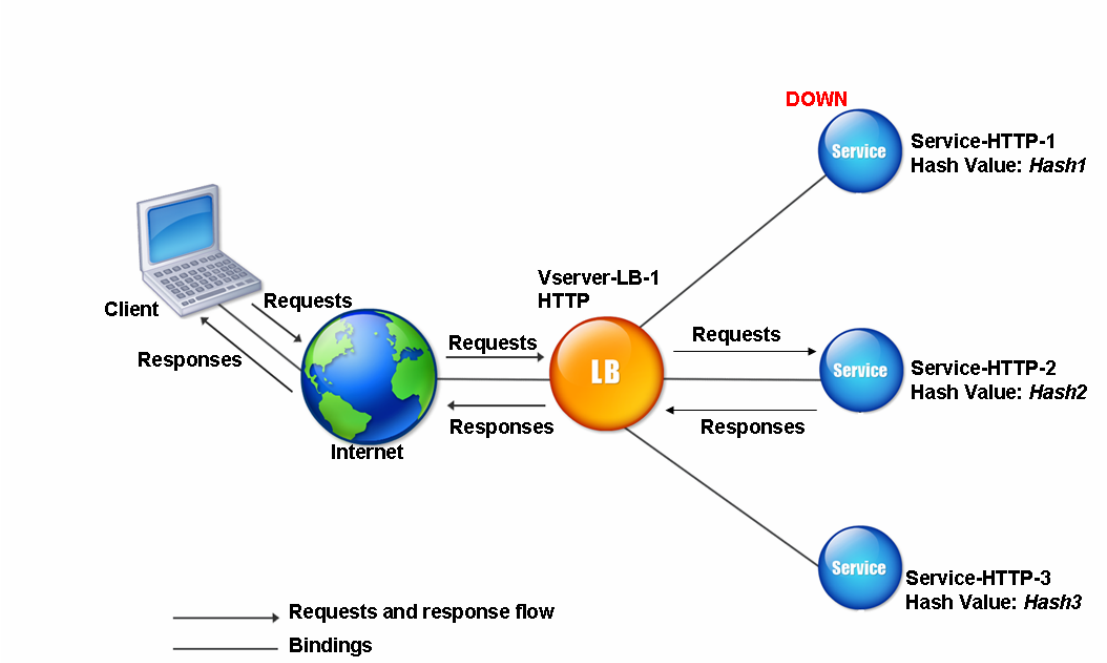


Figure 2. Entity Model for Hashing Methods

Note: If the NetScaler appliance fails to select a service by using a hashing method, it defaults to the least connection method to select a service for the incoming request. You should adjust server pools by removing services during periods of low traffic to enable the caches to repopulate without affecting performance on your load balancing setup.

The URL Hash Method

When you configure the NetScaler appliance to use the URL hash method for load balancing the services, for selecting a service, the NetScaler generates a hash value of the HTTP URL present in the incoming request. If the service selected by the hash value is DOWN, the algorithm has a method to select another service from the list of active services. The NetScaler caches the hashed value of the URL, and when it receives subsequent requests that use the same URL, it forwards them to the same service. If the NetScaler cannot parse an incoming request, it uses the round robin method for load balancing instead of the URL hash method.

For generating the hash value, NetScaler uses a specific algorithm and considers a part of the URL. By default, the NetScaler considers the first 80 bytes of the URL. If the URL is of less than 80 bytes, the complete URL is used. You can specify a different length. The hash length can be from 1 to 4096 bytes. Generally, if long URLs are used where only a small number of characters are different, it is a good idea to make the hash length as high as possible to try to ensure a more even load distribution.

Consider a scenario where three services, Service-HTTP-1, Service-HTTP-2, and Service-HTTP-3, are bound to a virtual server, and the load balancing method configured on the virtual server is the URL hash method. The virtual server receives a request and the hash value of the URL is U1. NetScaler selects Service-HTTP-1. If Service-HTTP-1 is DOWN, the NetScaler selects Service-HTTP-2.

The following diagram illustrates this process.

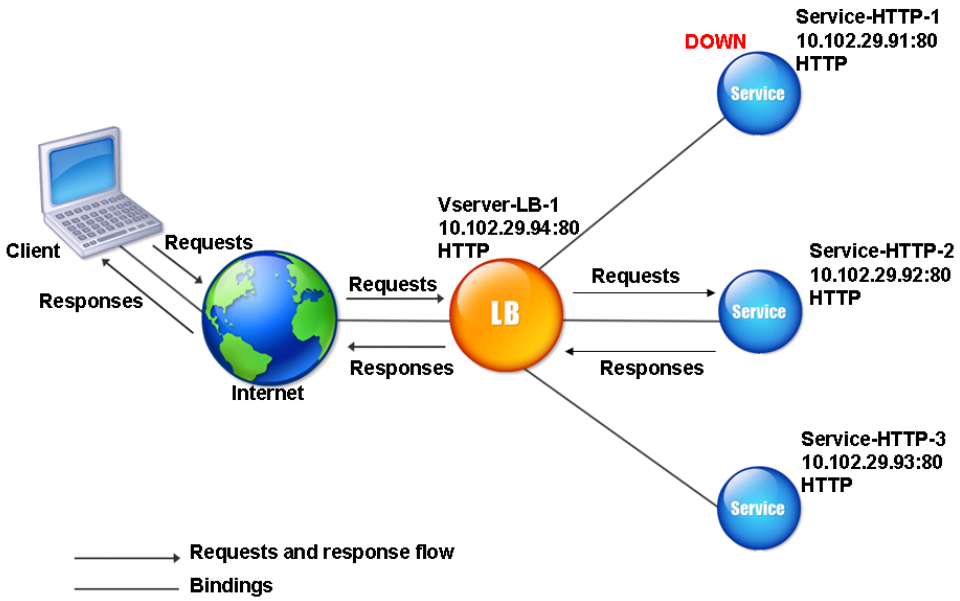


Figure 1. How URL Hashing Operates

If both Service-HTTP-1 and Service-HTTP-2 are DOWN, NetScaler sends requests with hash value U1 to Service-HTTP-3.

If Service-HTTP-1 and Service-HTTP-2 are down, requests that generate the hash URL1 are sent to Service-HTTP-3. If these services are UP, requests that generate the hash URL1 are distributed in the following manner:

- If the Service-HTTP-2 is up, the request is sent to Service-HTTP-2.
- If the Service-HTTP-1 is up, the request is sent to Service-HTTP-1.
- If Service-HTTP-1 and Service-HTTP-2 are up at the same time, the request is sent to Service-HTTP-1.

To configure the URL hash method, see Configuring a Load Balancing Method that Does Not Include a Policy. Select the load balancing method as URL Hash, and set the hash length to the number of bytes to be used for generating the hash value.

The Domain Hash Method

A load balancing virtual server configured to use the domain hash method uses the hashed value of the domain name in the HTTP request to select a service. The domain name is taken from either the incoming URL or the Host header of the HTTP request. If the domain name appears in both the URL and the Host header, the NetScaler gives preference to the URL.

If you configure domain name hashing, and an incoming HTTP request does not contain a domain name, the NetScaler appliance defaults to the round robin method for that request.

The hash-value calculation uses the name length or hash length value, whichever is smaller. By default, the NetScaler appliance calculates the hash value from the first 80 bytes of the domain name. To specify a different number of bytes in the domain name when calculating the hash value, you can set the hashLength parameter (Hash Length in the configuration utility) to a value of from 1 to 4096 (bytes).

To configure the domain hash method, see Configuring a Load Balancing Method that Does Not Include a Policy.

The Destination IP Hash Method

A load balancing virtual server configured to use the destination IP hash method uses the hashed value of the destination IP address to select a server. You can mask the destination IP address to specify which part of it to use in the hash value calculation, so that requests that are from different networks but destined for the same subnet are all directed to the same server. This method supports IPv4 and IPv6-based destination servers.

This load balancing method is appropriate for use with the cache redirection feature.

To configure the destination IP hash method for an IPv4 destination server, you set the netMask parameter. To configure this method for an IPv6 destination server, you use the v6NetMaskLen parameter. In the configuration utility, text boxes for setting these parameters appear when you select the Destination IP Hash method.

To configure the destination IP hash method, see Configuring a Load Balancing Method that Does Not Include a Policy.

The Source IP Hash Method

A load balancing virtual server configured to use the source IP hash method uses the hashed value of the client IPv4 or IPv6 address to select a service. To direct all requests from source IP addresses that belong to a particular network to a specific destination server, you must mask the source IP address. For IPv4 addresses, use the netMask parameter. For IPv6 addresses, use the v6NetMaskLength parameter.

To configure the source IP hash method, see Configuring a Load Balancing Method that Does Not Include a Policy.

The Source IP Destination IP Hash Method

A load balancing virtual server configured to use the source IP destination IP hash method uses the hashed value of the source and destination IP addresses (either IPv4 or IPv6) to select a service. Hashing is symmetric; the hash-value is the same regardless of the order of the source and destination IPs. This ensures that all packets flowing from a particular client to the same destination are directed to the same server.

To direct all requests that belong to a particular network to a specific destination server, you must mask the source IP address. For IPv4 addresses, use the netMask parameter. For IPv6 addresses, use the v6NetMaskLength parameter.

To configure the source IP destination IP hash method, see Configuring a Load Balancing Method that Does Not Include a Policy.

The Source IP Source Port Hash Method

A load balancing virtual server configured to use the source IP source port hash method uses the hash value of the source IP (either IPv4 or IPv6) and source port to select a service. This ensures that all packets on a particular connection are directed to the same service.

This method is used in connection mirroring and firewall load balancing. For more information about connection mirroring, see Connection Failover.

To direct all requests that belong to a particular network to a specific destination server, you must mask the source IP address. For IPv4 addresses, use the netMask parameter. For IPv6 addresses, use the v6NetMaskLength parameter.

To configure the source IP source port hash method, see Configuring a Load Balancing Method that Does Not Include a Policy.

The Call ID Hash Method

A load balancing virtual server configured to use the call ID hash method uses the hash value of the call ID in the SIP header to select a service. Packets for a particular SIP session are therefore always directed to the same proxy server.

This method is applicable to SIP load balancing. For more information about SIP load balancing, see Monitoring SIP Services.

To configure the call ID hash method, see Configuring a Load Balancing Method that Does Not Include a Policy.

The Least Bandwidth Method

A load balancing virtual server configured to use the least bandwidth method selects the service that is currently serving the least amount of traffic, measured in megabits per second (Mbps). The following example shows how the virtual server selects a service for load balancing by using the least bandwidth method.

Consider three services, Service-HTTP-1, Service-HTTP-2, and Service-HTTP-3.

- Service-HTTP-1 has 3 Mbps bandwidth.
- Service-HTTP-2 has 5 Mbps bandwidth.
- Service-HTTP-3 has 2 Mbps bandwidth.

The following diagram illustrates how the virtual server uses the least bandwidth method to forward requests to the three services.

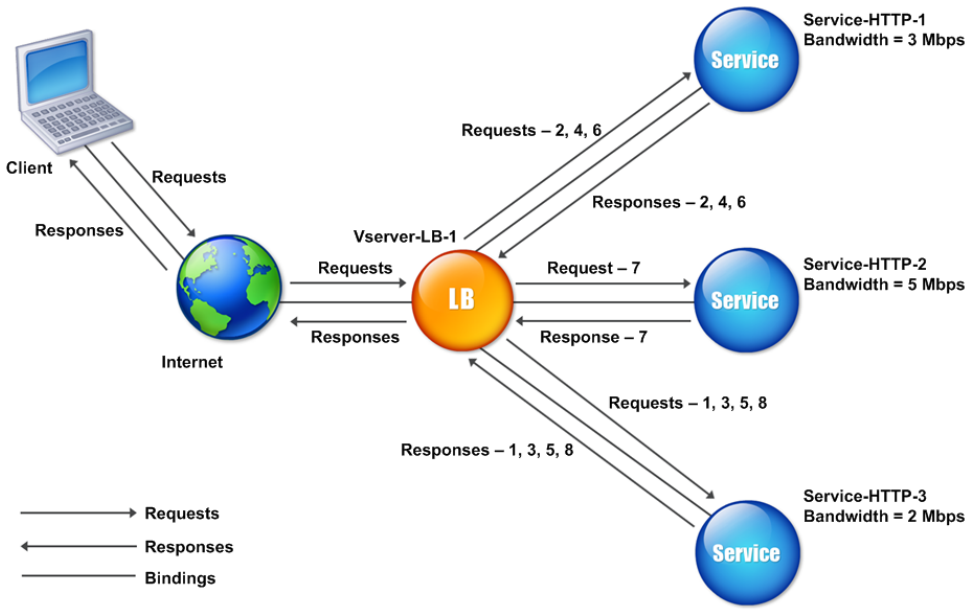


Figure 1. How the Least Bandwidth Load Balancing Method Works

The virtual server selects the service by using the bandwidth value (N), which is the sum of the number of bytes transmitted and received over the previous 14 seconds. If each request requires 1 Mbps bandwidth, the NetScaler appliance delivers requests as follows:

- Service-HTTP-3 receives the first request, because this service has the lowest N value.

- Since Service-HTTP-1 and Service-HTTP-3 now have same N value, the virtual server switches to the round robin method for these servers, alternating between them. Service-HTTP-1 receives the second request, Service-HTTP-3 receives the third request, Service-HTTP-1 receives the fourth request, Service-HTTP-3 receives the fifth request, and Service-HTTP-1 receives the sixth request.

- Since Service-HTTP-1, Service-HTTP-2, and Service-HTTP-3 now all have same N value, the virtual server includes Service-HTTP-2 in the round robin list. Therefore, Service-HTTP-2 receives the seventh request, Service-HTTP-3 receives the eighth request, and so on.

The following table summarizes how N is calculated.

Request Received	Service Selected	Current N Value	Remarks
Request-1	Service-HTTP-3 (N = 2)	N = 3	Service-HTTP-3 has the lowest N value.
Request-2	Service-HTTP-1 (N = 3)	N = 4	Service-HTTP-1 and Service-HTTP-3 have the same N values.
Request-3	Service-HTTP-3 (N = 3)	N = 4	
Request-4	Service-HTTP-1 (N = 4)	N = 5	
Request-5	Service-HTTP-3 (N = 4)	N = 5	
Request-6	Service-HTTP-1 (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2, and Service-HTTP-3 have the same N values.
Request-7	Service-HTTP-2 (N = 5)	N = 6	
Request-8	Service-HTTP-3 (N = 5)	N = 6	

Note: If you enable the RTSP NAT option on the virtual server, the NetScaler appliance uses the number of data and control bytes exchanged to determine the bandwidth usage for RTSP services. For more information about RTSP NAT option, see Managing RTSP Connections.

The NetScaler appliance also performs load balancing by using the bandwidth and weights if different weights are assigned to the services. It selects a service by using the value (Nw) in the following expression:

*Nw = (N) * (10000 / weight)*

As in the preceding example, suppose Service-HTTP-1 is assigned a weight of 2, Service-HTTP-2 is assigned a weight of 3, and Service-HTTP-3 is assigned a weight of 4. The

NetScaler appliance delivers requests as follows:

- Service-HTTP-3 receives the first second, third, fourth, and fifth requests, because this service has the lowest Nw value.
- Service-HTTP-1 receives the sixth request, because this service has the lowest Nw value.
- Service-HTTP-3 receives the seventh request, because this service has the lowest Nw value.
- Service-HTTP-2 receives the eighth request, because this service has the lowest Nw value.

The following table summarizes how Nw is calculated.

Request Received	Service Selected	Current Nw Value (Number of Active Transactions) * (10000 / Weight)	Remarks
Request-1	Service-HTTP-3 (Nw = 5000)	Nw = 5000	Service-HTTP-3 has the lowest Nw value.
Request-2	Service-HTTP-3 (Nw = 5000)	Nw = 7500	
Request-3	Service-HTTP-3 (Nw = 7500)	Nw = 10000	
Request-4	Service-HTTP-3 (Nw = 10000)	Nw = 12500	
Request-5	Service-HTTP-3 (Nw = 12500)	Nw = 15000	
Request-6	Service-HTTP-1 (Nw = 15000)	Nw = 20000	Service-HTTP-1 and Service-HTTP-3 have the same Nw value.
Request-7	Service-HTTP-3 (Nw = 15000)	Nw = 17500	
Request-8	Service-HTTP-2 (Nw = 16666.67)	Nw = 20000	Service-HTTP-2 has the lowest Nw value.

The following diagram illustrates how the virtual server uses the least bandwidth method when weights are assigned to the services.

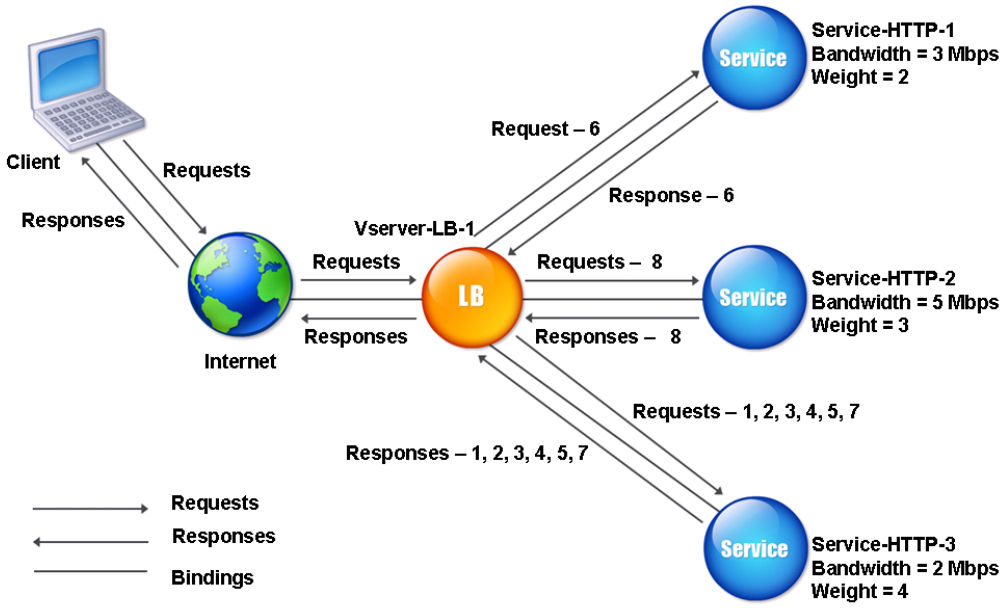


Figure 2. How the Least Bandwidth Load Balancing Method Works When Weights Are Assigned

To configure the least bandwidth method, see Configuring a Load Balancing Method that Does Not Include a Policy.

The Least Packets Method

A load balancing virtual server configured to use the least packets method selects the service that has received the fewest packets in the last 14 seconds.

For example, consider three services, Service-HTTP-1, Service-HTTP-2, and Service-HTTP-3.

- Service-HTTP-1 has handled three packets in last 14 seconds.
- Service-HTTP-2 has handled five packets in last 14 seconds.
- Service-HTTP-3 has handled two packets in last 14 seconds.

The following diagram illustrates how the NetScaler appliance uses the least packets method to choose a service for each request that it receives.

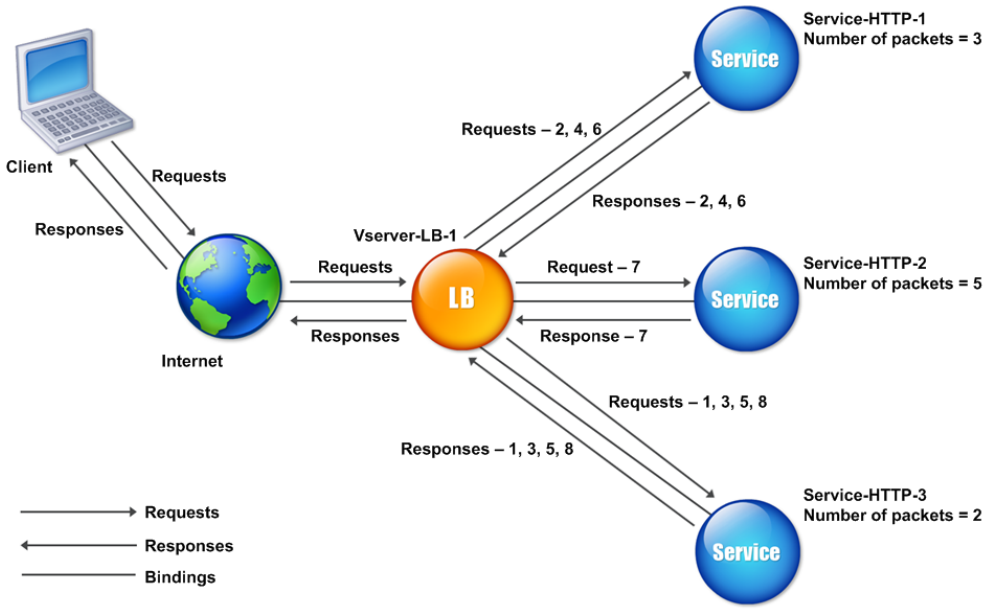


Figure 1. How the Least Packets Load Balancing Method Works

The NetScaler appliance selects a service by using the number of packets (N) transmitted and received by each service in the last 14 seconds. Using this method, it delivers requests as follows:

- Service-HTTP-3 receives the first request, because this service has the lowest N value.
- Since Service-HTTP-1 and Service-HTTP-3 now have the same N value, the virtual server switches to the round robin method. Service-HTTP-1 therefore receives the second

request, Service-HTTP-3 receives the third request, Service-HTTP-1 receives the fourth request, Service-HTTP-3 receives the fifth request, and Service-HTTP-1 receives the sixth request.

- Since Service-HTTP-1, Service-HTTP-2, and Service-HTTP-3 all now have same N value, the virtual server switches to the round robin method for Service-HTTP-2 as well, including it in the round robin list. Therefore, Service-HTTP-2 receives the seventh request, Service-HTTP-3 receives the eighth request, and so on.

The following table summarizes how N is calculated.

Request Received	Service Selected	Current N Value	Remarks
Request-1	Service-HTTP-3 (N = 2)	N = 3	Service-HTTP-3 has the lowest N value.
Request-2	Service-HTTP-1 (N = 3)	N = 4	Service-HTTP-1 and Service-HTTP-3 have the same N values.
Request-3	Service-HTTP-3 (N = 3)	N = 4	
Request-4	Service-HTTP-1 (N = 4)	N = 5	
Request-5	Service-HTTP-3 (N = 4)	N = 5	
Request-6	Service-HTTP-1 (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2, and Service-HTTP-3 have the same N values.
Request-7	Service-HTTP-2 (N = 5)	N = 6	
Request-8	Service-HTTP-3 (N = 5)	N = 6	

Note: If you enable the RTSP NAT option on the virtual server, the NetScaler uses the number of data and control packets to calculate the number of packets for RTSP services. For more information about RTSP NAT option, see Managing RTSP Connections.

The NetScaler appliance also performs load balancing by using the number of packets and weights when a different weight is assigned to each service. It selects a service by using the value (Nw) in the following expression:

*Nw = (N) * (10000 / weight)*

As in the preceding example, suppose Service-HTTP-1 is assigned a weight of 2, Service-HTTP-2 is assigned a weight of 3, and Service-HTTP-3 is assigned a weight of 4. The NetScaler appliance delivers requests as follows:

- Service-HTTP-3 receives the first second, third, fourth, and fifth requests, because this service has the lowest Nw value.
- Service-HTTP-1 receives the sixth request, because this service has the lowest Nw value.
- Service-HTTP-3 receives the seventh request, because this service has the lowest Nw value.
- Service-HTTP-2 receives the eighth request, because this service has the lowest Nw value.

The following table summarizes how Nw is calculated.

Request Received	Service Selected	Current Nw Value (Number of Active Transactions) * (10000 / weight)	Remarks
Request-1	Service-HTTP-3 (Nw = 5000)	Nw = 5000	Service-HTTP-3 has the lowest Nw value.
Request-2	Service-HTTP-3 (Nw = 5000)	Nw = 7500	
Request-3	Service-HTTP-3 (Nw = 7500)	Nw = 10000	
Request-4	Service-HTTP-3 (Nw = 10000)	Nw = 12500	
Request-5	Service-HTTP-3 (Nw = 12500)	Nw = 15000	
Request-6	Service-HTTP-1 (Nw = 15000)	Nw = 20000	Service-HTTP-1 and Service-HTTP-3 have the same Nw value.
Request-7	Service-HTTP-3 (Nw = 15000)	Nw = 17500	
Request-8	Service-HTTP-2 (Nw = 16666.67)	Nw = 20000	Service-HTTP-2 has the lowest Nw value.

The following diagram illustrates how the virtual server uses the least packets method when weights are assigned.

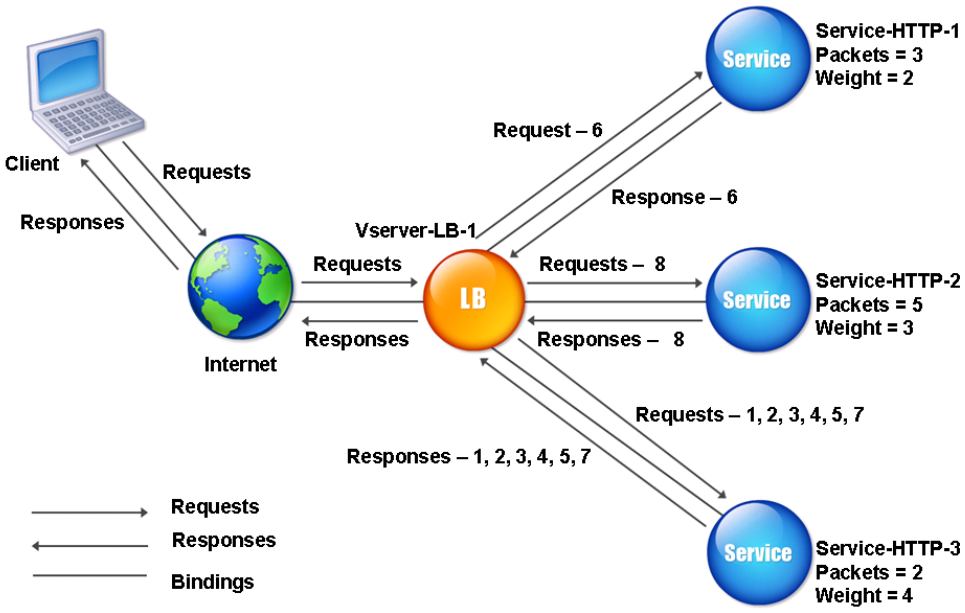


Figure 2. How the Least Packets Method Works When Weights Are Assigned

To configure the least packets method, see Configuring a Load Balancing Method that Does Not Include a Policy.

The Custom Load Method

Custom load balancing is performed on server parameters such as CPU usage, memory, and response time. When using the custom load method, the NetScaler appliance usually selects a service that is not handling any active transactions. If all of the services in the load balancing setup are handling active transactions, the appliance selects the service with the smallest load. A special type of monitor, known as a load monitor, calculates the load on each service in the network. The load monitors do not mark the state of a service, but they do take services out of the load balancing decision when those services are not UP.

For more information about load monitors, see Understanding Load Monitors. The following diagram illustrates how a load monitor operates.

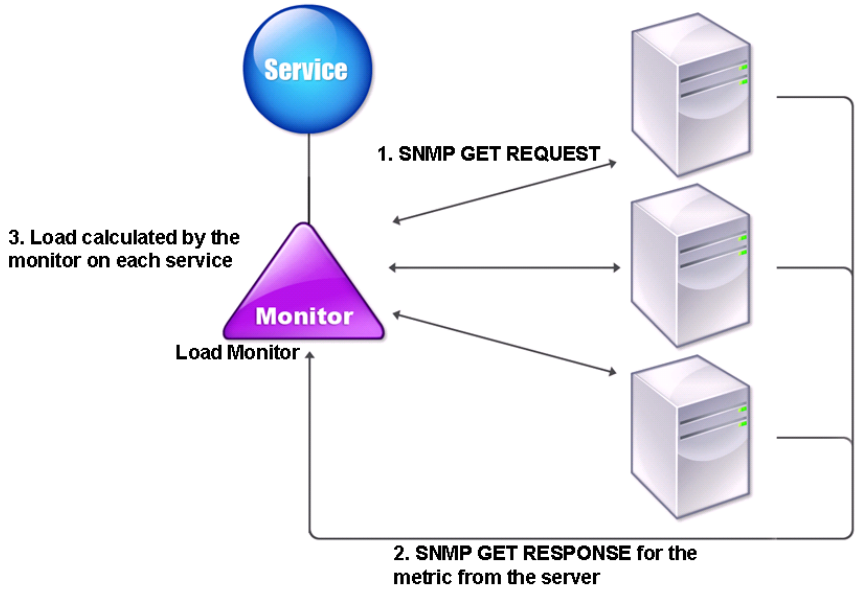


Figure 1. How Load Monitors Operate

The load monitor uses Simple Network Management Protocol (SNMP) probes to calculate load on each service by sending an SNMP GET request to the service. This request contains one or more object IDs (OIDs). The service responds with an SNMP GET response, with metrics corresponding to the SNMP OIDs. The load monitor uses the response metrics, described below, to calculate the load on the service.

The load monitor calculates the load on a service by using the following parameters:

- Metrics values retrieved through SNMP probes that exist as tables in the NetScaler.
- Threshold value set for each metric.

- Weight assigned to each metric.

For example, consider three services, Service-HTTP-1, Service-HTTP-2, and Service-HTTP-3.

- Service-HTTP-1 is using 20 megabytes (MB) of memory.
- Service-HTTP-2 is using 70 MB of memory.
- Service-HTTP-3 is using 80 MB of memory.

The load balanced servers can export metrics such as CPU and memory usage to the services, which can in turn provide them to the load monitor. The load monitor sends an SNMP GET request containing the OIDs 1.3.6.1.4.1.5951.4.1.1.41.1.5, 1.3.6.1.4.1.5951.4.1.1.41.1.4, and 1.3.6.1.4.1.5951.4.1.1.41.1.3 to the services. The three services respond to the request. The NetScaler appliance compares the exported metrics, and then selects Service-HTTP-1 because it has more available memory. The following diagram illustrates this process.

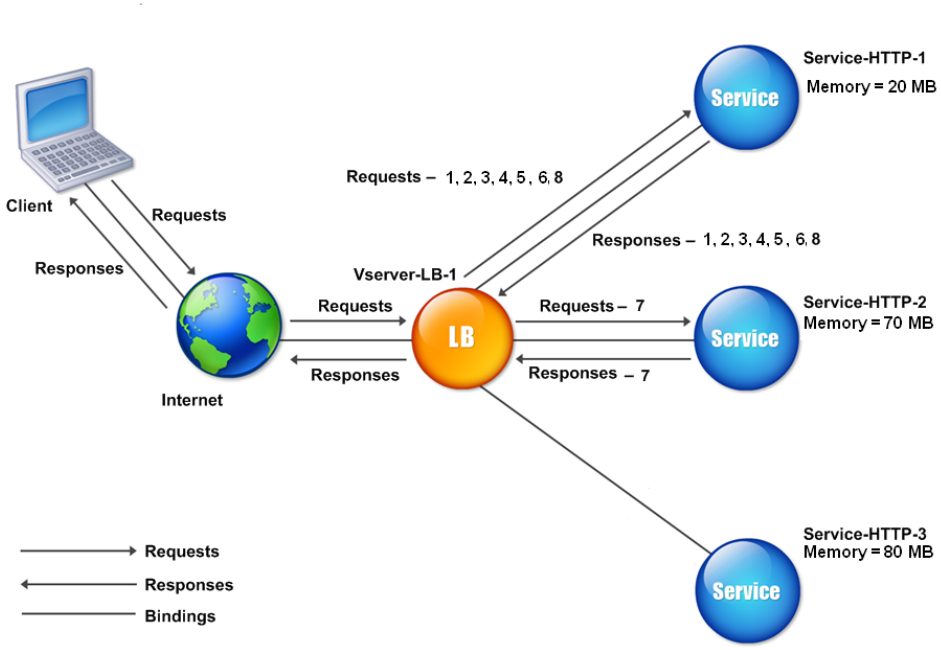


Figure 2. How the Custom Load Method Works

If each request uses 10 MB memory, the NetScaler appliance delivers requests as follows:

- Service-HTTP-1 receives the first, second, third, fourth, and fifth requests, because this service has the lowest N value.
- Service-HTTP-1 and Service-HTTP-2 now have the same load, so the virtual server reverts to the round robin method for these servers. Therefore, Service-HTTP-2 receives the sixth request, and Service-HTTP-1 receives the seventh request.

- Since Service-HTTP-1, Service-HTTP-2, and Service-HTTP-3 all now have same load, the virtual server reverts to the round robin method for Service-HTTP-3 as well. Therefore, Service-HTTP-3 receives the eighth request.

The following table summarizes how N is calculated.

Request received	Service selected	Current N Value (Number of Active Transactions)	Remarks
Request-1	Service-HTTP-1 (N = 20)	N = 30	Service-HTTP-3 has the lowest N value.
Request-2	Service-HTTP-1 (N = 30)	N = 40	
Request-3	Service-HTTP-1 (N = 40)	N = 50	
Request-4	Service-HTTP-1 (N = 50)	N = 60	
Request-5	Service-HTTP-1 (N = 60)	N = 70	
Request-6	Service-HTTP-1 (N = 70)	N = 80	Service-HTTP-2 and Service-HTTP-3 have the same N values.
Request-7	Service-HTTP-2 (N = 70)	N = 80	
Request-8	Service-HTTP-1 (N = 80)	N = 90	Service-HTTP-1, Service-HTTP-2, and Service-HTTP-3 have the same N values.

If different weights are assigned to the services, the custom load algorithm considers both the load on each service and the weight assigned to each service. It selects a service by using the value (Nw) in the following expression:

*Nw = (N) * (10000 / weight)*

As in the preceding example, suppose Service-HTTP-1 is assigned a weight of 4, Service-HTTP-2 is assigned a weight of 3, and Service-HTTP-3 is assigned a weight of 2. If each request uses 10 MB memory, the NetScaler appliance delivers requests as follows:

- Service-HTTP-1 receives the first, second, third, fourth, fifth, sixth, seventh, and eighth requests, because this service has the lowest Nw value.

- Service-HTTP-2 receives the ninth request, because this service has the lowest Nw value.

Service-HTTP-3 has the highest Nw value, and is therefore not considered for load balancing.

The following table summarizes how Nw is calculated.

Request received	Service selected	Current Nw Value (Number of Active Transactions) * (10000 / Weight)	Remarks
Request-1	Service-HTTP-1 (Nw = 50000)	Nw = 75000	Service-HTTP-1 has the lowest Nw value.
Request-2	Service-HTTP-1 (Nw = 5000)	Nw = 100000	
Request-3	Service-HTTP-1 (Nw = 15000)	Nw = 125000	
Request-4	Service-HTTP-1 (Nw = 20000)	Nw = 150000	
Request-5	Service-HTTP-1 (Nw = 23333.34))	Nw = 175000	
Request-6	Service-HTTP-1 (Nw = 25000)	Nw = 200000	
Request-7	Service-HTTP-1 (Nw = 23333.34)	Nw = 225000	
Request-8	Service-HTTP-1 (Nw = 25000)	Nw = 250000	
Request-9	Service-HTTP-2 (Nw = 233333.34)	Nw = 266666.67	Service-HTTP-2 has the lowest Nw value.
Service-HTTP-1 is selected for load balancing when it completes its active transactions or when the Nw value of other services (Service-HTTP-2 and Service-HTTP-3) is equal to 400,000.			

The following diagram illustrates how the NetScaler appliance uses the custom load method when weights are assigned.

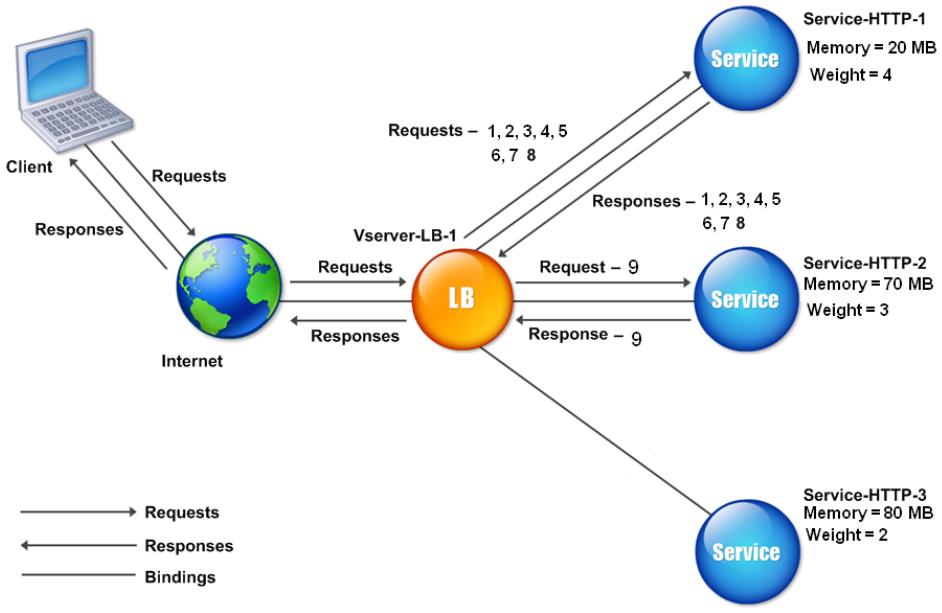


Figure 3. How the Custom Load Method Works When Weights Are Assigned

To configure the custom load method, see Configuring a Load Balancing Method that Does Not Include a Policy.

Configuring the Token Method

A load balancing virtual server configured to use the token method bases its selection of a service on the value of a data segment extracted from the client request. The data segment is called the token. You configure the location and size of the token. For subsequent requests with the same token, the virtual server chooses the same service that handled the initial request.

This method is content aware; it operates differently for TCP, HTTP, and HTTPS connections. For HTTP or HTTPS services, the token is found in the HTTP headers, the URL, or the BODY. To locate the token, you specify or create a classic or advanced expression. For more information on classic or advanced expressions, see Policy Configuration and Reference.

For HTTP services, the virtual server searches for the configured token in the first 24 kilobytes (KB) of the TCP payload. For non-HTTP (TCP, SSL, and SSL_TCP) services, the virtual server searches for the configured token in the first 16 packets if the total size of the 16 packets is less than 24 KB. But if the total size of the 16 packets is greater than 24 KB, the NetScaler searches for the token in the first 24 KB of payload. You can use this load balancing method across virtual servers of different types to make sure that requests presenting the same token are directed to appropriate services, regardless of the protocol used.

For example, consider a load balancing setup consisting of servers that contain Web content. You want to configure the NetScaler appliance to search for a specific string (the token) inside the URL query portion of the request. Server-1 has two services, Service-HTTP-1 and Service-TCP-1, and Server-2 has two services, Service-HTTP-2 and Service-TCP-2. The TCP services are bound to Vserver-LB-2, and the HTTP services are bound to Vserver-LB-1.

If Vserver-LB-1 receives a request with the token AA, it selects the service Service-HTTP-1 (bound to server-1) to process the request. If Vserver-LB-2 receives a different request with the same token (AA), it directs this request to the service Service-TCP-1. The following diagram illustrates this process.

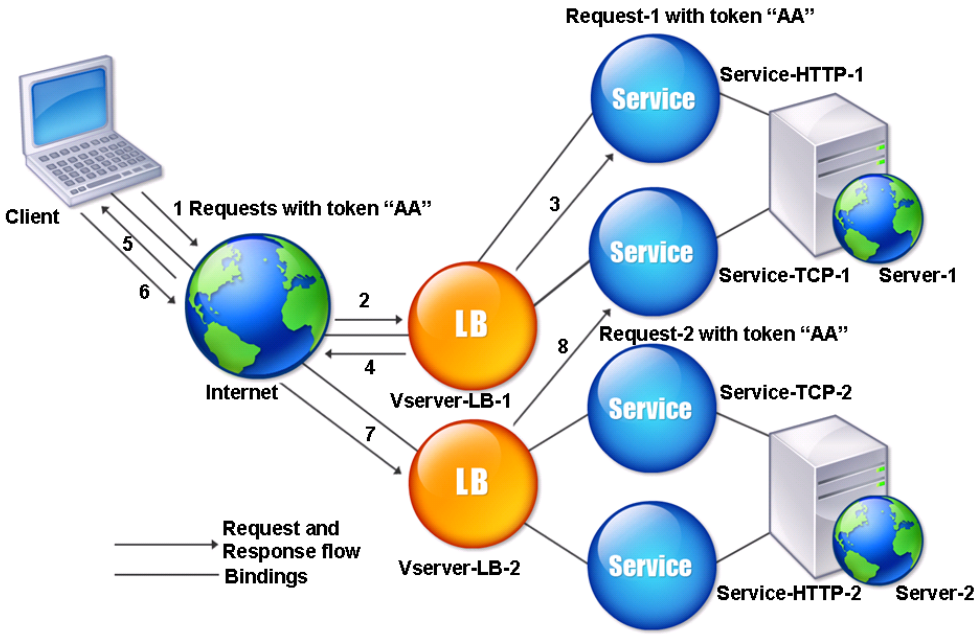


Figure 1. How the Token Method Works

To configure the Token load balancing method by using the command line interface

At the command prompt, type the following commands to configure the token load balancing method and verify the configuration:

- set lb vserver <name> -lbMethod TOKEN -rule <rule> -datalength <length> -dataoffset <offset>
- show lb vserver <name>

Example

set lb vserver LB-VServer-1 -lbMethod TOKEN -rule 'AA' -datalength 2 -dataoffset 25

show lb vserver LB-VServer-1

Parameters for Configuring the Token Load Balancing Method

name

Name of the virtual server. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

rule

A string. The string can be an existing rule name, or it can be an inline expression with a maximum of 256 characters.

datalength

Length of the token in bytes. This parameter is applicable to HTTP virtual servers and TCP virtual servers configured for Token load balancing. Valid values: 0-100. Default: No default.

dataoffset

Offset of the data to be taken as a token. This parameter is applicable to TCP virtual servers configured for Token load balancing. The token must be within the first 24 KB of the client TCP data. Valid values: 0-25400. Default: No default

To configure the Token load balancing method by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure a rule, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, click the Method and Persistence tab and under LB Method, select Token.
4. Click Configure next to the Rule text box.
5. In the Create Expression dialog box, select Classic Syntax or Advanced Syntax.
6. Under Expression, click Add.
7. In the Add Expression dialog box, enter an expression. For more information about expressions, see Policy Configuration and Reference. For example, if you are configuring a classic expression, you can select an Expression Type of General, a Flow Type of REQ, a Protocol of HTTP, a Qualifier of URLQUERY, an Operator of CONTAINS, and in the Value text box, type AA.
8. Click OK, and then click Close.
9. In the Create Expression dialog box, click Create. The expression you created appears in the Rule text box.
10. Click OK.

Configuring a Load Balancing Method That Does Not Include a Policy

After you select a load balancing algorithm for your load balancing setup, you must configure the NetScaler appliance to use that algorithm. You can configure it by using the NetScaler command line or by using the configuration utility.

Note:

The token method is policy based and requires more configuration than is described here. To configure the token method, see Configuring the Token Method.

For some hash-based methods, you can mask an IP address to direct requests belonging to the same subnet to the same server. For more information, see The Destination IP Hash Method, The Source IP Hash Method, The Source IP Destination IP Hash Method, and The Source IP Source Port Hash Method.

To set the load balancing method by using the command line interface

At the command prompt, type:

set lb vserver <name> -lbMethod <method>

Example

set lb vserver Vserver-LB-1 -lbMethod LeastConnection

Parameters for specifying a load balancing method

name

Name of the virtual server. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

lbMethod

Load balancing method used by the virtual server. Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, URLHASH, DOMAINHASH, DESTINATIONIPHASH, SOURCEIPHASH, SRCIPDESTIPHASH, LEASTBANDWIDTH, LEASTPACKETS, TOKEN, SRCIPSRCPORTHASH, LRTM, CALLIDHASH, CUSTOMLOAD. Default: LEASTCONNECTION.

To set the load balancing method by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure an LB method, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, click the Method and Persistence tab.
4. From the drop-down menu under LB Method, select a method, (for example, Least Response Time).
5. Click OK.

Persistence and Persistent Connections

Unless you configure persistence, a load balancing stateless protocol, such as HTTP, disrupts the maintenance of state information about client connections. Different transmissions from the same client might be directed to different servers even though all of the transmissions are part of the same session. You must configure persistence on a load balancing virtual server that handles certain types of Web applications, such as shopping cart applications.

Before you can configure persistence, you need to understand the different types of persistence, how they are used, and what the implications of each type is. You then need to configure the NetScaler appliance to provide persistent connections for those Web sites and Web applications that require them.

You can also configure backup persistence, which takes effect in the event that the primary type of persistence configured for a load balancing virtual server fails. You can configure persistence groups, so that a client transmission to any virtual server in a group can be directed to a server that has received previous transmissions from the same client.

For information about persistence with RADIUS load balancing, see Configuring RADIUS Load Balancing with Persistence.

About Persistence

You can choose from among any of several types of persistence for a given load balancing virtual server, which then routes to the same service all connections from the same user to your shopping cart application, Web-based email, or other network application. The persistence session remains in effect for a period of time, which you specify.

If a server participating in a persistence session goes DOWN, the load balancing virtual server uses the configured load balancing method to select a new service, and establishes a new persistence session with the server represented by that service. If the server goes OUT OF SERVICE, it continues to process existing persistence sessions, but the virtual server does not direct any new traffic to it. After the shutdown period elapses, the virtual server ceases to direct connections from existing clients to the service, closes existing connections, and redirects those clients to new services if necessary.

Depending on the persistence type you configure, the NetScaler appliance might examine the source IPs, destination IPs, SSL session IDs, Host or URL headers, or some combination of these things to place each connection in the proper persistence session. It might also base persistence on a cookie issued by the Web server, on an arbitrarily assigned token, or on a logical rule. Almost anything that allows the appliance to match connections with the proper persistence session and be used as the basis for persistence.

The following table summarizes the persistence types available on the NetScaler appliance.

Table 1. Types of Persistence

Persistence Type	Description
Source IP	SOURCEIP. Connections from the same client IP address are parts of the same persistence session.
HTTP Cookie	COOKIEINSERT. Connections that have the same HTTP Cookie header are parts of the same persistence session.
SSL Session ID	SSLSESSION. Connections that have the same SSL Session ID are parts of the same persistence session.
URL Passive	URLPASSIVE. Connections to the same URL are treated as parts of the same persistence session.
Custom Server ID	CUSTOMSERVERID. Connections with the same HTTP HOST header are treated as parts of the same persistence session.
Destination IP	DESTIP. Connections to the same destination IP are treated as parts of the same persistence session.

Source and Destination IPs	SRCIPDESTIP. Connections that are both from the same source IP and to the same destination IP are treated as parts of the same persistence session.
SIP Call ID	CALLID. Connections that have the same call ID in the SIP header are treated as parts of the same persistence session.
RTSP Session ID	RTSPSID. Connections that have the same RTSP Session ID are treated as parts of the same persistence session.
User-Defined Rule	RULE. Connections that match a user-defined rule are treated as parts of the same persistence session.

Depending on the type of persistence that you have configured, the virtual server can support either 250,000 simultaneous persistent connections or any number of persistent connections up to the limits imposed by the amount of RAM on your NetScaler appliance. The following table shows which types of persistence fall into each category.

Table 2. Persistence Types and Numbers of Simultaneous Connections Supported

Persistence Type	Number of Simultaneous Persistent Connections Supported
Source IP, SSL Session ID, Rule, destination IP, source IP/destination IP, SIP Call ID, RTSP Session ID	250 K
Cookie, URL Server ID, Custom Server ID	Memory limit. In case of CookieInsert, if timeout is not 0, the number of connections is limited by memory.

Some types of persistence are specific to particular types of virtual server. The following table lists each type of persistence and indicates which types of persistence are supported on which types of virtual server.

Table 3. Relationship of Persistence Type to Virtual Server Type

Persistence Type	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge	SSL_TCP	RTSP	SIP_UDP
SOURCEIP	YES	YES	YES	YES	YES	YES	NO	NO
COOKIEINSERT	YES	YES	NO	NO	NO	NO	NO	NO
SSLSESSION	NO	YES	NO	NO	YES	YES	NO	NO
URLPASSIVE	YES	YES	NO	NO	NO	NO	NO	NO
CUSTOMSERVERID	YES	YES	NO	NO	NO	NO	NO	NO

RULE	YES	YES	YES	NO	NO		NO	NO
SRCIP DESTIP	YES	YES	YES	YES	YES	YES	NO	NO
DESTIP	YES	YES	YES	YES	YES	YES	NO	NO
CALLID	NO	NO	NO	NO	NO	NO	NO	YES
RTSPID	NO	NO	NO	NO	NO	NO	YES	NO

Persistence Based on Source IP Address

When source IP persistence is configured, the load balancing virtual server uses the configured load balancing method to select a service for the initial request, and then uses the source IP address (client IP address) to identify subsequent requests from that client and send them to the same service. You can set a time-out value, which specifies the maximum inactivity period for the session. When the time-out value expires, the session is discarded, and the configured load balancing algorithm is used to select a new server.

Caution: In some circumstances, using persistence based on source IP address can overload your servers. All requests to a single Web site or application are routed through the single gateway to the NetScaler appliance, even though they are then redirected to multiple locations. In multiple proxy environments, client requests frequently have different source IP addresses even when they are sent from the same client, resulting in rapid multiplication of persistence sessions where a single session should be created. This issue is called the "Mega Proxy problem." You can use HTTP cookie-based persistence instead of Source IP-based persistence to prevent this from happening.

To configure persistence based on Source IP Address, see Configuring Persistence Types That Do Not Require a Rule.

Note: If all incoming traffic comes from behind a Network Address Translation (NAT) device or proxy, the traffic appears to the NetScaler appliance to come from a single source IP address. This prevents Source IP persistence from functioning properly. Where this is the case, you must select a different persistence type.

Persistence Based on HTTP Cookies

When HTTP cookie persistence is configured, the NetScaler appliance sets a cookie in the HTTP headers of the initial client request. The cookie contains the IP address and port of the service selected by the load balancing algorithm. As with any HTTP connection, the client then includes that cookie with any subsequent requests.

When the NetScaler appliance detects the cookie, it forwards the request to the service IP and port in the cookie, maintaining persistence for the connection. You can use this type of persistence with virtual servers of type HTTP or HTTPS. This persistence type does not consume any NetScaler resources and therefore can accommodate an unlimited number of persistent clients.

Note: If the client's Web browser is configured to refuse cookies, HTTP cookie-based persistence will not work. It might be advisable to configure a cookie check on the Web site, and warn clients that do not appear to be storing cookies properly that they will need to enable cookies for the Web site if they want to use it.

The format of the cookie that the NetScaler appliance inserts is:

NSC_XXXX=<*ServiceIP* ><*ServicePort*>

where:

- *NSC_XXXX* is the virtual server ID that is derived from the virtual server name.
- *ServiceIP* and *ServicePort* are encoded representations of the service IP address and service port, respectively. The IP address and port are encoded separately.

You can set a time-out value for this type of persistence to specify an inactivity period for the session. When the connection has been inactive for the specified period of time, the NetScaler appliance discards the persistence session. Any subsequent connection from the same client results in a new server being selected based on the configured load balancing method, and a new persistence session being established.

Note: If you set the time-out value to 0, the NetScaler appliance does not specify an expiration time, but sets a session cookie that is not saved when the client's browser is shut down.

By default, the NetScaler appliance sets HTTP version 0 cookies for maximum compatibility with client browsers. (Only certain HTTP proxies understand version 1 cookies; most commonly used browsers do not.) You can configure the appliance to set HTTP version 1 cookies, for compliance with RFC2109. For HTTP version 0 cookies, the appliance inserts the cookie expiration date and time as an absolute Coordinated Universal Time (GMT). It calculates this value as the sum of the current GMT time on the appliance and the time-out value. For HTTP version 1 cookies, the appliance inserts a relative expiration time by setting the "Max-Age" attribute of the HTTP cookie. In this case, the client's browser calculates the actual expiration time.

To configure persistence based on a cookie inserted by the appliance, see Configuring Persistence Types That Do Not Require a Rule.

In the HTTP cookie, the appliance by default sets the httponly flag to indicate that the cookie is nonscriptable and should not be revealed to the client application. Therefore, a client-side script cannot access the cookie, and the client is not susceptible to cross-site scripting.

Certain browsers, however, do not support the httponly flag and, therefore, might not return the cookie. As a result, persistence is broken. For browsers that do not support the flag, you can omit the httponly flag in the persistence cookie.

To change the httponly flag setting by using the command line interface

At the command prompt, type:

set lb parameter -httpOnlyCookieFlag (ENABLED|DISABLED)

Example

```
>  set lb parameter -httpOnlyCookieFlag disabled
   Done
> show lb parameter
  Global LB parameters:
      Persistence Cookie HttpOnly Flag: DISABLED
      Use port for hash LB: YES
 Done
```

Parameter for customizing the httponly flag

httpOnlyCookieFlag

Flag the persistence cookie as nonscriptable so that it is not revealed to the client application. Possible values: ENABLED, DISABLED. Default: ENABLED.

To change the httponly flag setting by using the configuration utility

1. In the navigation pane, click Load Balancing.
2. In the Settings group, click Configure Load Balancing Parameters.
3. To not set the httponly flag in the persistence cookie, clear the Persistence Cookie HTTPOnly Flag check box.
4. Click OK.
5. Open the Configure Load Balancing Parameters dialog box and verify the setting you just configured.

Persistence Based on SSL Session IDs

When SSL Session ID persistence is configured, the NetScaler appliance uses the SSL Session ID, which is part of the SSL handshake process, to create a persistence session before the initial request is directed to a service. The load balancing virtual server directs subsequent requests that have the same SSL session ID to the same service. This type of persistence is used for SSL bridge services.

Note:

There are two issues that users should consider before choosing this type of persistence. First, the NetScaler appliance does not encrypt or decrypt data when it forwards requests to services in an SSL bridge configuration, because it must maintain the data structures to keep track of the sessions. This type of persistence therefore consumes resources on the NetScaler appliance, which limits the number of concurrent persistence sessions that it can support. If you expect to support a very large number of concurrent persistence sessions, you might want to choose another type of persistence.

Second, if the client and the load-balanced server should renegotiate the session ID during their transactions, persistence is not maintained, and a new persistence session is created when the client's next request is received. This may result in the client's activity on the Web site being interrupted and the client being required to reauthenticate or restart the session. It may also result in large numbers abandoned sessions if the timeout is set to too large a value.

To configure persistence based on SSL session ID, see Configuring Persistence Types That Do Not Require a Rule.

Persistence Based on Diameter AVP Number

You can use persistence based on the AVP number of a Diameter message to create persistent Diameter sessions. When the NetScaler appliance finds the AVP in the Diameter message, it creates a persistence session based on the value of the AVP. All subsequent messages that match the value of the AVP are directed to the previously selected server. If the value of the AVP does not match the persistence session, a new session is created for the new value.

Note: If the AVP number is not defined in Diameter base-protocol RFC 3588, and if the number is nested inside a grouped AVP, you must define a sequence of AVP numbers (maximum of 3) in parent-to-child order. For example, if persist AVP number X is nested inside AVP Y, which is nested in Z, define the list as Z Y X.

To configure Diameter-based persistence on a virtual server by using the command line interface

At the command prompt, type the following command:

set lb vserver <name> -PersistenceType <type-> persistAVPno <positive_integer>

Example

```
set lb vserver diameter_vs -persistenceType DIAMETER -persistAVPno
263
```

Custom Server ID Persistence

In the Custom Server ID persistence method, the Server ID specified in the client request is used to maintain persistence. For this type of persistence to work, you must first set a server ID on the services. The NetScaler appliance checks the URL of the client request and connects to the server associated with the specified server ID. The service provider should make sure that the users are aware of the server IDs to be provided in their requests for specific services.

For example, if your site provides different types of data, such as images, text, and multimedia, from different servers, you can assign each server a server ID. On the NetScaler appliance, you specify those server IDs for the corresponding services, and you configure custom server ID persistence on the corresponding load balancing virtual server. When sending a request, the client inserts the server ID into the URL indicating the required type of data.

To configure custom server ID persistence:

- In your load balancing setup, assign a server ID to each service for which you want to use the user-defined server ID to maintain persistence. Alphanumeric server IDs are allowed.
- Specify rules, in the default-syntax expression language, to examine the URL queries for the server ID and forward traffic to the corresponding server.
- Configure custom server ID persistence.

Note: The persistence time-out value does not affect the Custom Server ID persistence type. There is no limit on the maximum number of persistent clients because this persistence type does not store any client information.

Example

In a load balancing setup with two services, assign server ID 2345-photo-56789 to Service-1, and server ID 2345-drawing-abb123 to Service-2. Bind these services to a virtual server named Web11.

```
set service Service-1 10.102.29.5 -serverID 2345-photo-56789
set service Service-1 10.102.29.6 -serverID 2345-drawing-abb123
```

On virtual server Web11, enable Custom Server ID persistence.

Example

```
set lb vserver Web11 -persistenceType customserverID
bind lb vserver Web11 Service-[1-2]
```

Create the following expression so that all URL queries containing the string "sid=" are examined.

```
HTTP.REQ.URL.AFTER_STR(“sid=”)
```

When a client sends a request with the following URL to the IP address of Web11, the NetScaler directs the request to Service-2 and honors persistence.

Example

http://www.example.com/index.asp?&sid=2345-drawing-abb123

For more information about default-syntax policy expressions, see the Policy Configuration and Reference.

Parameters for configuring custom server ID persistence

ServiceName

The name of the service that you are configuring.

vServerName

The name of the virtual server

persistenceType

Method of persistence. Select CUSTOMSERVERID.

rule

Rule to examine the URL for server ID.

To configure custom server ID persistence by using the configuration utility

1. Assign a server ID to each of the services for which you want to configure custom server ID persistence.

    a. In the navigation pane, expand Load Balancing, and then click Services.

    b. In the details pane, select the service for which you want to specify a server ID, and then click Open.

    c. In the Configure Service dialog box, click the Advanced tab.

    d. Scroll down, and under Others, in the Server ID box, type an ID for the server.

    e. Click OK.
2. Configure custom server ID persistence on the virtual server to which the services are bound.

    a. In the navigation pane, expand Load Balancing, and then click Virtual Servers.

    b. In the details pane, select the virtual server for which you want to specify persistence, and then click Open.

    c. On the Method and Persistence tab, in the Persistence group, select CUSTOMSERVERID.

    d. In the Rule box, type an expression, or click Configure, and use the options available in the Create Expression dialog box, to create the expression.

    e. Click OK.

Persistence Based on Destination IP Addresses

With destination IP address-based persistence, when the NetScaler appliance receives a request from a new client, it creates a persistence session based on the IP address of the service selected by the virtual server (the destination IP address). Subsequently, it directs requests to the same destination IP to the same service. This type of persistence is used with link load balancing. For more information about link load balancing, see Link Load Balancing.

The time-out value for destination IP persistence is the same as that for source IP persistence, described in Persistence Based on Source IP Address.

To configure persistence based on the destination IP address, see Configuring Persistence Types That Do Not Require a Rule.

Persistence Based on Source and Destination IP Addresses

With source and destination IP address-based persistence, when the NetScaler appliance receives a request, it creates a persistence session based on both the IP address of the client (the source IP address) and the IP address of the service selected by the virtual server (the destination IP address). Subsequently, it directs requests from the same source IP and to the same destination IP to the same service.

The time-out value for destination IP persistence is the same as that for source IP persistence, described in Persistence Based on Source IP Address.

To configure persistence based on both source and destination IP addresses, see Configuring Persistence Types That Do Not Require a Rule.

Persistence Based on SIP Call ID

With SIP Call ID persistence, the NetScaler appliance chooses a service based on the call ID in the SIP header. This enables it to direct packets for a particular SIP session to the same service and, therefore, to the same load balanced server. This persistence type is applicable specifically to SIP load balancing. For more information about SIP load balancing, see Monitoring SIP Services.

To configure persistence based on SIP Call ID, see Configuring Persistence Types That Do Not Require a Rule.

Persistence Based on RTSP Session IDs

With RTSP Session ID persistence, when the NetScaler appliance receives a request from a new client, it creates a new persistence session based on the Real-Time Streaming Protocol (RTSP) session ID in the RTSP packet header, and then directs the request to the RTSP service selected by the configured load balancing method. It directs subsequent requests that contain the same session ID to the same service. This persistence type is applicable specifically to SIP load balancing. For more information about SIP load balancing, see Monitoring SIP Services.

Note: RTSP Session ID persistence is configured by default on RTSP virtual servers, and you cannot modify that setting.

Sometimes different RTSP servers issue the same session IDs. When this happens, unique sessions cannot be created between the client and the RTSP server by using only the RTSP session ID. If you have multiple RTSP servers that may issue the same session IDs, you can configure the appliance to append the server IP address and port to the session ID, creating a unique token that can be used to establish persistence. This is called session ID mapping.

To configure persistence based on RTSP Session IDs, see Configuring Persistence Types That Do Not Require a Rule.

Important: If you need to use session ID mapping, you must set the following parameter when configuring each service within the load balancing setup. Also, make sure that no non-persistent connections are routed through the RTSP virtual server.

Parameter to Set When Configuring Services

session

Map the RTSP session ID by appending the IP address and port of the server to the session ID, guaranteeing that all session IDs are unique within the load balancing setup.

Note: When Session ID Mapping is enabled, the NetScaler appliance rejects any packet that does not contain a mapped ID. Possible values: ON and OFF. Default: OFF.

Note: If a client sends multiple SETUP requests on a single TCP connection, the NetScaler appliance sends those SETUP requests to the same service, because it makes a load balancing decision for every TCP connection. When this occurs, the appliance does not forward the SETUP requests to different servers based on the RTSP session ID.

Configuring URL Passive Persistence

With URL Passive persistence, when the NetScaler appliance receives a request from a client, it extracts the server IP address-port information (expressed as a single hexadecimal number) from the client request.

URL passive persistence requires configuring an advanced expression that specifies the query element that contains the server IP address-port information. For more information about classic and advanced policy expressions, see Policy Configuration and Reference.

The following expression configures the appliance to examine requests for URL queries that contain the string "urlp=", extract the server IP address-port information, convert it from a hexadecimal string to an IP and port number, and forward the request to the service configured with this IP address and port number.

HTTP.REQ.URL.AFTER_STR(“urlp=”)

If URL passive persistence is enabled and the above expression is configured, a request with the following URL and server IP address-port string is directed to 10.102.29.10:80.

http://www.example.com/index.asp?&urlp=0A661D0A0050

The persistence time-out value does not affect this persistence type; persistence is maintained as long as the server IP address-port information can be extracted from client requests. This persistence type does not consume any NetScaler resources, so it can accommodate an unlimited number of persistent clients.

To configure URL passive persistence, you first configure persistence as described in Configuring Persistence Types That Do Not Require a Rule. You set the persistence type to URLPASSIVE. You then perform the procedures provided below.

To configure URL passive persistence by using the command line interface

At the command prompt, type:

set lb vserver <vserverName> [-rule <expression>]

Example

set lb vserver LB-VServer-1 –rule HTTP.REQ.URL.AFTER_STR(“urlp=”)

Parameters for Rule-Based Persistence

rule

Value used to set the URLPASSIVE persistence type. The value can be an existing rule name, or it can be a classic or advanced expression. The default value is none. The maximum length is 14999.

The rule evaluates either requests that are directed to the load balanced servers or responses from the servers.

To configure URL passive persistence by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the Configure Virtual Server (Load Balancing) dialog box, on the Method and Persistence tab, in Persistence, select URLPASSIVE.
3. Click the Configure button next to the Rule field.
4. In the dialog box that appears, create the rule that you want to use. For more information about creating rules, see Policy Configuration and Reference.
5. Click OK.

Configuring Persistence Based on User-Defined Rules

When rule based persistence is configured, the NetScaler appliance creates a persistence session based on the contents of the matched rule before directing the request to the service selected by the configured load balancing method. Subsequently, it directs all requests that match the rule to the same service. You can configure rule based persistence for services of type HTTP, SSL, RADIUS, ANY, TCP, and SSL_TCP.

Rule based persistence requires a classic or default syntax expression. You can use a classic expression to evaluate request headers, or you can use a default syntax expression to evaluate request headers, Web form data in a request, response headers, or response bodies. For example, you could use a classic expression to configure persistence based on the contents of the HTTP Host header. You could also use a default syntax expression to configure persistence based on application session information in a response cookie or custom header. For more information on creating and using classic and default syntax expressions, see Policy Configuration and Reference.

The expressions that you can configure depends on the type of service for which you are configuring rule based persistence. For example, certain RADIUS-specific expressions are not allowed for protocols other than RADIUS, and TCP-option based expressions are not allowed for service types other than the ANY type. For TCP and SSL_TCP service types, you can use expressions that evaluate TCP/IP protocol data, Layer 2 data, TCP options, and TCP payloads.

Note: For a use case that involves configuring rule based persistence on the basis of Financial Information eXchange ("FIX") Protocol data transmitted over TCP, see Configuring Rule Based Persistence Based on a Name-Value Pair in a TCP Byte Stream.

Rule based persistence can be used for maintaining persistence with entities such as Branch Repeater appliances, Branch Repeater plug-ins, cache servers, and application servers.

Note: On an ANY virtual server, you cannot configure rule-based persistence for the responses.

To configure persistence based on a user-defined rule, you first configure persistence as described in Configuring Persistence Types That Do Not Require a Rule, and set the persistence type to RULE. You then perform the procedures provided below. You can configure rule based persistence by using the configuration utility or the NetScaler command line.

To configure persistence based on user-defined rules by using the command line interface

At the command prompt, type:

set lb vserver <vserverName> [-rule <expression>][-resRule <expression>]

Example

```
set lb vserver vsvr_name –rule http.req.header("cookie").value(0).typecast_nvlist_t('=',';').value("server")

set lb vserver vsvr_name –resrule http.res.header("set-cookie").value(0).typecast_nvlist_t('=',';').value("serve
```

Parameters for Rule-Based Persistence

rule

Value used to set the RULE persistence type. The value can be an existing rule name, or it can be a classic or default syntax expression. You can specify this parameter for services of type . You can specify an expression that evaluates requests from clients.

Maximum length: 1499 characters. Default: NONE.

resRule

Value used to set the RULE persistence type. The response rule evaluates responses from the load balanced servers. You can configure this parameter for services of type . The expression must be a default syntax expression that evaluates responses from the load balanced servers.

Maximum length: 1499 characters. Default: NONE.

To configure persistence based on user-defined rules by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click **Add**.
3. In the Configure Virtual Server (Load Balancing) dialog box, on the Method and Persistence tab, choose the type of rule you want to configure.
   - If you want to base the rule on the request, click the Configure button next to the Rule field.
   - If you want to base the rule on the response, click the Configure button next to the Response Rule field.
4. In the dialog box that appears, select Switch to Classic Syntax or Switch to Advanced Syntax.
5. Select or create the rule that you want to use. Some examples of rules that you might find useful are provided below. For more information, see Policy Configuration and Reference.
6. Click OK.

Example: Classic Expression for a Request Payload

The following classic expression creates a persistence session based on the presence of a User-Agent HTTP header that contains the string, “MyBrowser”, and directs any subsequent client requests that contain this header and string to the same server that was selected for the initial request.

```
http header User-Agent contains MyBrowser
```

Example: Default syntax Expression for a Request Header

The following default syntax expression does exactly the same thing as the previous classic expression.

```
HTTP.REQ.HEADER("User-Agent").CONTAINS ("MyBrowser")
```

Example: Default syntax Expression for a Response Cookie

The following expression examines responses for “server” cookies, and then directs any requests that contain that cookie to the same server that was selected for the initial request.

```
HTTP.RES.HEADER("SET-COOKIE").VALUE(0).TYPECAST_NVLIST_T('=',';').VALUE("server")
```

Configuring Persistence Types That Do Not Require a Rule

To configure persistence, you must first set up a load balancing virtual server, as described in Setting Up Basic Load Balancing. You then configure persistence on the virtual server.

To configure persistence on a virtual server by using the command line interface

At the command prompt, type the following commands to configure persistence and verify the configuration:

- set lb vserver <name> -PersistenceType <type> [-timeout <integer>]
- show lb vserver

Example

set lb vserver Vserver-LB-1 -persistenceType SOURCEIP

show lb vserver

Note: For IP-based persistence, you can also set the persistMask parameter.

Parameters for configuring persistence

PersistenceType

Persistence type supported on the virtual server. Valid Values: SOURCEIP, COOKIEINSERT, SSLSESSION, RULE, URLPASSIVE, CUSTOMSERVERID, DESTIP, SRCIPDESTIP, CALLID, RTSPID, and NONE. Default: NONE.

persistMask

Defines which IP range is used to determine whether a connection is part of an existing persistence session or not. This parameter is used only if the persistence type is IP-based. The default value, 255.255.255.255, specifies that only connections from the same IP are part of an existing session. Valid values include the full range of available subnet masks.

Note: Setting this parameter to 0 has the same effect as setting it to 255.255.255.255.

timeout

The period, in minutes, for which a persistence session remains in effect. Maximum value: 1440 minutes. Default: 2 minutes.

To configure persistence on a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure persistence, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, on the Method and Persistence tab, in the Persistence list, select the persistence type you want to use (for example, SOURCEIP).
4. In the Time-out and Netmask text boxes type the time-out and subnet mask values (for example, 2 and 255.255.255.255).
5. Click OK.

Configuring Backup Persistence

The NetScaler appliance uses backup persistence to choose a new type of persistence when the primary persistence type fails. For example, if the primary persistence type is set to Cookie Insert, and backup persistence is set to Source IP, the NetScaler appliance uses Source IP-based persistence when the cookie is missing from the HTTP header or when the client browser does not support cookies.

You can set a time-out value for backup persistence only when the primary persistence type is HTTP Cookie-based or RTSP session ID-based persistence, and the backup persistence type is Source IP-based.

To set backup persistence for a virtual server by using the command line interface

At the command prompt, type:

set lb vserver <name>@ -persistenceType <PersistenceType> -persistenceBackup <BackupPersistenceType>

Example

set lb vserver Vserver-LB-1 -persistenceType CookieInsert -persistenceBackup SourceIP

Parameter for configuring backup persistence

persistenceBackup

Backup persistence type for the group. Possible values: SOURCEIP, NONE. Default: NONE.

To set backup persistence for a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure backup persistence (for example, Vserver-LB-1), and then click Open.
3. The Configure Virtual Server (Load Balancing) dialog box, click the Method and Persistence tab.
4. In the Persistence list, select the persistence type you want (for example, COOKIEINSERT).
5. In the Time-out text box, type the time-out value you want (for example, 20).
6. In the Backup Persistence list, select the backup persistence type that you want to configure (for example, SOURCEIP).
7. In the Backup Time-out and Netmask text boxes, type the backup time-out value and netmask (for example, 20 and 255.255.255.255).
8. Click OK.

Configuring Persistence Groups

When you have load-balanced servers that handle several different types of connections (such as Web servers that host multimedia), you can configure a virtual server group to handle these connections. To create a virtual server group, you bind different types of virtual servers, one for each type of connection that your load balanced servers accept, into a single group. You then configure a persistence type for the entire group.

You can configure either source IP-based persistence or HTTP cookie-based persistence for persistence groups. After you set persistence for the entire group, you cannot change it for individual virtual servers in the group. If you configure persistence on a group and then add a new virtual server to the group, the persistence of the new virtual server is changed to match the persistence setting of the group.

When persistence is configured on a group of virtual servers, persistence sessions are created for initial requests, and subsequent requests are directed to the same service as initial request, regardless of the virtual server in the group that receives each client request.

If you configure HTTP cookie-based persistence, the domain attribute of the HTTP cookie is set. This setting causes the client software to add the HTTP cookie into client requests if different virtual servers have different public host names. For more information about CookieInsert persistence type, see Persistence Based on HTTP Cookies.

To create a virtual server persistency group by using the command line interface

At the command prompt, type:

bind lb group <vServerGroupName> <vServerName> -persistenceType <PersistenceType>

Example

bind lb group Vserver-Group-1 Vserver-LB-1 -persistenceType CookieInsert

Parameters for configuring virtual server persistency groups

name

Name of the persistence group. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( )

persistenceType

Persistence type for the group. Possible values: SOURCEIP, COOKIEINSERT, NONE.

Note: If you specify NONE, the persistence configured for each of the individual virtual servers is applied, and the persistence group does not function.

persistMask

Netmask specified when the persistency type is SOURCEIP.

timeout

Time period for which the persistence is in effect for a specific client. The value ranges from 2 through 1440 minutes. The default value is 2 minutes. The maximum value is 1440 minutes (1 day).

To create a virtual server persistency group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Persistency Groups.
2. On the Persistency Groups pane, click Add.
3. In the Create Persistency Group dialog box, in the Group Name text box type a name for the group (for example, Vserver-Group-1).
4. In the Persistence list, select a persistence type (for example, SOURCEIP).
5. In the Persistence Mask and Time-out text boxes, type the persistence mask and timeout values (for example, 255.255.255.255 and 2).
6. Under Virtual Server List, in the Available Virtual Server list box, select the virtual server that you want to bind to the group (for example, Vserver-LB-1), and then click Add.
7. Click Create, and then click Close. The virtual server group you created appears in the Persistence Groups pane.

You can also change the backup persistence type, backup persistence time-out, and cookie domain value on an existing persistence group.

To modify a virtual server group by using the command line interface

At the command prompt, type:

set lb group <vServerGroupName> -PersistenceBackup <BackupPersistenceType> -persistMask <SubnetMaskAddress>

Example

```
set lb group vserver-Group-1 -PersistenceBackup SourceIP -persistMask 255.255.255.255
```

Parameters for modifying virtual server persistency groups

PersistenceBackup

Backup persistence type for the group. The valid options for this parameter are: SOURCEIP and NONE

backupPersistenceTimeout

Maximum time, in minutes, for which the backup persistence is in effect for a specific client. Maximum value: 1440. Default: 2.

cookieDomain

Domain attribute of the HTTP cookie.

To modify a virtual server group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Persistency Groups.
2. In the Persistency Groups pane, select the virtual server group that you want to modify (for example, Vserver-Group-1), and click Open.
3. The Configure Virtual Server Group dialog box appears.
4. In the Backup Persistence list, select the type of backup persistence (for example, SOURCEIP).
5. In the Persistence Mask text box, type the subnet mask (for example, 255.255.255.255).
6. Click OK.

Configuring RADIUS Load Balancing with Persistence

Today's complex networking environment often requires coordinating a high-volume, high-capacity load balancing configuration with robust authentication and authorization. Application users may connect to a VPN through mobile access points such as consumer-grade DSL or Cable connections, WiFi, or even dial-up nodes. Those connections usually use dynamic IPs, which can change during the connection.

If you configure RADIUS load balancing on the NetScaler appliance to support persistent client connections to RADIUS authentication servers, the appliance uses the user logon or the specified RADIUS attribute instead of the client IP as the session ID, directing all connections and records associated with that user session to the same RADIUS server. Users are therefore able to log on to your VPN from mobile access locations without experiencing disconnections when the client IP or WiFi access point changes.

To configure RADIUS load balancing with persistence, you must first configure RADIUS authentication for your VPN. For information and instructions, see the Authentication, Authorization, Auditing (AAA) chapter in AAA Application Traffic. You must also choose either the Load Balancing or Content Switching feature as the basis for your configuration, and make sure that the feature you chose is enabled. The configuration process with either feature is almost the same.

Then, you configure either two load balancing, or two content switching, virtual servers, one to handle RADIUS authentication traffic and the other to handle RADIUS accounting traffic. Next, you configure two services, one for each load balancing virtual server, and bind each load balancing virtual server to its service. Finally, you create a load balancing persistency group and set the persistency type to RULE.

Enabling the Load Balancing or Content Switching Feature

To use the Load Balancing or Content Switching feature, you must first ensure that the feature is enabled. If you are configuring a new NetScaler appliance that has not previously been configured, both of these features are already enabled, so you can skip to the next section. If you are configuring a NetScaler appliance with a previous configuration on it, and you are not certain that the feature you will use is enabled, you must do that now.

- For instructions on enabling the load balancing feature, see Enabling Load Balancing.
- For instructions on enabling the content switching feature, see Enabling Content Switching.

Configuring Virtual Servers

After enabling the load balancing or content switching feature, you must next configure two virtual servers to support RADIUS authentication:

- **RADIUS authentication virtual server.** This virtual server and its associated service will handle authentication traffic to your RADIUS server. Authentication traffic consists of connections associated with users logging onto your protected application or virtual private network (VPN).
- **RADIUS accounting virtual server.** This virtual server and its associated service will handle accounting connections to your RADIUS server. Accounting traffic consists of connections that track an authenticated user's activities on your protected application or VPN.

Important: You must create either a pair of load balancing virtual servers or a pair of content switching virtual servers to use in your RADIUS persistence configuration. You cannot mix virtual server types.

To configure a load balancing virtual server by using the command line interface

At the command prompt type the following commands to create a new load balancing virtual server and verify the configuration:

- add lb vserver <name> RADIUS <IP address> <port> -lbmethod TOKEN -rule <rule>
- show lb vserver <name>

To configure an existing load balancing virtual server, replace the above add lb virtual server command with the set lb vserver command, which takes the same arguments.

To configure a content switching virtual server by using the command line interface

At the command prompt type the following commands to create a new content switching virtual server and verify the configuration:

- add cs vserver <name> RADIUS <IP address> <port> -lbmethod TOKEN -rule <rule>
- show cs vserver <name>

To configure an existing content switching virtual server, replace the above add cs vserver command with the set cs vserver command, which takes the same arguments.

Example

```
add lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812
    -lbmethod TOKEN -rule CLIENT.UDP.RADIUS.USERNAME
add lb vserver radius_acct_vs1 RADIUS 192.168.46.34 1813
    -lbmethod TOKEN -rule CLIENT.UDP.RADIUS.USERNAME
set lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812
    -lbmethod TOKEN -rule CLIENT.UDP.RADIUS.USERNAME
set lb vserver radius_auth_vs1 RADIUS 192.168.46.34 1813
    -lbmethod TOKEN -rule CLIENT.UDP.RADIUS.USERNAME
```

Parameters for configuring virtual servers

name

A name for your new virtual server, or the name of the existing virtual server you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols.

protocol

RADIUS

IPAddress

The IP address assigned to your virtual server. This is normally an Internet-routable IP.

Note: If the virtual server uses IPv6, select the IPv6 check box and enter the address in IPv6 format. (For example, 1000:0000:0000:0000:0005:0600:700a:888b.)

port

The port on which your virtual server listens for connections.

lbmethod

TOKEN

rule

Which policy rule to use as the basis for persistence. The two supported rules are:

- CLIENT.UDP.RADIUS.USERNAME. Use the client login name.
- CLIENT.UDP.RADIUS.ATTR_TYPE(INT). Use the specified RADIUS attribute type. For INT, substitute the integer assigned to that attribute type as specified in RFC4014.

To configure a load balancing or content switching virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing or Content Switching, and then click Virtual Servers.

   Note: Except for the GUI location where you create or configure the virtual server, the process is the same.

2. In the details pane, do one of the following:

   - To create a new virtual server, click Add.

   - To modify an existing virtual server, select the virtual server, and then click Open.

3. In the Create Virtual Server (Load balancing) or Configure Virtual Server (Content Switching) dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring virtual servers" as shown:

   - Name*—name

   - Protocol*—protocol

   - IP address*—IPAddress

   - Port*—port

   * A required parameter

4. In the Method and Persistence tab, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring virtual servers" as shown:

   - Method*—method

   - Rule*—rule

   * A required parameter

5. Click Close. The virtual server that you created now appears in the Virtual Servers pane.

Configuring Services

After configuring your virtual servers, you must next configure two services, one for each of the virtual servers that you created. For instructions, see Configuring Services. You should set the service parameters as described in "Parameters for configuring services."

Note: Once configured, these services are in the DISABLED state until the NetScaler appliance can connect to your RADIUS server's authentication and accounting IPs and monitor their status.

Parameters for configuring services

name

A name for your new service, or the name of the existing service you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols.

IPAddress

The IP address used to connect to the RADIUS server for authentication or accounting, as appropriate, in either IPv4 or IPv6 format. When you provide the IP address of the service, the NetScaler appliance automatically creates a server object with this IP address as its name.

serviceType

The service type, always RADIUS when configuring RADIUS load balancing with persistence.

port

The port on which your service listens for connections.

Binding Virtual Servers to Services

After configuring your services, you must next bind each of the virtual servers that you created to the appropriate service. For instructions, see Binding Services to the Virtual Server.

Configuring a Persistency Group for Radius

After binding your load balancing virtual servers to the corresponding services, you must set up your RADIUS load balancing configuration to support persistence. To do so, you configure a load balancing persistency group that contains your RADIUS load balancing virtual servers and services, and configure that load balancing persistency group to use rule-based persistence. For instructions, see Configuring Persistence Groups. You should set the parameters as described in "Parameters for configuring RADIUS load balancing persistency groups."

Parameters for configuring RADIUS load balancing persistency groups

name

The name of the load balancing persistency group that you are setting or binding. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols.

vservername

The name of the load balancing virtual server that you are binding to the load balancing persistency group. The name can have the same length and characteristics as the name described above.

newname

The new name of the load balancing persistency group that you are renaming. The name can have the same length and characteristics as the name described above.

rule

Which policy rule to use as the basis for persistence. The two supported rules are:

- CLIENT.UDP.RADIUS.USERNAME. Use the client login name.
- CLIENT.UDP.RADIUS.ATTR_TYPE(INT). Use the specified RADIUS attribute type. For INT, substitute the integer assigned to that attribute type as specified in RFC4014

Your RADIUS load balancing configuration is now complete.

Viewing Persistence Sessions

You can view the different persistence sessions that are in effect globally or for a particular virtual server.

Note: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

To view a persistence session by using the command line interface

At the command prompt, to view all persistence sessions type:

show lb persistentSessions [<vServer>]

Example

show lb persistentSessions myVserver

Parameters for viewing a persistence session

vServer

Name of the virtual server on which the persistence sessions are running.

To view persistence sessions by using the configuration utility

1. In the navigation pane, click Load Balancing.
2. In the details pane, under Monitor Sessions, click Virtual Server persistence sessions.

Clearing Persistence Sessions

You might need to clear persistence sessions from the NetScaler if sessions fail to time out. You can do one of the following:

- Clear all sessions for all virtual servers at once.
- Clear all sessions for a given virtual server at once.
- Clear a particular session that is associated with a given virtual server.

Note: The functionality for clearing a particular session that is associated with a given virtual server is available only on NetScaler 10.e.

To clear a persistence session by using the command line interface

At the command prompt, type the following commands to clear persistence sessions and verify the configuration:

- clear lb persistentSessions [<vServer> [-persistenceParam <string>]]
- show persistentSessions <vServer>

Examples

Example 1 clears all persistence sessions for load balancing virtual server `lbvip1`. Example 2 first displays the persistence sessions for load balancing virtual server `lbvip1`, clears the session with persistence parameter `xls`, and then displays the persistence sessions to verify that the session was cleared.

Example

```
> clear persistentSessions lbvip1
 Done
> show persistentSessions
 Done
>
```

Example 2

```
> show persistentSessions lbvip1
Type       SRC-IP    ...   PERSISTENCE-PARAMETER
RULE       0.0.0.0   ...   xls
RULE       0.0.0.0   ...   txt
RULE       0.0.0.0   ...   html
 Done
> clear persistentSessions lbvip1 -persistenceParam xls
 Done
```

```
> show persistentSessions lbvip1
Type       SRC-IP    ...    PERSISTENCE-PARAMETER
RULE       0.0.0.0   ...    txt
RULE       0.0.0.0   ...    html
 Done
>
```

Parameters for clearing persistence sessions

vServer (Virtual Server)

The name of the load balancing virtual server whose persistence sessions are to be flushed. If not specified, all persistence sessions will be flushed . Maximum Length: 127.

persistenceParam (Persistence Parameter)

The persistence parameter whose sessions you want to flush. Maximum Length: 127.

To clear persistence sessions by using the configuration utility

1. In the navigation pane, click Load Balancing.
2. In the details pane, under Monitor Sessions, click Clear persistence sessions.
3. In the Clear Persistence Sessions dialog box, do one of the following:
   - If you want to clear all sessions for all virtual servers on the appliance, in Virtual Server, select All Virtual Servers.
   - If you want to clear all sessions for a given virtual server, in Virtual Server, select the virtual server.
   - If you want to clear a particular session, in Virtual Server, select the virtual server, and then, in Persistence Parameter, select the persistence parameter whose session you want to clear.
4. Click OK.

Overriding Persistence Settings for Overloaded Services

Note: This feature is available only on NetScaler 10.e.

When a service is loaded or is otherwise unavailable, service to clients is degraded. To work around this situation, you might have to configure the NetScaler appliance to temporarily forward to other services the requests that would otherwise be included in the persistence session that is associated with the overloaded service. In other words, you might have to override the persistence setting that is configured for the load balancing virtual server. You can achieve this functionality by setting the skippersistency parameter. With the parameter set, when the virtual server receives new connections for an overloaded service, the virtual server disregards any existing persistence sessions that are associated with that service, until the service returns to a state at which it can accept requests. Persistence sessions associated with other services are not affected. The functionality is available for only virtual servers whose type is ANY or UDP.

In Branch Repeater load balancing configurations, you must also configure a load monitor and bind it to the service. The monitor takes the service out of subsequent load balancing decisions until the load on the service is brought below the configured threshold. For information about configuring a load monitor for your virtual server, see Understanding Load Monitors.

You can configure the virtual server to perform one of the following actions with the requests that would otherwise form a part of the persistence session:

- **Send each request to one of the other services.** The virtual server takes a load balancing decision and sends each request to one of the other services on the basis of the configured load balancing method. If all the services are overloaded, requests are dropped until a service becomes available.

  Both wildcard and IP address–based virtual servers support this option. This action is appropriate for all deployments, including deployments in which the virtual server is load balancing Branch Repeater appliances or firewalls.

- **Bypass the virtual server-service configuration.** The virtual server does not take a load balancing decision. Instead, it simply bridges each request through to a physical server on the basis of the destination IP address in the request.

  Only wildcard virtual servers of type ANY and UDP support the bypass option. Wildcard virtual servers have a *:* IP and port combination. This action is appropriate for deployments in which you are using the virtual server to load balance Branch Repeater appliances or firewalls. In these deployments, the NetScaler appliance first forwards a request to a Branch Repeater appliance or firewall, and then forwards the processed response to a physical server. If you configure the virtual server to bypass the virtual server–service configuration for overloaded services, if a Branch Repeater appliance or firewall gets overloaded, the virtual server bridges requests directly to their destination IP addresses until the Branch Repeater appliance or firewall can accept requests.

To override persistence settings for overloaded services by using the command line interface

At the command prompt, type the following commands to override persistence settings for overloaded services and verify the configuration:

- set lb vserver <name> -skippersistency <skippersistency>
- show lb vserver <name>

Example

```
> set lb vserver mylbvserver -skippersistency ReLb
 Done
> show lb vserver mylbvserver
    mylbvserver (*:*) - ANY Type: ADDRESS
       . . .
       . . .
 Skip Persistency: ReLb
       . . .
 Done
>
```

Parameters for overriding persistence for overloaded services

name

The name of the load balancing virtual server.

skippersistency

Disregard the persistence settings that are configured for the virtual server when the virtual server receives new connections for a service that is overloaded or unavailable. Possible values: Bypass, ReLb, None. Default value: None.

If you set the parameter to `ReLb`, the virtual server sends requests to other services on the basis of the configured load balancing method until the overloaded service returns to a state at which it can accept requests. This action is appropriate for all deployments, including deployments in which the virtual server is load balancing Branch Repeater appliances. If all the services are overloaded, requests are dropped until a service becomes available.

If you set the parameter to `Bypass`, the virtual server bypasses the virtual server–service configuration and bridges the requests through to the servers.

To override persistence settings for overloaded services by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click the virtual server that you want to override persistence settings when services are overloaded, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, on the Advanced tab, in the Skip Persistency list, select the option that you want.
4. Click OK.

Troubleshooting

The statistics from the NetScaler VPX appliance indicate that the appliance has reached the session persistence limit. As a result, persistence sessions are failing. Is possible to increase the session persistence limit?

Cause: The NetScaler appliance has the system limit of 250,000 persistence session for a core.

Resolution: To resolve this issue, you can perform any of the following tasks:

- Reduce the time out value for persistence
- Increase the number of cores for the appliance

After configuring Cookie Insert persistence on the NetScaler appliance, the users report that the connections work fine for some time, but then start getting disconnected. What best practice should I follow when configuring persistence?

Cause: By default, the time-out value for Cookie Insert persistence is 120 seconds.

Resolution: When you configure persistence for applications for which idle time cannot be determined, set the Cookie Insert persistence time-out value to 0. With this setting, the connection does not time out.

After configuring an HTTP virtual server on the NetScaler appliance, I need to make sure that a user always connects to the same server for the requested content, so I configured SourceIP persistence. Now, increasing the time-out value for persistence introduces latency. How can I increase the timeout value without affecting performance?

Resolution: Consider using Cookie Insert persistence with the time-out value set to 0. This setting enables long-duration persistence settings, because the appliance does not specify a time for expiring the cookie.

After configuring Cookie Insert persistence on the NetScaler appliance, it works as expected when clients from the same time zone access the content. However, when a client from another time zone makes an attempt to connect, the connection is immediately timed out.

Cause: Time based Cookie Insert persistence works as expected when a client from the same time zone makes a connection. However, when the client machine and NetScaler appliance are in different time zones, the cookie is not valid. For example, when a client in EST time zone sends a cookie at 11:00 AM EST to a NetScaler appliance in the PST time zone, the appliance receives the cookie at 2:00 PM PST. As a result of the difference in time, the cookie is not valid, and the connection is immediately timed-out.

Resolution: Set the time-out value for Cookie Insert persistence to 0.

A NetScaler appliance is used to load balance application servers, such as Oracle Weblogic server. To make sure that clients get persistent connections to these servers, SourceIP persistence is configured. It works as expected when a connection is made

from a computer. However, when thin clients attempt a connection through a terminal server and, as a result, the appliance receives requests from multiple clients from the same IP address (the terminal server IP address). Therefore, the connections from all thin clients are directed to the same application server. Is it possible to configure persistency for requests from individual thin clients based on the client IP address?

Cause: The NetScaler appliance receives requests from the terminal server and the source IP address of the request remains the same. As a result, the appliance cannot distinguish among the requests received from the thin clients and provide persistence according to the requests from thin clients.

Resolution: To avoid this problem, you can configure Rule persistence based on some unique parameter value for each thin client.

The NetScaler appliance is used to load balance Web Interface servers. When accessing the servers, the user receives the "State Error" error message. Additionally, when one of the Web Interface servers is shut down or not available, some of the users receive an error message.

Cause: Lack of persistence to the Web Interface servers can result in error messages when a user attempts to connect to the server.

Resolution: Citrix recommends that you specify the Cookie Insert persistence method on the NetScaler appliance when load balancing Web Interface servers.

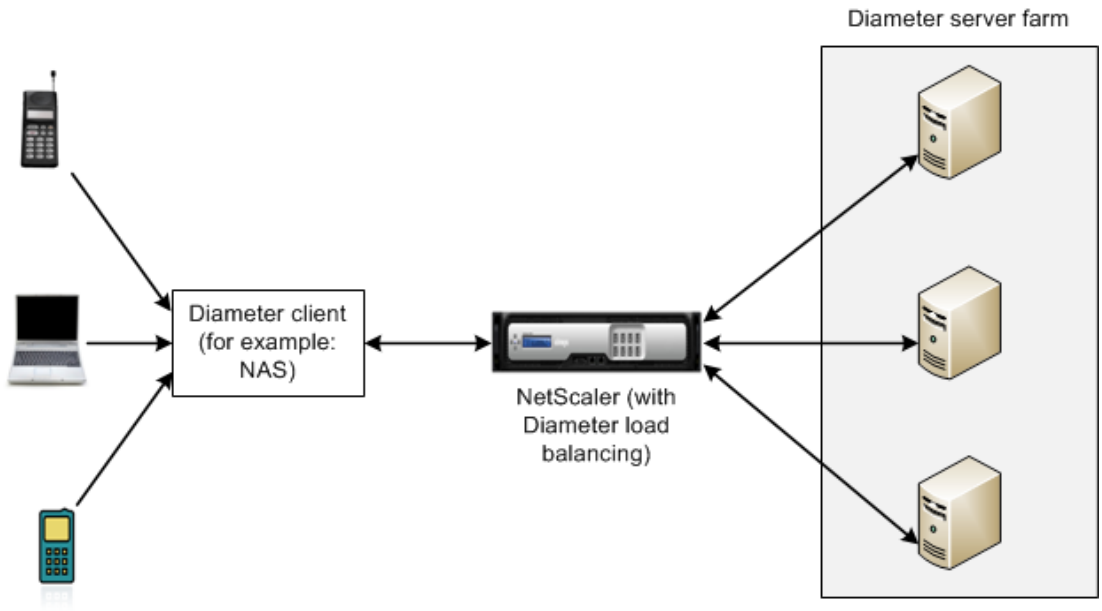
Configuring Diameter Load Balancing

The Diameter protocol is a next generation Authentication, Authorization, and Accounting (AAA) signaling protocol used mainly on mobile devices such as laptops and mobile phones. It is a peer-to-peer protocol, as opposed to the traditional client-server model used by most other protocols. However, in most Diameter deployments, the clients originates the request and the server responds to the request.

When Diameter messages are exchanged, the Diameter server usually does much more processing than does the Diameter client. With the increase in control plane signaling volume, the Diameter server becomes a bottleneck. Therefore, Diameter messages must be load balanced to multiple servers. A virtual server performing load balancing of Diameter messages provides the following benefits:

- Lighter load on Diameter servers, which translates to faster response time to end users.
- Server health monitoring and better failover capabilities.
- Better scalability in terms of server addition without changing client configuration.
- High availability.
- SSL-Diameter offloading.

The following figure shows a Diameter system in a NetScaler deployment:



A Diameter system has the following components:

- **Diameter client.** Supports Diameter client applications in addition to the base protocol. Diameter clients are often implemented in devices situated at the edge of a network and provide access control services for that network. Typical examples of Diameter clients are a Network Access Server (NAS) and the Mobile IP Foreign Agent (FA).

- **Diameter agent.** Provides relay, proxy, redirect, or translation services. The NetScaler appliance (configured with a Diameter load balancing virtual server) plays the role of a Diameter agent.

- **Diameter server.** Handles the authentication, authorization, and accounting requests for a particular realm. A Diameter server must support Diameter server applications in addition to the base protocol.

In a typical Diameter topology, when an end-user device (such as a mobile phone) needs a service, it sends a request to a Diameter client. Each Diameter client establishes a single connection (TCP connection—SCTP is not yet supported) with a Diameter server as specified by the Diameter base-protocol RFC 3588 bis. The connection is long-lived and all messages between the two Diameter nodes (client and server) are exchanged over this connection. The NetScaler uses message based load balancing .

Example

A mobile service provider uses Diameter for its billing system. When a subscriber uses a prepaid number, the Diameter client repeatedly sends requests to the server to check the available balance. The Diameter protocol establishes a connection between the client and the server, and all requests are exchanged over that connection. Connection based load balancing would be pointless, because there is only one connection. However, with the large number of messages on the connection, message based load balancing expedites the process of billing the prepaid mobile subscriber.

How Diameter Load Balancing Works

A Diameter client opens a connection to the NetScaler appliance and sends a Diameter capability exchange (CER) message. Diameter messages are composed of command codes and each command has a set of Attribute-Value Pairs (AVPs), such as Origin-Host and Host-IP-Address.

The NetScaler selects a Diameter server, opens a connection to the server, and forwards the CER message to the server. The server reads the client identity and determines that it is directly connected to the client.

The Diameter server prepares the Diameter handshake reply and sends it to the NetScaler appliance. The appliance modifies the handshake and inserts its own identity. At this point, the Diameter client determines that it is directly connected to the NetScaler (the agent).

Note: Until the Diameter handshake is complete, all Diameter request messages from the client are queued on the selected server. The packets are forwarded to the server when the handshake is complete.

Load Balancing Diameter Traffic

When a client sends a request to the NetScaler appliance, the appliance parses the request and contextually load balances it to a Diameter server on the basis of a persist AVP. The NetScaler has advertised the client identity to the server, so it does not add route entries, because the server is expecting messages directly from client.

Server initiated requests are not as frequent as client requests. Server initiated requests are similar to client initiated requests, except:

- Since messages are received from multiple servers, the NetScaler maintains the transaction state by adding a unique Hop by Hop (HbyH) number to each forwarded request message. When the message response arrives (with same HbyH number), the appliance translates this HbyH number to the HbyH number that was received on the server when the request arrived.

- NetScaler adds a route entry by putting its identity, because the client sees the NetScaler as a relay agent.

Note: If a Diameter message spans more than one packet, the NetScaler accumulates the packets in an incomplete header queue and forwards them to the server when the full message is accumulated. Similarly, if a single packet contains more than one Diameter message, the NetScaler splits the packet and forwards the messages to servers as determined by the load balancing virtual server.

Disconnecting a Session

A Disconnect Peer Request (DPR) indicates the peer's intention of closing the connection, with the reason for closing the connection. The peer replies with a DPA (TCP always provides successful DPA).

- When the NetScaler receives a DPR from the client, it broadcasts the DPR to all servers and immediately replies with a DPA to the client. The servers reply with DPAs, but the

NetScaler ignores them. The client sends a FIN, which the NetScaler broadcasts to all servers.

- When the NetScaler receives a DPR from the server, it replies with a DPA to that server alone, and does not remove the server from the reuse pool. When the server sends a FIN, the NetScaler replies with FIN/ACK and removes connections from the reuse pool.
- If the NetScaler receives a FIN from the client, it sends the client a FIN/ACK, broadcasts the FIN, and immediately removes the server connection from the reuse pool.
- If the NetScaler receives a FIN from the server, it sends a FIN/ACK and removes it from reuse pool. Any new message for this server is sent on a new connection.

Configuring Load Balancing for Diameter Traffic

To configure the NetScaler appliance to load balance Diameter traffic, you must first set the Diameter parameters on the appliance, then add the Diameter monitor, add the Diameter services, bind the services to the monitor, add the Diameter load balancing virtual server, and bind the services to the virtual server.

To configure load balancing for Diameter traffic by using the command line interface

1. Configure the Diameter parameters.

   set ns diameter -identity <string> -realm <string> -serverClosePropagation <YES|NO>

   Example

   set ns diameter -identity mydomain.org -realm org -serverClosePropagation YES

2. Add a Diameter monitor.

   add lb monitor <monitorName> DIAMETER -originHost <string> -originRealm <string>

   Example

   add lb monitor diameter_mon DIAMETER -originHost mydomain.org -originRealm org

3. Create the Diameter services.

   add service <name>@ <IP>@ DIAMETER <port>

   Example

   add service diameter_svc0 10.102.82.86 DIAMETER 3868
   add service diameter_svc1 10.102.82.87 DIAMETER 3868
   add service diameter_svc2 10.102.82.88 DIAMETER 3868
   add service diameter_svc3 10.102.82.89 DIAMETER 3868

4. Bind the Diameter services to the Diameter monitor.

   bind service <name>@ monitorName <monitorName>

   -**Example**

   bind service diameter_svc0 -monitorName diameter_mon
   bind service diameter_svc1 -monitorName diameter_mon
   bind service diameter_svc2 -monitorName diameter_mon
   bind service diameter_svc3 -monitorName diameter_mon

5. Add a Diameter load balancing virtual server with Diameter persistence.

   add lb vserver <name>@ DIAMETER <IPAddress> <port> -persistenceType DIAMETER
   -persistAVPno <positive_integer>

   Example

   add lb vserver diameter_vs DIAMETER 10.102.112.152 3868 -persistenceType DIAMETER -persistAVPno 26

6. Bind the Diameter services to the Diameter load balancing virtual server.

   bind lb vserver <name>@ <serviceName>

Example

```
bind lb vserver diameter_vs diameter_svc0
bind lb vserver diameter_vs diameter_svc1
bind lb vserver diameter_vs diameter_svc2
bind lb vserver diameter_vs diameter_svc3
```

7. Save the configuration.

   ```
   save ns config
   ```

   Note: You can also configure load balancing of Diameter traffic over SSL by using the **SSL_DIAMETER** service type.

To configure load balancing for Diameter traffic by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, click Change Diameter Parameters.
3. In the Configure Diameter Parameters dialog box, specify values for the following parameters.
   - Host Identity
   - Realm
   - Server Close Propagation
4. Click OK to configure the Diameter parameters.
5. In the navigation pane, expand Load Balancing, and then click Monitors.
6. In the details pane, click Add.
7. In the Create Monitor dialog box, create a monitor with Type as Diameter.
8. On the Special Parameters tab, enter values for Origin Host and Origin Realm.
9. In the navigation pane, expand Load Balancing, and then click Services.
10. In the details pane, click Add.
11. In the Create Service dialog box, create a service with Protocol as Diameter and bind the created Diameter monitor to this service.
12. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
13. In the details pane, click Add.
14. In the Create Virtual Server (Load Balancing) dialog box, create a load balancing virtual server with Protocol as DIAMETER and bind the created Diameter services to this virtual server.
15. On the Method and Persistence tab, select the Persistence as DIAMETER and specify a **AVP Number**.

Customizing the Hash Algorithm for Persistence across Virtual Servers

The NetScaler appliance uses hash-based algorithms for maintaining persistence across virtual servers. By default, the hash-based load balancing method uses a hash value of the IP address and port number of the service. If a service is made available at different ports on the same server, the algorithm generates different hash values. Therefore, different load balancing virtual servers might send requests for the same application to different services, breaking the pseudo-persistence.

As an alternative to using the port number to generate the hash value, you can specify a unique hash identifier for each service. For a service, the same hash identifier value must be specified on all the virtual servers. If a physical server serves more than one type of application, each application type should have a unique hash identifier.

The algorithm for computing the hash value for a service works as follows:

- By default, a global setting specifies the use of port number in a hash calculation.
- If you configure a hash identifier for a service, it is used, and the port number is not, regardless of the global setting.
- If you do not configure a hash identifier, but change the default value of the global setting so that it does not specify use of the port number, the hash value is based only on the IP address of the service.
- If you do not configure a hash identifier or change the default value of the global setting to use the port number, the hash value is based on the IP address and the port number of the service.

You can also specify hash identifiers when using the NetScaler command line to bind services to a service group. In the configuration utility, you can open a service group and add hash identifiers on the Members tab.

To change the use-port-number global setting by using the command line interface

At the command prompt, type:

set lb parameter -usePortForHashLb (YES | NO)

Example

```
> set lb parameter -usePortForHashLb NO
 Done
>show lb parameter
Global LB parameters:
```

```
        Persistence Cookie HttpOnly Flag: DISABLED
        Use port for hash LB: NO
Done
```

To change the use-port-number global setting by using the configuration utility

1. In the navigation pane, click Load Balancing.
2. In the Settings group, click Configure Load Balancing Parameters.
3. To not use the port number to generate the hash value, clear the Use Port for Hash Based LB Methods check box.
4. Click OK.
5. Open the Configure Load Balancing Parameters dialog box and verify the setting you just configured.

To create a new service and specify a hash identifier for a service by using the command line interface

At the command prompt, type the following commands to set the hash ID and verify the setting:

add service < name > (< ip > |< serverName >) < serviceType > < port > -hashId < positive_integer >

show service <name>

Example

```
> add service flbkng 10.101.10.1 http 80 -hashId 12345
 Done
>show service flbkng
        flbkng (10.101.10.1:80) - HTTP
        State: DOWN
        Last state change was at Thu Nov  4 10:14:52 2010
        Time since last state change: 0 days, 00:00:15.990
        Server Name: 10.101.10.1
        Server ID : 0   Monitor Threshold : 0

        Down state flush: ENABLED
        Hash Id: 12345

1)      Monitor Name: tcp-default
                State: DOWN     Weight: 1
```

```
Done
```

To specify a hash identifier for an existing service by using the command line interface

Type the set service command, the name of the service, and **-hashID** followed by the ID value.

To specify a hash identifier while adding a service group member

To specify a hash identifier for each member to be added to the group and verify the setting, at the command prompt, type the following commands (Be sure to specify a unique hashID for each member.):

bind servicegroup <serviceGroupName> <memberName> <port> -hashId <positive_integer>

show servicegroup <serviceGroupName>

Example

```
 bind servicegroup http_svc_group 10.102.27.153 80 -hashId 2222222

>show servicegroup SRV
      SRV - HTTP
      State: ENABLED  Monitor Threshold : 0
      …

      1)       1.1.1.1:80   State: DOWN    Server Name: 1.1.1.1    Server ID: 123  Weight: 1
      Hash Id: 32211

            Monitor Name: tcp-default      State: DOWN
      …

      2)       2.2.2.2:80   State: DOWN    Server Name: 2.2.2.2    Server ID: 123  Weight: 1
      Hash Id: 12345

            Monitor Name: tcp-default      State: DOWN
      …
Done
```

Parameters for configuring a service

name

Name of the service. This alphanumeric string is required. The name must not exceed 127 characters, and the leading character must be a number or a letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

ip

IP address of the server that is associated with the service, in either IPv4 or IPv6 format.

serverName

Name of the server that is associated with the service. The name must not exceed 127 characters, and the leading character must be a number or a letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serviceType

Protocol supported by the service. Possible values: HTTP, FTP, TCP, UDP, SSl, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, DNS_TCP, ADNS_TCP, RDP, RADIUS.

port

The port number used for the service.

hashId

The hash identifier for the service. Must be unique for each service. Minimum value: 1, Maximum value: 4294967295.

To specify a hash identifier for a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and click Services.
2. In the details pane, do one of the following:
   - To create a new service, click Add.
   - To modify an existing service, select the service and then click Open.
3. In the Create Service or Configure Service dialog box, specify values for the following parameters, which correspond to the parameters described in "Parameters for adding a service," as shown:
   - ServiceName*—name
   - Server*—ip or serverName
   - Protocol*—serviceType
   - Port*—port
4. Click the Advanced tab and then scroll down in the dialog box.
5. In the Hash ID box, type a unique hash ID value.
6. Click Create.
7. Open the service and verify the settings you just configured.

To specify a hash identifier for an already configured service group member by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.
2. Select a service group, and then click Open.
3. On the Members tab, under Configured Members, in the row of the member for which you want to specify a hash ID value, double-click the space in the Hash ID column.
4. Type a unique hash ID value.
5. Click OK.
6. Open the service group and verify the hash IDs of the service group members you just configured.

Configuring the Redirection Mode

The redirection mode configures the method used by a virtual server to determine where to forward incoming traffic. The NetScaler appliance supports the following redirection modes:

- IP-Based forwarding (the default)
- MAC-Based forwarding

You can configure MAC-Based forwarding on networks that use direct server return (DSR) topology, link load balancing, or firewall load balancing. For more information on MAC-Based forwarding, see Networking.

To configure the redirection mode by using the command line interface

At the command prompt, type:

set lb vserver <name>@ -m <RedirectionMode>

Example

set lb vserver Vserver-LB-1 -m MAC

Parameter for configuring the redirection mode

m

The load balancing redirection mode. Possible Values: IP, MAC. Default: IP.

If set to IP, the destination IP address of the request is changed to the IP address of the server to which you are redirecting traffic, and the traffic is then forwarded to that server.

If set to MAC, the destination MAC address is changed to the MAC address of the server to which you are redirecting traffic, and the traffic is then forwarded to that server. With this setting, the destination IP address of the traffic is not changed.

To configure the redirection mode by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure the redirection mode, and then click Open.
3. On the Advanced tab, under Redirection Mode, click either IP-Based or MAC-Based.
4. Click OK.

Configuring per-VLAN Wildcarded Virtual Servers

If you want to configure load balancing for traffic on a specific virtual local area network (VLAN), you can create a wildcarded virtual server with a listen policy that restricts it to processing traffic only on the specified VLAN.

To configure a wildcarded virtual server that listens to a specific VLAN by using the command line interface

At the command prompt, type the following commands to configure a wildcarded virtual server that listens to a specific VLAN and verify the configuration:

- add lb vserver <name> <serviceType> IPAddress * Port * -listenpolicy <expression> [-listenpriority <positive_integer>]
- show vserver

Example

add lb vserver Vserver-LB-vlan1 ANY -listenpolicy "CLIENT.VLAN.ID.EQ(2)" -listenpriority 10

show vserver Vserver-LB-vlan1

Parameters for configuring per-VLAN wildcarded virtual servers

name

Name of the virtual server. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

IPAddress

IP address of the virtual server. For wildcarded virtual servers bound to VLANs, this is always *

serviceType

Behavior of the service. Select one of the following service types: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, DNS_TCP, ADNS_TCP, RADIUS, MYSQL, MSSQL, and RDP.

port

Port on which the virtual server listens for client connections. The port number must be in the range 0-65535. For wildcarded virtual servers bound to VLANs, the setting is normally *.

listenpolicy

Use this parameter to specify the listen policy for LB Vserver. The string can be either an existing expression name (configured using add policy expression command) or else it can be an in-line expression with a maximum of 1500 characters.

listenpriority

The priority assigned to the listen policy. This can be any positive integer. Priority is evaluated in reverse order; the lower the number, the higher the priority assigned to the listen policy.

rule

The policy rule to use to identify the VLAN that you want this virtual server to listen to. This rule is:

- CLIENT.VLAN.ID.EQ(<integer>)
- For <integer>, substitute the ID number assigned to the VLAN.

To configure a wildcarded virtual server that listens to a specific VLAN by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, do one of the following:
   - To create a new virtual server, click Add.
   - To modify an existing virtual server, select the virtual server, and then click Open.
3. In the Create Virtual Server or Configure Virtual Server dialog box, on the Services tab, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring per-VLAN wildcarded virtual servers” as shown:
   - Name*—name
   - Protocol*—serviceType
   - IP address*—IPAddress
   - Port—port

   *A required parameter
4. In the Advanced tab, expand Listen Policy, and then specify values for the following parameters, which correspond to parameters described in “Parameters for configuring per-VLAN wildcarded virtual servers” as shown:
   - Listen Priority*—listenpriority
   - Listen Policy Rule*—rule

   *A required parameter
5. Click Create or OK, depending on whether you are creating a new virtual server or modifying an existing virtual server.
6. Click Close. The virtual server that you created now appears in the Virtual Servers page.
7. To remove a virtual server, in the Virtual Servers pane select the virtual server, and then click Remove.

After you have created this virtual server, you bind it to one or more services as described in Setting Up Basic Load Balancing.

Assigning Weights to Services

In a load balancing configuration, you assign weights to services to indicate the percentage of traffic that should be sent to each service. Services with higher weights can handle more requests; services with lower weights can handle fewer requests. Assigning weights to services allows the NetScaler appliance to determine how much traffic each load balanced server can handle, and therefore more effectively balance load.

Note: If you use a load balancing method that supports weighting of services (for example, the round robin method), you can assign a weight to the service.

The following table describes the load balancing methods that support weighting, and briefly describes the manner in which weighting affects how a service is selected for each one.

Load Balancing Methods	Service Selection with Weights
Round Robin	The virtual server prioritizes the queue of available services such that services with the highest weights come to the front of the queue more frequently than those with the lowest weights and receive proportionately more traffic. For a complete description, see The Round Robin Method.
Least Connection	The virtual server selects the service with the best combination of fewest active transactions and highest weight. For a complete description, see The Least Connection Method.
Least Response Time and Least Response Time Method using Monitors	The virtual server selects the service with the best combination of fewest active transactions and fastest average response time. For a complete description, see The Least Response Time Method.
Least Bandwidth	The virtual server selects the service with the best combination of least traffic and highest bandwidth. For a complete description, see The Least Bandwidth Method.
Least Packets	The virtual server selects the service with the best combination of fewest packets and highest weight. For a complete description, see The Least Packets Method.
Custom Load	The virtual server selects the service with the best combination of lowest load and highest weight. For a complete description, see The Custom Load Method.

Hashing methods and Token method	Weighting is not supported by these load balancing methods.

To configure a virtual server to assign weights to services by using the command line interface

At the command prompt, type:

set lb vserver <name>@ -weight <Value> <ServiceName>

Example

set lb vserver Vserver-LB-1 -weight 10 Service-HTTP-1

Parameter for setting weights

weight

Weight to be assigned to the specified service. The minimum value is 1 and the maximum value is 100.

To configure a virtual server to assign weights to services by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server, and then click Open.
3. On the Services tab, in the Weights spin box, type or select the weight to assign to the service (for example, 10).
4. Click OK.

Configuring the Microsoft SQL Server Version Setting

You can specify the version of Microsoft® SQL Server® for a load balancing virtual server that is of type MSSQL. The version setting is recommended if you expect some clients to not be running the same version as your Microsoft SQL Server product. The version setting provides compatibility between the client-side and server-side connections by ensuring that all communication conforms to the server's version.

To set the Microsoft SQL Server version parameter by using the command line interface

At the command prompt, type the following commands to set the Microsoft SQL Server version parameter for a load balancing virtual server and verify the configuration:

- set lb vserver <name> -mssqlServerVersion <mssqlServerVersion>
- show lb vserver <name>

Example

```
> set lb vserver myMSSQLvip -mssqlServerVersion 2008R2
 Done
> show lb vserver myMSSQLvip
    myMSSQLvip (190.0.2.12:1433) - MSSQL    Type: ADDRESS
 . . .
 . . .
    MSsql Server Version: 2008R2
    . . .
    . . .
 Done
>
```

Parameters for configuring the MS SQL Server version setting

name

The name of the virtual server for which you want to configure the MS SQL Server version setting.

mssqlServerVersion

The version of MS SQL Server that you are using. Following are the possible values:

- `70`, for Microsoft SQL Server 7.0
- `2000`, for Microsoft SQL Server 2000
- `2000SP1`, for Microsoft SQL Server 2000 Service Pack 1 (SP1)
- `2005`, for Microsoft SQL Server 2005
- `2008`, for Microsoft SQL Server 2008
- `2008R2`, for Microsoft SQL Server 2008 R2

To set the Microsoft SQL Server version parameter by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure the setting, and then click Open.
3. In the Configure Virtual Server dialog box, do the following:
   a. In the advanced tab, click MsSql.
   b. In the Server Version list, select the version of your Microsoft SQL Server product.
   c. Click Create or OK, and then click Close.

Protecting the Load Balancing Configuration against Failure

When a load balancing virtual server fails, or when the virtual server is unable to handle excessive traffic, the load balancing setup can fail. You can protect your load balancing setup against failure by configuring the NetScaler appliance to redirect excess traffic to an alternate URL, configuring a backup load balancing virtual server, and configuring stateful connection failover.

Redirecting Client Requests to an Alternate URL

In the event that a load balancing virtual server of type HTTP or type HTTPS goes DOWN or is disabled, you can redirect requests to an alternate URL by using an HTTP 302 redirect. The alternate URL can provide information about the status of the server.

You can redirect to a page on the local server or a remote server. You can redirect to a relative URL or an absolute URL. If you configure a redirect to a relative URL consisting of a domain name with no path, the NetScaler appliance appends the path of the incoming URL to the domain. If you use an absolute URL, the HTTP redirect is sent to that URL with no modification.

Note: If a load balancing virtual server is configured with both a backup virtual server and a redirect URL, the backup virtual server takes precedence over the redirect URL. A redirect is used only when both the primary and backup virtual servers are DOWN.

To configure a virtual server to redirect the client request to a URL by using the command line interface

At the command prompt, type:

set lb vserver <vServerName> -redirectURL <URLValue>

Example

set lb vserver Vserver-LB-1 -redirectURL http://www.newdomain.com/mysite/maintenance

Parameters for Redirecting Client Requests to an Alternative URL

redirectURL

URL to which traffic is redirected when the load balancing virtual server is unavailable. This URL length must not exceed 127 characters.

Note: The domain specified in the URL must not match the domain specified in the domain name argument of a content switching policy. If the same domain is specified in both arguments, the request is redirected continuously to the same unavailable load balancing virtual server.

To configure a virtual server to redirect the client request to a URL by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure redirect URL, and then click Open.
3. On the Advanced tab, in the Redirect URL text box, type the URL (for example, http://www.newdomain.com/mysite/maintenance).
4. Click OK.

Configuring a Backup Load Balancing Virtual Server

You can configure the NetScaler appliance to direct requests to a backup virtual server in the event that the primary load balancing virtual server is DOWN or unavailable. The backup virtual server is a proxy and is transparent to the client. The appliance can also send a notification message to the client regarding the site outage.

You can configure a backup load balancing virtual server when you create it, or you can change the optional parameters of an existing virtual server. You can also configure a backup virtual server for an existing backup virtual server, thus creating cascading backup virtual servers. The maximum depth of cascading backup virtual servers is 10.

If you have multiple virtual servers that connect to two servers, you have a choice for what happens if the primary virtual server goes DOWN and then comes back up. The default behavior is for the primary virtual server to resume its role as primary. However, you may want to configure the backup virtual server to remain in control in the event that it takes over. For example, you may want to sync updates on the backup virtual server to the primary virtual server and then manually force the original primary server to resume its role. In this case, you can designate the backup virtual server to remain in control in the event that the primary virtual server goes DOWN and then comes back up.

You can configure a redirect URL on the primary load balancing virtual server as a fallback for when both the primary and the backup virtual servers are DOWN or have reached their threshold for handling requests. When services bound to virtual servers are OUT OF SERVICE, the appliance uses the redirect URL.

Note: If a load balancing virtual server is configured with both a backup virtual server and a redirect URL, the backup virtual server takes precedence over the redirect URL. A redirect is used only when the primary and backup virtual servers are down.

To set a backup virtual server by using the command line interface

At the command prompt, type:

set lb vserver <vServerName> -backupVserver <BackupVServerName> [-disablePrimaryOnDown]

Example

set lb vserver Vserver-LB-1 -backupVserver Vserver-LB-2 -disablePrimaryOnDown

Parameters for configuring a backup load balancing virtual server

backupVserver

Name of the backup virtual server. You can create a virtual server and specify the name, IP address, port, and type as described in “Creating a Virtual Server,” on page 38. You can use the name of the virtual server as a backup virtual server

disablePrimaryOnDown

Configures the backup virtual server to remain in control, after it takes over, until you manually reenable the primary virtual server.

To set a backup virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure the backup virtual server, and then click Open.
3. On the Advanced tab, in the Backup Virtual Server list, select the backup virtual server.
4. If you want the backup virtual server to remain in control until you manually re-enable the primary virtual server even if the primary virtual server comes back up, select the Disable Primary When Down check box.
5. Click OK.

Diverting Excess Traffic to a Backup Virtual Server

In addition to taking over for a primary virtual server when it becomes unavailable, a backup load balancing virtual server can handle excess traffic when the primary virtual server reaches its limit. To set this up, you configure the spillover option to divert new connections to the backup virtual server when the number of connections to the primary virtual server exceeds the threshold. You can allow the NetScaler appliance to calculate the threshold dynamically, or you can configure the value manually.

When spillover is configured, the appliance compares the number of established TCP connections on the primary virtual server with the threshold value. When the number of connections reaches the threshold, it diverts new connections to the backup virtual server.

You can configure persistence with spillover. When persistence is configured, connections that are diverted to the backup virtual server are not moved back to the primary virtual server after the number of connections on it drops below the threshold. Instead, the primary virtual server accepts new client connections.

If the backup virtual server reaches its own threshold and is unable to accept additional connections, the appliance diverts all requests to the redirect URL. If a redirect URL is not configured on the primary virtual server, any requests over the threshold are dropped.

Note: With RTSP virtual servers, the appliance uses only data connections for spillover. If the backup RTSP virtual server is not available, the requests are redirected to an RTSP URL and an RTSP redirect message is sent to the client.

To configure a primary virtual server to divert new connections to a backup virtual server by using the command line interface

At the command prompt, type:

set lb vserver <vServerName> -soMethod <spillOverType> -soThreshold <positiveInteger> -soPersistence ENABLED -soPersistenceTimeout <positiveInteger>

Example

set lb vserver Vserver-LB-1 -soMethod Connection -soThreshold 1000 -soPersistence enabled -soPersistenceTi

Parameters diverting excess traffic to a backup virtual server

soMethod

The spillover method to use for diverting traffic to the backup virtual server when the primary virtual server reaches the spillover threshold. Available settings function as follows:

- CONNECTION. Spillover occurs when the number of client connections at the virtual server exceeds the static threshold value (the value of the Threshold parameter).
- DYNAMICCONNECTION. Spillover occurs when the number of client connections at the virtual server exceeds a dynamically calculated threshold. The dynamic threshold is the sum of the maximum client (Max Clients) settings of the bound services that are up. Do not specify a spillover threshold for this setting, because the threshold is implied by the Max Clients settings of bound services.
- BANDWIDTH. Spillover occurs when the bandwidth consumed by the virtual server's incoming and outgoing traffic exceeds the static threshold value.
- HEALTH. Spillover occurs when the percentage of weights of the services that are UP drops below the static threshold value. For example, if services svc1, svc2, and svc3 are bound to a virtual server, with weights 1, 2, and 3, and the spillover threshold is 50%, spillover occurs if svc1 and svc3 or svc2 and svc3 transition to DOWN.
- NONE. Spillover does not occur.

soThreshold

Threshold at which spillover occurs. Specify an integer for the CONNECTION spillover method, a bandwidth value in kilobits per second for the BANDWIDTH method (do not enter the units), or a percentage for the HEALTH method (do not enter the percentage symbol).

soPersistence

If spillover occurs, maintain source IP address based persistence for both primary and backup virtual servers. Possible values: ENABLED, DISABLED. Default: DISABLED.

soPersistenceTimeout

Time-out for spillover persistence, in minutes. Minimum value: 2. Maximum value: 1440. Default: 2.

To set a primary virtual server to divert new connections to a backup virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure the spillover, and then click Open.
3. On the Advanced tab, in the Method list, select the type of threshold, and in Threshold text box, type the threshold value.
4. Under Spillover, select the Persistence check box, and in Persistence Time-out (min) text box type the time-out.
5. Click OK.

Configuring Connection-Based Spillover

You can use connection-based spillover to configure a maximum threshold for the number of active client connections on a virtual server. When the client connections exceed the configured threshold limit, new client connections are diverted to the backup virtual server.

To configure connection-based spillover, see Diverting Excess Traffic to a Backup Virtual Server.

Note: Global Server Load Balancing (GSLB) virtual servers do not support connection-based spillover.

Configuring Dynamic Spillover

When you configure dynamic spillover, if the number of client connections to the primary load balancing virtual server exceeds the sum of the maximum client values, new connections are diverted to the backup virtual server.

To configure dynamic spillover, you must first enable it on the primary virtual server. Next, you configure each service that is bound to that virtual server with appropriate maximum client values for that service. Different services can have different maximum client values. If the value for maximum client is set to 0, the spillover limit is treated as infinity, and spillover never occurs.

Note: Content-based virtual servers do not support dynamic spillover.

To configure dynamic spillover, see Diverting Excess Traffic to a Backup Virtual Server.

Configuring Bandwidth-Based Spillover

With bandwidth-based spillover, when the bandwidth used by the primary load balancing virtual server exceeds the specified bandwidth threshold value, the NetScaler appliance diverts new connections to the backup virtual server. You can also configure the backup virtual server with a threshold value. When the threshold for the backup virtual server is reached, the appliance diverts new client connections to the next backup virtual server.

To configure bandwidth-based spillover, see Diverting Excess Traffic to a Backup Virtual Server.

Connection Failover

Connection failover helps prevent disruption of access to applications deployed in a distributed environment. In a NetScaler High Availability (HA) setup, *connection failover* (or *connection mirroring-CM*) refers to keeping active an established TCP or UDP connection when a failover occurs. The new primary NetScaler appliance has information about the connections established before the failover and continues to serve those connections. After failover, the client remains connected to the same physical server. The new primary appliance synchronizes the information with the new secondary appliance by using the SSF framework. If the L2Conn parameter is set, Layer 2 connection parameters are also synchronized with the secondary.

You can set up connection failover in either stateless or stateful mode. In the stateless connection failover mode, the HA nodes do not exchange any information about the connections that are failed over. This method has no runtime overhead.

In the stateful connection failover mode, the primary appliance synchronizes the data of the failed-over connections with the new secondary appliance.

How Connection Failover Works on NetScaler Appliances

In stateless connection failover, the new primary appliance tries to re-create the packet flow according to the information contained in the packets it receives.

In stateful failover, to maintain current information about the mirrored connections, the primary appliance sends messages to the secondary appliance. The secondary appliance maintains the data related to the packets but uses it only in the event of a failover. If a failover occurs, the new primary (old secondary) appliance starts using the stored data about the mirrored connections and accepting traffic. During the transition period, the client and server may experience a brief disruption and retransmissions.

Note:

Verify that the primary appliance is able to authorize itself on the secondary appliance. To verify correct configuration of the passwords, use the show rpcnode command from command line or use the RPC option of the Network menu from the configuration utility.

A basic HA configuration with connection failover contains the entities shown in the following figure.

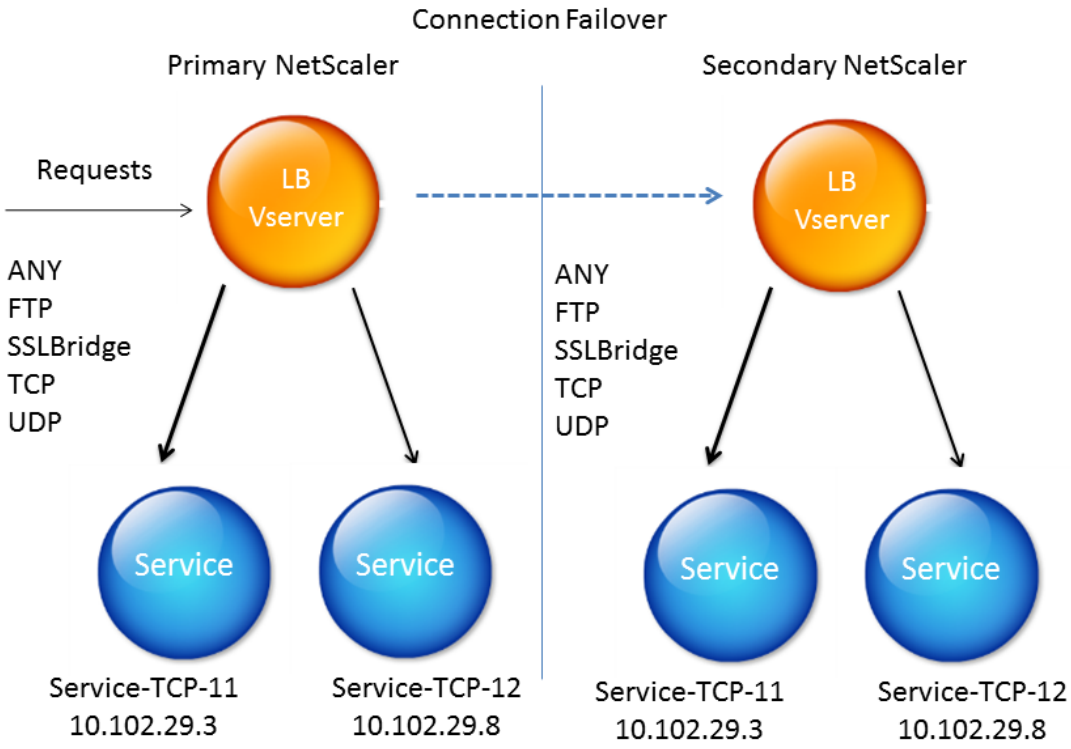


Figure 1. Connection Failover Entity Diagram

Supported Setup

Connection failover can be configured only on load balancing virtual servers. It cannot be configured on content-switching virtual servers.

The following table describes the setup supported for connection failover.

Table 1. Connection Failover - Supported Setup

Setting	Stateless	Stateful
Service type	ANY.	ANY, UDP, TCP, FTP, SSL_BRIDGE.
Load balancing methods	All methods supported for the service type ANY. However, if Source IP persistence is not set, the SRCIPSRCPORTHASH method must be used.	All methods applicable to the supported service types.

Persistence types	SOURCEIP persistence.	All types applicable to the supported service types are supported.
USIP	Must be ON.	No restriction. It can be ON or OFF.
Service bindings	Service can be bound to only one virtual server.	Service can be bound to one or more virtual servers.
Internet Protocol (IP) versions	IPv4 and IPv6	IPV4
Redundancy support	Clustering and high availability	High availability

Features Affected by Connection Failover

The following table lists the features affected if connection failover is configured.

Table 2. How Connection Failover Affects NetScaler Features

Feature	Impact of Connection Failover
SYN protection	For any connection, if a failover occurs after the NetScaler issues SYN-ACK but before it receives the final ACK, the connection is not supported by connection failover. The client must reissue the request to establish the connection.
Surge protection	If the failover occurs before a connection with the server is established, the new primary NetScaler tries to establish the connection with the server. It also retransmits all the packets held in the course of surge protection.
Access down	If enabled, the access-down functionality takes precedence over connection failover.
Application Firewall™	The Application Firewall feature is not supported.
INC	Independent network configuration is not supported in the high availability (HA) mode.
TCP buffering	TCP buffering is not compatible with connection mirroring.
Close on response	After failover, the NATPCBs may not be closed on response.
IPv6 virtual servers	Not yet supported.

Configuring Connection Failover

You can configure connection failover on a load balancing virtual server.

To configure connection failover by using the command line interface

At the command prompt, type:

set lb vserver <vServerName> -connFailover <Value>

Example

set lb vserver Vserver-LB-1 -connFailover stateful

Parameters for configuring connection failover

connFailover

State of connection failover on the virtual server. Valid values: STATELESS, STATEFUL, DISABLE. Default: DISABLE.

To configure connection failover by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the Load Balancing Virtual Servers pane, select the virtual server for which you want to configure connection failover, and click Open.
3. On the Advanced tab, in the Connection Failover drop-down list, select Stateful.
4. Click OK.

Disabling Connection Failover

When connection failover is disabled on a virtual server, the resources allocated to the virtual server are freed.

To disable a connection failover by using the command line interface

At the command prompt, type:

set lb vserver <vServerName> -connFailover <Value>

Example

set lb vserver Vserver-LB-1 -connFailover disable

To disable a connection failover by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the Load Balancing Virtual Servers pane, select the virtual server for which you want to configure a connection failover and click Open.
3. On the Advanced tab, in the Connection Failover drop-down list box, select Disable.
4. Click OK.

Flushing the Surge Queue

When a physical server receives a surge of requests, it becomes slow to respond to the clients that are currently connected to it, which leaves users dissatisfied and disgruntled. Often, the overload also causes clients to receive error pages. To avoid such overloads, the NetScaler appliance provides features such as surge protection, which controls the rate at which new connections to a service can be established.

The appliance does connection multiplexing between clients and physical servers. When it receives a client request to access a service on a server, the appliance looks for an already established connection to the server that is free. If it finds a free connection, it uses that connection to establish a virtual link between the client and the server. If it does not find an existing free connection, the appliance establishes a new connection with the server, and establishes a virtual link between client and the server. However, if the appliance cannot establish a new connection with the server, it sends the client request to a surge queue. If all the physical servers bound to the load balancing or content switching virtual server reach the upper limit on client connections (max client value, surge protection threshold or maximum capacity of the service), the appliance cannot establish a connection with any server. The surge protection feature uses the surge queue to regulate the speed at which connections are opened with the physical servers. The appliance maintains a different surge queue for each service bound to the virtual server.

The length of a surge queue increases whenever a request comes for which the appliance cannot establish a connection, and the length decreases whenever a request in the queue gets sent to the server or a request gets timed out and is removed from the queue.

If the surge queue for a service or service group becomes too long, you may want to flush it. You can flush the surge queue of a specific service or service group, or of all the services and service groups bound to a load balancing virtual server. Flushing a surge queue does not affect the existing connections. Only the requests present in the surge queue get deleted. For those requests, the client has to make a fresh request.

You can also flush the surge queue of a content switching virtual server. If a content switching virtual server forwards some requests to a particular load balancing virtual server, and the load balancing virtual server also receives some other requests, when you flush the surge queue of the content switching virtual server, only the requests received from this content switching virtual server are flushed; the other requests in the surge queue of the load balancing virtual server are not flushed.

Note: You cannot flush the surge queues of cache redirection, authentication, VPN or GSLB virtual servers or GSLB services.

Note: Do not use the Surge Protection feature if Use Source IP (USIP) is enabled.

To flush a surge queue by using the command line interface

The flush ns surgeQ command works in the following manner:

- You can specify the name of a service, service group, or virtual server whose surge queue has to be flushed.
- If you specify a name while executing the command, surge queue of the specified entity will be flushed. If more than one entity has the same name, the appliance flushes surge queues of all those entities.
- If you specify the name of a service group, and a server name and port while executing the command, the appliance flushes the surge queue of only the specified service group member.
- You cannot directly specify a service group member (<serverName> and <port>) without specifying the name of the service group (<name>) and you cannot specify <port> without a <serverName>. Specify the <serverName> and <port> if you want to flush the surge queue for a specific service group member.
- If you execute the command without specifying any names, the appliance flushes the surge queues of all the entities present on the appliance.
- If a service group member is identified with a server name, you must specify the server name in this command; you cannot specify its IP address.

At the command prompt, type:

flush ns surgeQ [-name <name>] [-serverName <serverName> <port>]

Examples

1.
flush ns surgeQ –name SVC1ANZGB –serverName 10.10.10.1 80
The above command flushes the surge queue of the service or virtual server that is named SVC1ANZGB and h
2.
flush ns surgeQ
The above command flushes all the surge queues on the appliance.

Parameters for flushing a surge queue

name

Name of a virtual server, service or service group

serverName

Name of a service group member

To flush a surge queue by using the configuration utility

1. In the navigation pane, expand Load Balancing.
2. To select an entity, do one of the following:
   - To flush the surge queue of a virtual server, click Virtual Servers, and then select the virtual server.
   - To flush the surge queue of a service, click Services, and then select the service.
   - To flush the surge queue of all the members in a service group, click Service Groups, and then select the service group.
   - To flush the surge queue of a specific member in a service group, click Service Groups, and in the action pane, click Manage Members. In the Manage Members of a Service Group dialog box, select the service group member.

   Note: You can select multiple entities in any window.

   Note: To flush the surge queue of a content switching virtual server, in Steps 1 and 2, expand Content Switching, and then select a virtual server.
3. In the action pane, click Flush Surge Queue.
4. Click OK.

   Note: On the appliance, if there are other entities with the same name as you selected, you are alerted that the surge queues of those entities would also be flushed. Take an appropriate action.

Managing a Load Balancing Setup

An existing Load Balancing setup does not require a great deal of work to maintain as long as it is unchanged, but most do not remain unchanged for long. Increasing load requires new load-balanced servers and eventually new NetScaler appliances, which must be configured and added to the existing setup. Old servers wear out and need to be replaced, requiring removal of some servers and addition of others. Upgrades to your networking equipment or changes to topology may also require modifications to your load balancing setup. Therefore, you will need to perform operations on server objects, services, and virtual servers. The Visualizer can display your configuration graphically, and you can perform operations on the entities in the display. You can also take advantage of a number of other features that facilitate management of the traffic through your load balancing setup.

Managing Server Objects

During basic load balancing setup, when you create a service, a server object with the IP address of the service is created, if one does not already exist. If you prefer for your service objects named with domain names rather than IP addresses, you might also have created one or more server objects manually. You can enable, disable, or remove any server object.

When you enable or disable a server object, you enable or disable all services associated with the server object. When you refresh the NetScaler appliance after disabling a server object, the state of its service appears as OUT OF SERVICE. If you specify a wait time when disabling a server object, the server object continues to handle established connections for the specified amount of time, but rejects new connections. If you remove a server object, the service to which it is bound is also deleted.

To enable a server by using the command line interface

At the command prompt, type:

enable server <name>@

Example

enable server 10.102.29.5

To enable a server object by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Servers.
2. In the details pane, select the server that you want to enable, and then click Enable.
3. In the Enable dialog box, click Yes.

To disable a server object by using the command line interface

At the command prompt, type:

disable server <name>@ <delay>

Example

disable server 10.102.29.5 30

Wait time parameter

delay

The time, in seconds, after which the server object is marked DOWN.

To disable a server object by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Servers.
2. In the details pane, select the server that you want to disable, and then click Disable.
3. In the Wait Time dialog box, type the wait time after which the server is to be disabled (for example 30).
4. Click Enter.

To remove a server object by using the command line interface

At the command prompt, type:

rm server <name>@

Example

rm server 10.102.29.5

To remove a server object by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Servers.
2. In the details pane, select the server that you want to remove, and then click Remove.
3. In the Remove dialog box, click Yes.

Managing Services

Services are enabled by default when you create them. You can disable or enable each service individually. When disabling a service, you normally specify a wait time during which the service continues to handle established connections, but rejects new ones, before shutting down. If you do not specify a wait time, the service shuts down immediately. During the wait time, the service's state is OUT OF SERVICE.

You can remove a service when it is no longer used. When you remove a service, it is unbound from its virtual server and deleted from the NetScaler configuration.

To enable a service by using the command line interface

At the command prompt, type:

enable service <name>

Example

enable service Service-HTTP-1

To enable a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service that you want to enable (for example, Service-HTTP-1), and click Enable.
3. In the Enable dialog box, click Yes.

To disable a service by using the command line interface

At the command prompt, type:

disable service <name>@ <DelayInSeconds>

Example

disable service Service-HTTP-1 30

Wait Time Parameter

delay

The time, in seconds, after which the service is marked DOWN.

To disable a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service that you want to disable (for example, Service-HTTP-1), and then click Disable.
3. In the Wait Time dialog box, type the wait time after which the service is to be disabled (for example, 30).
4. Click Enter.

To remove a service by using the command line interface

At the command prompt, type:

rm service <name>@

Example

rm service Service-HTTP-1

To remove a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service that you want to remove (for example, Service-HTTP-1), and then click Remove.
3. In the Remove dialog box, click Yes.

Managing a Load Balancing Virtual Server

Virtual servers are enabled by default when you create them. You can disable and enable virtual servers manually. If you disable a virtual server, the virtual server's state appears as OUT OF SERVICE. When this happens, the virtual server terminates all connections, either immediately or after allowing existing connections to complete, depending on the setting of the downStateFLush parameter. If downStateFLush is ENABLED (default), all the connections are flushed. If DISABLED, the virtual server continues to serve requests on existing connections.

You remove a virtual server only when you no longer require the virtual server. Before you remove it, you must unbind all services from it.

To enable a virtual server by using the command line interface

At the command prompt, type:

enable lb vserver <name>@

Example

enable lb vserver Vserver-LB-1

To enable a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to enable, and click Enable.
3. In the Enable dialog box, click Yes.

To disable a virtual server by using the command line interface

At the command prompt, type:

disable vserver

Example

disable lb vserver Vserver-LB-1

To disable a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to disable, and then click Disable.
3. In the Disable dialog box, click Yes.

Note: In the disabled state, a virtual server continues to exist on the network. The NetScaler appliance continues to respond to address resolution protocol (ARP) and Internet control message protocol (ICMP) requests directed to the IP address of the virtual server.

To unbind a service from a virtual server by using the command line interface

At the command prompt, type:

unbind lb vserver <name>@ <serviceName>

Example

unbind lb vserver Vserver-LB-1 Service-HTTP-1

To unbind a service from a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server from which you want to unbind a service, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, in the Services tab, clear the Active check box next to the service that you want to unbind from the virtual server.
4. Click OK.

To remove a virtual server by using the command line interface

At the command prompt, type:

rm lb vserver <name>@

Example

rm lb vserver Vserver-LB-1

To remove a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to remove, and then click Remove.
3. In the Remove dialog box, click Yes.

The Load Balancing Visualizer

The Load Balancing Visualizer is a tool that you can use to view and modify the load balancing configuration in graphical format. Following is an example of the Visualizer display

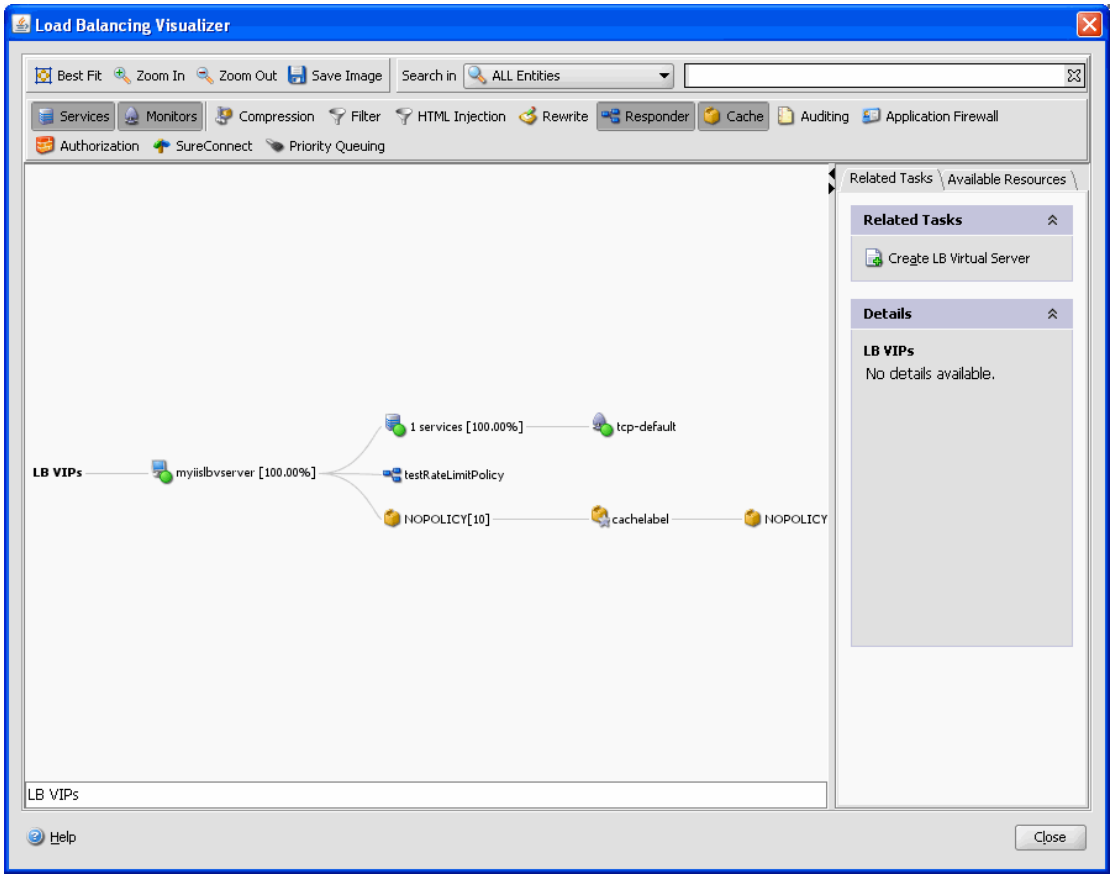


Figure 1. Load Balancing Visualizer Display

You can use the visualizer to view the following:

- The services and service groups that are bound to a virtual server.
- The monitors that are bound to each service.
- The policies that are bound to the virtual server.
- The policy labels, if configured.
- Configuration details of any displayed element.
- Load balancing virtual server statistics.
- Statistical information such as the number of requests received per second by the virtual server and the number of hits per second for rewrite, responder, and cache

policies.

- A comparative list of all the parameters whose values either differ or are not defined across service containers.

You can also use the Visualizer to add and bind new objects, modify existing ones, and enable or disable objects. Most configuration elements displayed in the Visualizer appear under the same names as in other parts of the configuration utility. However, unlike the rest of the configuration utility, the Visualizer groups services that have the same configuration details and monitor bindings into an entity called a *service container*.

A service container is set of similar services and service groups that are bound to a single load balancing virtual server. Next to the service container is a number that shows the number of services in the group. The services in the container have the same properties, with the exception of the name, IP address, and port, and their monitor bindings should have the same weight and binding state. When you bind a new service to a virtual server, it is placed into an existing container if its configuration and monitor bindings match those of other services; otherwise, it is placed in its own container.

The service container display can help you troubleshoot your configuration if something is not functioning as you expect. More than one container for a particular virtual server is an indication that something is wrong with the configuration of that virtual server and its services. To correct the problem, you must first identify the container that has the desired configuration. You can do so by using the Service Attributes Diff feature, described below. After you identify the container, you right-click the container and click Apply Configuration.

The following procedures provide only basic steps for using the Visualizer. Because the Visualizer duplicates functionality in other areas of the Load Balancing feature, other methods of viewing or configuring all of the settings that can be configured in the Visualizer are provided throughout the Load Balancing documentation.

Note: The Visualizer requires a graphic interface, so it is available only through the configuration utility.

To view load balancing virtual server properties by using the Visualizer

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to view, and then click Visualizer.
3. In the Load Balancing Visualizer dialog box, you can adjust the viewable area as follows:
   - Click the Zoom In and Zoom Out icons to increase or decrease the size of the viewed objects. You can click and drag the viewable area if an item that you want to see disappears from view after zooming in.
   - Click the Best Fit icon to optimize the viewing area.
   - Click the Save Image icon to save the graph as an image file.
   - Click the image, hold down the mouse button, and drag the image to pan the view.
   - In the Search in text field, begin typing the name of the item you are looking for. The item's location is then highlighted. To restrict the search, click the drop-down menu and select the type of element that you want to search for

To view configuration details for services, service groups, and monitors by using the Visualizer

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to view, and then click Visualizer.
3. In the Load Balancing Visualizer dialog box, to view configuration details for entities that are bound to this virtual server, you can do the following:
   - To view a summary of bound services, position the cursor over the virtual server icon.
   - To view services in a service container, click the icon for a service group, click the Related Tasks tab, click Show Member Services, and then click the service group name. To view additional details about the services click Open.
   - To view common properties of services in a service group, click the icon for the service group, click the Related Tasks tab, and view the Details section of the tab.
   - To view a comparative list of the parameters whose values either differ or are not defined across service containers, click the icon for a container, click the Related Tasks tab, and then click Service Attributes Diff. To view monitor binding details for the services in a container, in the Service Attributes Diff dialog box, in the Group column for the container, click Details.
   - To view the details for a monitor, position the cursor over the icon or click the icon for the monitor. For additional details, click the icon, click the Related Tasks tab, and then click View Monitor.
   - To view binding details of a monitor, click the connecting line between the monitor and its related service.

To view configuration details for policies and policy labels by using the Visualizer in the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to view, and then click Visualizer.
3. In the Load Balancing Visualizer dialog box, to view configuration details for entities that are bound to this virtual server, you can do the following:
   - To view policies that are bound to this virtual server, select one or more policy icons in the tool bar at the top of the dialog box. For example, you can select Compression, Filter, Rewrite, and Responder. If policy labels are configured, they appear in the main view area.
   - For bound policies that appear in the view pane of the Visualizer, to view a policy's expression and actions, position the cursor over the policy icon. To view binding details, position the cursor over the line that connects the policy to the virtual server. To view these details, click the policy. The details of the policy appear in the details pane.

To view statistical information by using the Visualizer

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to view, and then click Visualizer.
3. In the Load Balancing Visualizer dialog box, to view statistical information, you can do the following:
   - To view detailed statistics for the load balancing virtual server, click the icon for the virtual server, click the Related Tasks tab, and then click Statistics.
   - To view the number of requests received per second at a given point in time by the load balancing virtual server and the number of hits per second at a given point in time for rewrite, responder, and cache policies, click Show Stats. The statistical information is displayed on the respective nodes in the Visualizer. This information is not updated in real time and has to be refreshed manually. To refresh this information, click Refresh Stats.

     Note: The Show Stats option is available only on NetScaler nCore builds.

To save configuration properties for any entity by using the Visualizer

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to view, and then click Visualizer.
3. To copy configuration details for an element to a document or spreadsheet, click the icon for that element, click Related Tasks.
4. In the Related Tasks tab, click Copy Properties and then paste the information into a document.

To bind a resource to a load balancing configuration by using the Visualizer

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure bindings, and then click Visualizer.
3. In the Load Balancing Visualizer dialog box, click the Available Resources tab, select a resource type in the drop-down menu, and do one or more of the following:
   - To bind a new monitor to a service, select Monitors, click a particular monitor, and then drag it to the service container icon. Use CONTROL + click to select multiple monitors and drag them to the service.
   - To bind a service or service group, select Services or Service Groups, respectively, click a particular service or service group, and then drag it to the virtual server icon. To bind multiple services or service groups at one time, press CONTROL + click to select multiple services and drag them over the virtual server.
   - To bind a policy, select one of the policy groups, click a particular policy, and then drag it to a virtual server. To bind multiple policies (classic policies only) at one time, press CONTROL + policies and drag them over the virtual server. For details on classic and advanced policies, see Policy Configuration and Reference.

To unbind a resource by using the Visualizer

1. In the navigation pane, expand Load Balancing, and then click Virtual Server.
2. In the details pane, select the virtual server from which you want to unbind a service, policy, or monitor, and then click Visualizer.
3. In the Load Balancing Visualizer dialog box, on the Visualizer image, click the connecting line between the resources that you want to unbind, and then click Unbind. For example, to unbind a monitor, you would click the link between the monitor and its bound service and click Unbind.
4. In the Unbind dialog box, click Yes.

To modify a resource in a load balancing configuration by using the Visualizer

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to configure, and then click Visualizer.
3. In the Load Balancing Visualizer dialog box, on the Visualizer image, double-click the resource that you want to modify.

   Note: Alternatively, on the Available Resources tab, select the resource type from the drop-down menu, select the particular resource that you want to configure and then click Open.
4. In the modify dialog box, enter new settings for the resource.

To add, remove, or disable a resource in a load balancing configuration by using the Visualizer

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server that you want to configure, and then click Visualizer.
3. In the Load Balancing Visualizer dialog box, right-click the icon for the resource that you want to add, remove, or disable, and then select the corresponding option from the menu.

   Note: Alternatively, on the Available Resources tab, click the resource type from the drop-down menu, and then click Add to add an entity, or select the particular resource that you want to configure and then click Open.

   Note: These options are not available for service groups or policies.

Managing Client Traffic

Managing client connections properly helps to ensure that your applications remain available to users even when your NetScaler appliance is experiencing high loads. A number of load balancing features and other features available on the appliance can be integrated into a load balancing setup to process load more efficiently, divert it when necessary, and prioritize the tasks that the appliance must perform:

- **Sessionless load balancing.** You can configure sessionless load balancing virtual servers and perform load balancing without creating sessions in configurations that use DSR or intrusion detection systems (IDS).
- **Integrated caching.** You can redirect HTTP requests to a cache.
- **Priority queuing.** You can direct requests based on priority, by integrating your configuration with the Priority Queuing feature.
- **SureConnect.** You can use load balancing with the SureConnect feature to redirect important requests to a custom Web page, insulating them from delays due to network congestion.
- **Delayed cleanup.** You can configure delayed cleanup of virtual server connections to prevent the cleanup process from using CPU cycles during periods when the NetScaler appliance is experiencing high loads.
- **Rewrite.** You can use the Rewrite feature to modify port and protocol when performing HTTP redirection, or insert the virtual server IP address and port into a custom Request header.
- **RTSP NAT.**
- **Rate-based monitoring.** You can enable rate-based monitoring to divert excess traffic.
- **Layer 2 Parameters.** You can configure a virtual server to use the L2 parameters to identify a connection.
- **ICMP Response**. You can configure the NetScaler to send ICMP responses to PING requests according to your settings. On the IP address corresponding to the virtual server, set the ICMP RESPONSE to VSVR_CNTRLD, and on the virtual server, set the ICMP VSERVER RESPONSE.

  The following settings can be made on a virtual server:

  - When you set ICMP VSERVER RESPONSE to PASSIVE on all virtual servers, NetScaler always responds.
  - When you set ICMP VSERVER RESPONSE to ACTIVE on all virtual servers, NetScaler responds even if one virtual server is UP.
  - When you set ICMP VSERVER RESPONSE to ACTIVE on some and PASSIVE on others, NetScaler responds even if one virtual server set to ACTIVE is UP.

Configuring Sessionless Load Balancing Virtual Servers

When the NetScaler appliance performs load balancing, it creates and maintains sessions between clients and servers. The maintenance of session information places a significant load on the NetScaler resources, and sessions might not be needed in scenarios such as a direct server return (DSR) setup and the load balancing of intrusion detection systems (IDS). To avoid creating sessions when they are not necessary, you can configure a virtual server on the appliance for sessionless load balancing. In sessionless load balancing, the appliance carries out load balancing on a per-packet basis.

Sessionless load balancing can operate in MAC-based forwarding mode or IP-based forwarding mode.

For MAC-based forwarding, the IP address of the sessionless virtual server must be specified on all the physical servers to which the traffic is forwarded.

For IP-based forwarding in sessionless load balancing, the IP address and port of the virtual server need not be specified on the physical servers, because this information is included in the forwarded packets. When forwarding a packet from the client to the physical server, the appliance leaves client details such as IP address and port unchanged and adds the IP address and port of the destination.

Supported Setup

NetScaler sessionless load balancing supports the following service types and load balancing methods:

Service Types

- ANY for MAC-based redirection
- ANY, DNS, and UDP for IP-based redirection

Load Balancing Methods

- Round Robin
- Least Bandwidth
- LRTM (Least response time method)
- Source IP Hash
- Destination IP Hash
- Source IP Destination IP Hash

- Source IP Source Port Hash
- Custom Load

Limitations

Sessionless load balancing has the following limitations:

- The NetScaler must be deployed in two-arm mode.
- A service must be bound to only one virtual server.
- Sessionless load balancing is not supported for service groups.
- Sessionless load balancing is not supported for domain based services (DBS services).
- Sessionless load balancing in the IP mode is not supported for a virtual server that is configured as a backup to a primary virtual server.
- You cannot enable spillover mode.
- For all the services bound to a sessionless load balancing virtual server, the Use Source IP (USIP) option must be enabled.
- For a wildcard virtual server or service, the destination IP address will not be changed.

Note: While configuring a virtual server for sessionless load balancing, explicitly specify a supported load balancing method. The default method, Least Connection, cannot be used for sessionless load balancing.

Note: To configure sessionless load balancing in MAC-based redirection mode on a virtual server, the MAC-based forwarding option must be enabled on the NetScaler.

To add a sessionless virtual server by using the command line interface

At the command prompt, type the following commands to add a sessionless virtual server and verify the configuration:

- add lb vserver <name>@ <serviceType> <IPAddress>@ <port> -m <redirectionMode> -sessionless <(ENABLED|DISABLED)> -lbMethod <load_balancing_method>
- show lb vserver <name>

Example

```
add lb vserver sesslessv1 any 11.11.12.123 54 -sessionless ENABLED -lbMethod roundrobin -m ip
    Done
show lb vserver sesslessv1
    sesslessv1 (11.11.12.123:54) - ANY Type: ADDRESS
    State: DOWN
```

```
...
Effective State: DOWN
Client Idle Timeout: 120 sec
Down state flush: ENABLED
...
Persistence: NONE
Sessionless LB: ENABLED
Connection Failover: DISABLED
L2Conn: OFF
1) Policy : cmp_text Priority:8680 Inherited
2) Policy : cmp_nocmp_ie60 Priority:8690 Inherited
```

To configure sessionless load balancing on an existing virtual server

At the command prompt, type:

set lb vserver <name>@ -m <redirectionMode> -sessionless <(ENABLED|DISABLED)> -lbMethod <load_balancing_method>

Example

```
set lb vserver sesslessv1 -m mac -sessionless ENABLED -lbmethod lrtm
  Done
```

Parameters for configuring sessionless load balancing virtual servers

vServerName

The name of the virtual server that you are configuring.

m

The redirection mode that you want to use. MAC, IP.

sessionless

Perform load balancing on a per-packet basis, without establishing sessions. Possible values: ENABLED and DISABLED. Default: DISABLED.

lbMethod

The load balancing method. See Supported Setup.

To configure a sessionless virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, do one of the following:
   - To add a sessionless virtual server, click Add.
   - To specify sessionless load balancing for an existing virtual server, select it, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for Configuring Sessionless Load Balancing Virtual Servers" as shown:
   - Service Name*-serviceName
   - Protocol*-serviceType
   - Server*-serverName
   - Port*-port

   *A required parameter
4. In the Configure Virtual Server (Load Balancing) dialog box, on the Methods and Persistence tab, in the LB Method group, select a supported load balancing method.
5. In the Configure Virtual Server (Load Balancing) dialog box, on the Advanced tab, under Redirection Mode, select MAC Based or IP Based.
6. Select Sessionless.
7. Click Create or click OK.
8. In the details pane, click the arrow next to the name of the virtual server and verify the configuration.

Redirecting HTTP Requests to a Cache

The NetScaler cache redirection feature redirects HTTP requests to a cache. You can significantly reduce the impact of responding to HTTP requests and improve your Web site performance through proper implementation of the cache redirection feature.

A cache stores frequently requested HTTP content. When you configure cache redirection on a virtual server, the NetScaler appliance sends cacheable HTTP requests to the cache, and non-cacheable HTTP requests to the origin Web server.

To configure cache redirection on a virtual server by using the command line interface

At the command prompt, type:

set lb vserver <name>@ -cacheable <Value>

Example

set lb vserver Vserver-LB-1 -cacheable yes

Parameters for configuring cache redirection

vServerName

The name of the virtual server that you are configuring.

cacheable

Virtual server requests to be routed to the cache redirection virtual server before sending them to the configured servers. Possible values: YES and NO. Default: NO.

To configure cache redirection on a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure cache redirection, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, click the Advanced tab.
4. Select the Cache Redirection check box, and then click OK.

Directing Requests According to Priority

The NetScaler appliance supports prioritization of client requests with its priority queuing feature. This feature allows you to designate certain requests, such as those from important clients, as priority requests and sends them to the “front of the line,” so that the appliance responds to them first. This allows you to provide uninterrupted service to those clients through demand surges or DDoS attacks on your Web site.

To configure priority queuing on a virtual server by using the command line interface

At the command prompt, type:

set lb vserver <name>@ -pq <Value>

Example

set lb vserver Vserver-LB-1 -pq yes

Parameter for configuring priority queuing

vServerName

The name of the virtual server that you are configuring.

pq

Prioritizes client requests on the specified virtual server. Possible values: ON and OFF. Default: OFF.

To configure priority queuing on a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure priority queuing, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, click the Advanced tab.
4. Select the PQ check box, and then click OK.

Note: You must configure priority queuing globally for it to function correctly.

Directing Requests to a Custom Web Page

The NetScaler appliance provides the SureConnect option to ensure that web applications respond despite delays caused by limited server capacity or processing speed. SureConnect does this by displaying an alternative web page of your choice when the server that hosts the primary web page is either unavailable or responding slowly.

To configure SureConnect on a virtual server, you must first configure the alternative content. For information about configuring a SureConnect website, see SureConnect. After you configure the website, enable SureConnect on the load balancing virtual server to put your SureConnect custom web page in use.

Note: For SureConnect to function correctly, you must configure it globally.

To enable SureConnect on a virtual server by using the command line interface

At the command prompt, type:

set lb vserver <name>@ -sc <Value>

Example

set lb vserver Vserver-LB-1 -sc yes

Parameters for configuring SureConnect

vServerName

The name of the virtual server that you are configuring.

sc

Assurance of a response from an application despite possible delays due to server capacity or processing speed. Possible values: ON and OFF. Default: OFF.

To enable SureConnect on a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure SureConnect, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, click the Advanced tab.
4. Select the SC check box, and then click OK.

Enabling Cleanup of Virtual Server Connections

Under certain conditions, you can configure the downStateFlush setting to immediately terminate existing connections when a service or a virtual server is marked DOWN. Terminating existing connections frees resources, and in certain cases speeds recovery of overloaded load balancing setups.

The state of a virtual server depends on the states of the services bound to it. The state of each service depends on the responses of the load balanced servers to probes and health checks sent by the monitors that are bound to that service. Sometimes the load balanced servers do not respond. If a server is slow or busy, monitoring probes can time out. If repeated monitoring probes are not answered within the configured timeout period, the service is marked DOWN.

A virtual server is marked DOWN only when all services bound to it are marked DOWN. When a virtual server goes DOWN, it terminates all connections, either immediately or after allowing existing connections to complete.

You must not enable the downStateFlush setting on those application servers that must complete their transactions. You can enable this setting on Web servers whose connections can safely be terminated when they marked DOWN.

The following table summarizes the effect of this setting on an example configuration consisting of a virtual server, Vserver-LB-1, with two services bound to it, Service-TCP-1 and Service-TCP-2. The virtual server intercepts two connections, C1 and C2, and redirects them to Service-TCP-1 and Service-TCP-2, respectively. In the table, E and D denote the state of the downStateFlush setting: E means Enabled, and D means Disabled.

Vserver-LB-1	Service-TCP-1	State of connections
E	E	Both client and server connections are terminated.
E	D	Both client and server connections are terminated. In case of HTTP services, both client and server connections are terminated only if the transaction is active. If the transaction is not active, only client connections are terminated.

D	E	Both client and server connections are terminated. In case of HTTP services, both client and server connections are terminated only if the transaction is active. If the transaction is not active, only server connections are terminated.
D	D	Neither client nor server connections are terminated.

Note: In case of HTTP services, the downStateFlush setting is effective only when the client is connected to the server.

If you want to disable a service only when all the established connections are closed by the server or the client, you can use the graceful shutdown option. For information about the graceful shutdown of a service, see Graceful Shutdown of Services.

To configure the down state flush setting on a virtual server by using the command line interface

At the command prompt, type:

set lb vserver <name>@ -downStateFlush <Value>

Example

set lb vserver Vserver-LB-1 -downStateFlush enabled

Parameters for configuring down state flush

vServerName

The name of the virtual server that you are configuring.

downStateFlush

Flush all active transactions associated with a virtual server whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions. Possible values: ENABLED, DISABLED. Default: ENABLED

To configure the down state flush setting on a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure down state flush, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, click the Advanced tab.
4. Select the Down state flush check box, and then click OK.

Graceful Shut down of Services

During scheduled network outages such as system upgrades or hardware maintenance, you may have to close or disable some services. To avoid disrupting sessions that have already been established, you can specify a wait time, which places a service in the transition out of service (TROFS) state until the specified wait time expires. The service then enters the out of service (OFS) state.

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

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

The following table describes graceful shut down options.

Table 1. Graceful Shut down Options

State	Results
Graceful shutdown is enabled and a wait time is specified.	Service is shut down after the last of the current active client connections is served, even if the wait time has not expired. The appliance checks the status of the connections once every second. If the wait time expires, any open sessions are closed.
Graceful shutdown is disabled and a wait time is specified.	Service is shut down only after the wait time expires, even if all established connections are served before expiration.
Graceful shutdown is enabled and no wait time is specified.	Service is shut down only after the last of the previously established connections is served, regardless of the time taken to serve the last connection.
Graceful shutdown is disabled and no wait time is specified.	No graceful shutdown. Service is shut down immediately after the disable option is chosen or the disable command is issued. (The default wait time is zero seconds.)

To terminate existing connections when a service or a virtual server is marked DOWN, you can use the Down State Flush option. For more information, see Enabling Cleanup of Virtual Server Connections.

To configure graceful shutdown for a service by using the command line interface

At the command prompt, type the following commands to shut down a service gracefully and verify the configuration:

- disable service <name>@ [<delay>] [-graceFul (YES|NO)]
- show service <name>

Example

```
> disable service svc1 6000 -graceFul YES
Done
>show service svc1
svc1 (10.102.80.41:80) - HTTP
State: GOING OUT OF SERVICE (Graceful, Out Of Service in 5998 seconds)
Last state change was at Mon Nov 15 22:44:15 2010
Time since last state change: 0 days, 00:00:01.160
...
Down state flush: ENABLED

1 bound monitor:
1) Monitor Name: tcp-default
State: UP           Weight: 1
Probes: 13898    Failed [Total: 0 Current: 0]
Last response: Probe skipped - live traffic to service.
Response Time: N/A
Done

>show service svc1
svc1 (10.102.80.41:80) - HTTP
State: OUT OF SERVICE
Last state change was at Mon Nov 15 22:44:19 2010
Time since last state change: 0 days, 00:00:03.250
Down state flush: ENABLED

1 bound monitor:
1)  Monitor Name: tcp-default
State: UNKNOWN          Weight: 1
Probes: 13898    Failed [Total: 0 Current: 0]
Last response: Probe skipped - service state OFS.
Response Time: N/A
Done
```

Parameters for configuring a graceful shutdown for a service

serviceName

Name of the service. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

delayInSeconds

The time in seconds after which the service is marked as OUT OF SERVICE.

graceFul

Wait for all previously established connections to this service to be closed before disabling the service. Possible values: YES, NO. Default: NO.

To configure graceful shutdown for a service by using the configuration utility

1. In the navigation pane, expand Load Balancing and then click Services.
2. In the details pane, select the service, and then click Disable.
3. To delay disabling the service, in the Wait Time dialog box, type the wait time after which the service is to be disabled.
4. To disable the service only after all previously initiated transactions have been completed, check the Graceful Shutdown check box.
5. Click Enter.
6. In the Services pane, you can verify that the service is marked as UP until the wait time expires and after that, it is marked as OUT OF SERVICE.

Rewriting Ports and Protocols for HTTP Redirection

Virtual servers and the services that are bound to them may use different ports. When a service responds to an HTTP connection with a redirect, you might need to configure the NetScaler appliance to modify the port and the protocol to make sure that the redirection goes through successfully. You do this by enabling and configuring the redirectPortRewrite setting.

This setting affects only HTTP and HTTPS traffic. If this setting is enabled on a virtual server, the virtual server rewrites the port on redirects, replacing the port used by the service with the port used by the virtual server.

If the virtual server or service is of type SSL, you must enable SSL redirect on the virtual server or service. If both the virtual server and service are of type SSL, enable SSL redirect on the virtual server.

The redirectPortRewrite setting can be used in the following scenarios:

- The virtual server is of type HTTP and the services are of type SSL.
- The virtual server is of type SSL and the services are of type HTTP.
- The virtual server is of type HTTP and the services are of type HTTP.
- The virtual server is of type SSL and the services are of type SSL.

Scenario 1: The virtual server is of type HTTP and services are of type SSL. SSL redirect, and optionally port rewrite, is enabled on the service. If port rewrite is enabled, the port of HTTPS URLs is rewritten. HTTP URLs from the server are sent as is to the client.

Redirect URL from the Server	Redirect URL sent to the Client
Only SSL redirect is enabled. The virtual server can be configured on any port.	
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/
SSL redirect and port rewrite are enabled. The virtual server is configured on port 80.	
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com/
SSL redirect and port rewrite are enabled. Virtual server is configured on port 8080.	

http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	http://domain.com:8080/
https://domain.com:444/	http://domain.com:8080/

Scenario 2: The virtual server is of type SSL and services are of type HTTP. If port rewrite is enabled, only the port of HTTP URLs is rewritten. HTTPS URLs from the server are sent as is to the client.

Redirect URL from the Server	Redirect URL sent to the Client
SSL redirect is enabled on the virtual server. The virtual server can be configured on any port.	
http://domain.com/	https://domain.com/
http://domain.com:8080/	https://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/
SSL redirect and port rewrite are enabled on the virtual server. The virtual server is configured on port 443.	
http://domain.com/	https://domain.com/
http://domain.com:8080/	https://domain.com/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/
SSL redirect and port rewrite are enabled. The virtual server is configured on port 444.	
http://domain.com/	https://domain.com:444/
http://domain.com:8080/	https://domain.com:444/
https://domain.com/	https://domain.com/
https://domain.com:445/	https://domain.com:445/

Scenario 3: The virtual server and service are of type HTTP. Port rewrite must be enabled on the virtual server. Only the port of HTTP URLs is rewritten. HTTPS URLs from the server are sent as is to the client.

Redirect URL from the Server	Redirect URL sent to the Client
The virtual server is configured on port 80.	
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/
The virtual server is configured on port 8080.	
http://domain.com/	http://domain.com:8080/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/

https://domain.com:445/	https://domain.com:445/

Scenario 4: The virtual server and service are of type SSL. If port rewrite is enabled, only the port of HTTPS URLs is rewritten. HTTP URLs from the server are sent as is to the client.

Redirect URL from the Server	Redirect URL sent to the Client
SSL redirect is enabled on the virtual server. The virtual server can be configured on any port.	
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/
SSL redirect and port rewrite are enabled on the virtual server. The virtual server is configured on port 443.	
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com/
SSL redirect and port rewrite are enabled on the virtual server. The virtual server is configured on port 444.	
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com:444/
https://domain.com:445/	https://domain.com:444/

To configure HTTP redirection on a virtual server by using the command line interface

At the command prompt, type:

set lb vserver <name>@ -redirectPortRewrite (ENABLED | DISABLED)

Example

set lb vserver Vserver-LB-1 -redirectPortRewrite enabled

Parameters for redirect port rewrite

vServerName

The name of the virtual server that you are configuring.

redirectPortRewrite

Rewrite the port and change the protocol to ensure successful HTTP redirects from services. Possible values: ENABLED and DISABLED. Default: DISABLED.

To configure HTTP redirection on a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure HTTP redirection, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, click the Advanced tab.
4. Select the Redirect Port Rewrite check box, and then click OK.

To configure SSL Redirect on an SSL virtual server or service by using the command line interface

At the command prompt, type:

- set ssl vserver <vServerName> - sslRedirect (ENABLED | DISABLED)
- set ssl service <serviceName> - sslRedirect (ENABLED | DISABLED)

Example

```
set ssl vserver Vserver-SSL-1 -sslRedirect enabled
set ssl service service-SSL-1 -sslRedirect enabled
```

Parameters for SSL Redirect

vServerName

The name of the virtual server that you are configuring.

sslRedirect

State of HTTPS redirects for the SSL virtual server or service.

To configure SSL redirection and SSL port rewrite on an SSL virtual server or service by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers or Services.
2. In the details pane, select the virtual server or service for which you want to configure SSL redirection, and then click Open.
3. In the Configure Virtual Server (SSL Offload) dialog box, click the SSL Settings tab, and then click SSL Parameter.
4. In the Configure SSL Params dialog box, select SSL Redirect. Optionally, select SSL Redirect Port Rewrite.
5. Click OK.
6. In the Configure Virtual Server (SSL Offload) dialog box, click OK.

Inserting the IP Address and Port of a Virtual Server in the Request Header

If you have multiple virtual servers that communicate with different applications on the same service, you must configure the NetScaler appliance to add the IP address and port number of the appropriate virtual server to the HTTP requests that are sent to that service. This setting allows applications running on the service to identify the virtual server that sent the request.

If the primary virtual server is down and the backup virtual server is up, the configuration settings of the backup virtual server are added to the client requests. If you want the same header tag to be added, regardless of whether the requests are from the primary virtual server or backup virtual server, then you must configure the required header tag on both virtual servers.

Note: This option is not supported for wild card virtual servers or dummy virtual servers.

To insert the IP address and port of the virtual server in the client requests by using the command line interface

At the command prompt, type:

set lb vserver <name>@ -insertVserverIPPort <insertVserverIPPort> [<vipHeader>]

Example

set lb vserver Vserver-LB-1 -insertVserverIPPort VipAddr

Parameters for virtual server IP port insertion

vServerName

The name of the virtual server that you are configuring.

insertVserverIPPort

Insert an HTTP header, whose value is the IP address and port number of the virtual server, before forwarding a request to the server. The format of the header is <vipHeader>: <virtual server IP address>_<port number >, where vipHeader is the name that you specify for the header. If the virtual server has an IPv6 address, the address in the header is enclosed in brackets ([and]) to separate it from the port number. If you have mapped an IPv4 address to a virtual server's IPv6 address, the value of this

parameter determines which IP address is inserted in the header, as follows:

VIPADDR—Insert the IP address of the virtual server in the HTTP header regardless of whether the virtual server has an IPv4 address or an IPv6 address. A mapped IPv4 address, if configured, is ignored.

V6TOV4MAPPING—Insert the IPv4 address that is mapped to the virtual server's IPv6 address. If a mapped IPv4 address is not configured, insert the IPv6 address.

OFF—Disable header insertion.

vipHeader

Name for the inserted header. The default name is vip-header. Maximum Length: 79 characters.

To insert the IP address and port of the virtual server in the client requests by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to insert the IP address and port, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, click the Advanced tab.
4. In the Vserver IP Port Insertion list, select the VIPADDR or V6TOV4MAPPING, and then type the port header in a text box next to Vserver IP Port Insertion box.
5. Click OK.

Using a Specified Source IP for Backend Communication

For communication with the physical servers or other peer devices, the NetScaler appliance uses an IP address owned by it as the source IP address. NetScaler maintains a pool of its IP addresses, and dynamically selects an IP address while connecting with a server. Depending on the subnet in which the physical server is placed, NetScaler decides which IP address to use. This address pool is used for sending traffic as well as monitor probes.

In many situations, you may want the NetScaler to use a specific IP address or any IP address from a specific set of IP addresses for backend communications. The following are a few examples:

- A server can distinguish monitor probes from traffic if the source IP address used for monitor probes belongs to a specific set.
- To improve server security, a server may be configured to respond to requests from a specific set of IP addresses or, sometimes, from a single specific IP address. In such a case, the NetScaler can use only the IP addresses accepted by the server as the source IP address.
- The NetScaler can manage its internal connections efficiently if it can distribute its IP addresses into IP sets and use an address from a set only for connecting to a specific service.

To configure the NetScaler to use a specified source IP address, create net profiles (network profiles) and configure the NetScaler entities to use the profile. A net profile can be bound to load balancing or content switching virtual servers, services, service groups, or monitors. A net profile has NetScaler owned IP addresses (SNIPs) that can be used as the source IP address. It can be a single IP address or a set of IP addresses, referred to as an IP set. If a net profile has an IP set, NetScaler dynamically selects an IP address from the IP set at the time of connection. If a profile has a single IP address, the same IP address is used as the source IP.

If a net profile is bound to a load balancing or content switching virtual server, the profile will be used for sending traffic to all the services bound to it. If a net profile is bound to a service group, NetScaler uses the profile for all the members of the service group. If a net profile is bound to a monitor, NetScaler uses the profile for all the probes sent from the monitor.

Usage of a net profile for sending traffic:

If the Use Source IP Address (USIP) option is enabled, NetScaler uses the IP address of the client and ignores all the net profiles. If the USIP option is not enabled, NetScaler selects the source IP in the following manner:

- If there is no net profile on the virtual server or the service/service group, NetScaler uses the default method.

- If there is a net profile only on the service/service group, NetScaler uses that net profile.
- If there is a net profile only on the virtual server, NetScaler uses the net profile.
- If there is a net profile both on the virtual server and service/service group, NetScaler uses the net profile bound to the service/service group.

Usage of a net profile for sending monitor probes:

For monitor probes, NetScaler selects the source IP in the following manner:

- If there is a net profile bound to the monitor, NetScaler uses the net profile of the monitor. It ignores the net profiles bound to the virtual server or service/service group.
- If there is no net profile bound to the monitor,
  - If there is a net profile on the service/service group, NetScaler uses the net profile of the service/service group.
  - If there is no net profile even on the service/service group, NetScaler uses the default method of selecting a source IP.

Note: If there is no net profile bound to a service, NetScaler looks for a net profile on the service group if the service is bound to a service group.

To use a specified source IP address for communication, go through the following steps:

1. Create IP sets from the pool of SNIPs owned by the NetScaler. An IP set can consist of both SNIP addresses. For instructions, see Creating IP Sets.
2. Create net profiles. For instructions, see Creating a Net Profile.
3. Bind the net profiles to NetScaler entities. For instructions, see Binding a Net Profile to a NetScaler Entity.

Note: A net profile can have only the IP addresses specified as SNIP on the NetScaler.

Managing Net Profiles

A net profile (or network profile) contains an IP address or an IP set. During communication with physical servers or peers, the NetScaler appliance uses the addresses specified in the profile as the source IP address. For more information on the use of net profiles, see Using a User-specified Source IP Address for Backend Communication.

- For instructions on creating a network profile, see Creating a Network Profile.
- For instructions on binding a network profile to a NetScaler entity, see Binding a Network Profile.

Creating an IP Set

An IP set is a set of IP addresses, which are configured on the NetScaler appliance as Subnet IP addresses (SNIPs) . An IP set is identified with a meaningful name that helps in identifying the usage of the IP addresses contained in it. To create an IP set, add an IP set and bind NetScaler owned IP addresses to it. SNIP addresses can be present in the same IP set. For more information about the use of IP sets, see Using a User-specified Source IP Address for Backend Communication.

To create an IP set by using the command line interface

At the command prompt, type the following commands:

- add ipset <name>
- bind ipset <name> <IPAddress>@
  or
- bind ipset <name> <IPAddress>@
- show ipset [<name>]
  The above command shows the names of all the IP sets on the NetScaler if you do not pass any name. It shows the IP addresses bound to the specified IP set if you pass a name.

Examples

1.

```
> add ipset skpnwipset
 Done
> bind ipset skpnwipset 21.21.20.1
 Done
```

2.

```
 > add ipset testnwipset
 Done
> bind ipset testnwipset 21.21.21.[21-25]
 IPAddress "21.21.21.21" bound
 IPAddress "21.21.21.22" bound
 IPAddress "21.21.21.23" bound
 IPAddress "21.21.21.24" bound
 IPAddress "21.21.21.25" bound
 Done
```

3.

```
 > bind ipset skpipset 11.11.11.101
 ERROR: Invalid IP address
[This IP address could not be added because this is not an IP address owned by the NetScaler]
 > add ns ip 11.11.11.101 255.255.255.0 -type SNIP
 ip "11.11.11.101" added
 Done
 > bind ipset skpipset 11.11.11.101
 IPAddress "11.11.11.101" bound
```

Done

4.

> sh ipset
1) Name: ipset-1
2) Name: ipset-2
3) Name: ipset-3
4) Name: skpnewipset
Done

5.

> sh ipset skpnewipset
IP:21.21.21.21
IP:21.21.21.22
IP:21.21.21.23
IP:21.21.21.24
IP:21.21.21.25
Done

Parameters for configuring an IP set

name (Name)

The name of the IP set. The name can have up to 127 characters. It must begin with an alphanumeric character or underscore, and must contain only alphanumerics, '_', '#', '.', ' ', ':', '@', '=' or '-'.

ipAddress (IP Address)

A SNIP address on the NetScaler.

ipAddressRange

A contiguous range of SNIP or MIP address on the NetScaler.

To create an IP set by using the configuration utility

1. In the navigation pane, expand Network, and then click IP Sets.
2. In the details pane, do one of the following:
   - To create a new IP set, click Add.
   - To modify an existing IP set, select the IP set, and then click Open.
3. In the Create IP Set dialog box, set the following parameters:
   - Name
   - IP Address (The SNIPs specified on the NetScaler are displayed. Check the IP addresses that you want to bind to the IP set. You can select more than one.)

   If you want to add an IP address to the pool, do one of the following:
   - To add an IPv4 address, click Add IPv4, and then in the Create IP dialog box, type the necessary details.
   - To add an IPv6 address, click Add IPv6, and then in the Create IPV6 dialog box, type the necessary details.
4. Click Create.

Creating a Net Profile

A net profile (network profile) consists of one or more SNIP addresses of the NetScaler. For more information about the usage of net profiles, see Using a User-specified Source IP Address for Backend Communication.

To create a net profile by using the command line interface

At the command prompt, type:

add netprofile <name> [-srcIp <srcIpVal>] If the srcIpVal is not provided in this command, it can be provided later by using the set netprofile command.

Examples

```
> add netprofile skpnetprofile1 -srcIp 21.21.20.1
Done

> add netprofile baksnp -srcIp bakipset
Done

> set netprofile yahnp -srcIp 12.12.23.1
Done

> set netprofile citkbnp -srcIp citkbipset
Done
```

Parameters for creating a net profile

name (Name)

The name of the net profile. The name can have up to 127 characters. It must begin with an alphanumeric character or underscore, and must contain only alphanumerics, '_', '#', '.', ' ', ':', '@', '=' or '-'.

srcIpVal (IP address or IP Set)

IP address or the name of an IP set.

To create a net profile by using the configuration utility

1. In the navigation pane, expand Network, and then click Net Profiles.
2. In the Create Net Profile dialog box, type a name for the net profile.
3. To specify the source IP address, do one of the following:
   - Check IP Address and select an IP address from the IP Address drop-down list.
   - Check IP Set and select the name of an IP set from the IP Set drop-down list.

   If you want to add a new IP address or IP set, click New and type the necessary details in the dialog box that is displayed. If you want to modify an entry after selecting it from the drop-down list, click Modify and change the values. To unbind an IP address or IP set from a net profile, select the blank entry from the drop down list, and then click OK.
4. Click Create.

Binding a Net Profile to a NetScaler Entity

A net profile can be bound to a load balancing virtual server, service, service group, or a monitor. For more information about the effect of binding a net profile to a NetScaler entity, see Using a User-specified Source IP Address for Backend Communication.

Note: You can bind a net profile at the time of creating a NetScaler entity or bind it to an already existing entity.

To bind a net profile to a server by using the command line interface

You can bind a net profile to load balancing virtual servers and content switching virtual servers. Specify the appropriate virtual server.

At the command prompt, type:

- set lb vserver <name>@ -netProfile <net_profile_name>
  or

- set cs vserver <name> -netProfile <net_profile_name>

Examples

```
set lb vserver skpnwvs1 -netProfile gntnp
 Done
set cs vserver mmdcsv -netProfile mmdnp
 Done
```

To bind a net profile to a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing or Content Switching, and then click Virtual Servers.
2. In the details pane, select the virtual server to which you want to bind a net profile, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, or Configure Virtual Server (Content Switching) click the Profiles tab.
4. In the Net Profile drop-down list, select a net profile. In this dialog box, you can click New… to add a net profile or Modify… to modify the selected net profile.
5. Click OK.

To bind a net profile to a service by using the command line interface

At the command prompt, type:

set service <name>@ -netProfile <net_profile_name>

Example

```
set service brnssvc1 -netProfile brnsnp
 Done
```

To bind a net profile to a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service to which you want to bind a net profile, and then click Open.
3. In the Configure Service dialog box, click the Profiles tab.
4. In the Net Profile drop-down list, select a net profile. In this dialog box, you can click New… to add a net profile or Modify… to modify the selected net profile.
5. Click OK.

To bind a net profile to a service group by using the command line interface

At the command prompt, type:

set servicegroup <serviceGroupName>@ -netProfile <net_profile_name>

Example

```
set servicegroup ndhsvcgrp -netProfile ndhnp
 Done
```

To bind a net profile to a service group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.
2. In the details pane, select the service group to which you want to bind a net profile, and then click Open.
3. In the Configure Service Group dialog box, click the Profiles tab.
4. In the Net Profile drop-down list, select a net profile. In this dialog box, you can click New… to add a net profile or Modify… to modify the selected net profile.
5. Click OK.

To bind a net profile to a monitor by using the command line interface

At the command prompt, type:

```
set monitor <monitor_name> -netProfile <net_profile_name>
```

Example

```
set monitor brnsecvmon1 -netProfile brnsmonnp
 Done
```

To bind a net profile to a monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. In the details pane, select the monitor to which you want to bind a net profile, and then click Open.
3. In the Configure Monitor dialog box, in the Net Profile drop-down list, select a net profile.
4. Click OK.

Setting a Timeout Value for Idle Client Connections

You can configure a virtual server to terminate any idle client connections after a configured timeout period elapses. When you configure this setting, the NetScaler appliance waits for the time you specify and, if the client is idle after that time, it closes the client connection.

To set a time-out value for idle client connections by using the command line interface

At the command prompt, type:

set lb vserver <name>@ -cltTimeout <Value>

Example

set lb vserver Vserver-LB-1 -cltTimeout 100

Parameters for setting the client time-out value

vServerName

The name of the virtual server that you are configuring.

cltTimeout

Idle time (in seconds) after which the client connection is terminated. The default value is 180sec for HTTP/SSL-based services and 9000sec for TCP-based services.

To set a time-out value for idle client connections by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure a time-out value, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, click the Advanced tab.
4. In the Client Time-out (secs) text box, type the timeout value (for example, 100).
5. Click OK.

Managing RTSP Connections

The NetScaler appliance can use either of two topologies—*NAT-on mode* or *NAT-off mode*—to load balance RTSP servers. In NAT-on mode, Network Address Translation (NAT) is enabled and configured on the appliance. RTSP requests and responses both pass through the appliance. You must therefore configure the appliance to perform network address translation (NAT) to identify the data connection.

For more information about enabling and configuring NAT, see "IP Addressing."

In NAT-off mode, NAT is not enabled and configured. The appliance receives RTSP requests from the client and routes them to the service that it selects using the configured load balancing method. The load balanced RTSP servers send their responses directly to the client, bypassing the appliance. You must therefore configure the appliance to use Direct Server Return (DSR) mode, and assign publicly accessible FQDNs in DNS to your load balanced RTSP servers.

For more information about enabling and configuring DSR mode, see "Configuring Load Balancing in Direct Server Return Mode." For more information about configuring DNS, see "Domain Name System."

In either case, when you configure RTSP load balancing, you must also configure rtspNat to match the topology of your load balancing setup.

To configure RTSP NAT by using the command line interface

At the command prompt, type:

set lb vserver <name>@-RTSPNAT <ValueOfRTSPNAT>

Example

set lb vserver vserver-LB-1 -RTSPNAT ON

Parameters for configuring RTSP

vServerName

The name of the virtual server that you are configuring.

rtspNat

Whether the appliance is configured to use NAT or not when load balancing RTSP services. When the appliance is configured for the NAT-on mode, you must set rtspNat

ON. When the NetScaler is configured for NAT-off mode, you must set rtspNat OFF. Possible values: ON and OFF. Default value: OFF.

To configure RTSP NAT by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure RTSP NAT, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, click the Advanced tab.
4. Select the RTSP Natting check box, and then click OK.

Managing Client Traffic on the Basis of Traffic Rate

You can monitor the rate of traffic that flows through load balancing virtual servers and control the behavior of the NetScaler appliance based on the traffic rate. You can throttle the traffic flow if it is too high, cache information based on the traffic rate, and if the traffic rate is too high redirect excess traffic to a different load balancing virtual server. You can apply rate-based monitoring to HTTP and Domain Name System (DNS) requests.

For more information on rate-based policies, see Rate Limiting.

Identifying a connection with Layer 2 Parameters

Generally, to identify a connection, the NetScaler uses the 4-tuple of client IP address, client port, destination IP address, and destination port. When you enable the L2 Connection option, the Layer 2 parameters of the connection (channel number, MAC address, and VLAN ID) are used in addition to the normal 4-tuple.

Enabling the L2Conn parameter for a load balancing virtual server allows multiple TCP and non-TCP connections with the same 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>) to co-exist on the NetScaler appliance. The appliance uses both the 4-tuple and the Layer 2 parameters to identify TCP and non-TCP connections.

You can enable the L2Conn option in the following scenarios:

- Multiple VLANs are configured on the NetScaler appliance, and a firewall is set up for each VLAN.
- You want the traffic originating from the servers in one VLAN and bound for a virtual server in another VLAN to pass through the firewalls configured for both VLANs.

Therefore, when an nCore NetScaler appliance on which the l2Conn parameter is set for one or more load balancing virtual servers is downgraded to a Classic build or to an nCore build that does not support the l2Conn parameter, the load balancing configurations that use the l2Conn parameter become ineffective.

To configure the L2 connection option by using the command line interface

At the command prompt, type:

add lb vserver <name>@ <serviceType> <IPAddress>@ <port> -l2Conn ON

Example

add lb vserver LB-VIP1 HTTP 10.1.1.254 80 -l2Conn ON

Parameters for configuring a virtual server

vServerName

Name of the virtual server that is associated with the service. The name must not exceed 127 characters, and the leading character must be a number or a letter. The following

characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

ipAddress

IP address of the virtual server, in either IPv4 or Ipv6 format.

serviceType

The type of services to which the virtual server distributes requests.

port

Port on which the virtual server listens for client connections.

l2Conn

The tuple used to identify a connection includes the layer 2 parameters.

To configure the L2 connection option by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers .
2. In the details pane, click **Add**.
3. In the CreateVirtual Server (Load Balancing) dialog box, specify values which correspond to parameters described in "Parameters for configuring a virtual server" as shown:
   - Name*—vServerName
   - IP Address*—ipAddress
   - Protocol*—serviceType
   - Port*—port

   *A required parameter
4. On the Advanced tab, selectL2 Connection.
5. Click Create.
6. Open the virtual server you configured and verify the configuration.

Configuring the Prefer Direct Route Option

On a wildcard load balancing virtual server if you explicitly configure a route to a destination, by default, the NetScaler appliance forwards traffic according to the configured route. If you want the NetScaler to not look up for the configured route, you can set the Prefer Direct Route option to NO.

If a device is directly connected to a NetScaler appliance, the NetScaler directly forwards traffic to the device. For example, if the destination of a packet is a firewall, the packet need not be routed through another firewall. However, in some cases, you may want the traffic to go through the firewall even if the device is directly connected to it. In such cases, you can set the Prefer Direct Route Option to NO.

Note: The preferDirectRoute setting is applicable to all the wildcard virtual servers on the NetScaler appliance.

To set the prefer direct route option by using the command line interface

At the command prompt, type:

set lb parameter -preferDirectRoute (YES | NO)

Example

set lb parameter -preferDirectRoute YES

Parameter for configuring prefer direct route option

preferDirectRoute

If enabled, the NetScaler looks up for the configured route. Possible values: YES, NO. Default: YES.

To set the prefer direct route option by using the configuration utility

1. In the navigation pane, click Load Balancing.
2. Under Settings, click Configure Load Balancing Parameters.
3. In the Configure Load Balancing Parameters dialog box, select the Prefer Direct Route check box.
4. Click OK.

Advanced Load Balancing Settings

In addition to configuring virtual servers, you can configure advanced settings for services.

Gradually Stepping Up the Load on a New Service with Virtual Server–Level Slow Start

You can configure the NetScaler appliance to gradually increase the load on a service (the number of requests that the service receives per second) immediately after the service is either added to a load balancing configuration or has a state change from DOWN to UP (hereafter, the term “new service” is used for both situations). You can either increase the load manually with load values and intervals of your choice (manual slow start) or configure the appliance to increase the load at a specified interval (automated slow start) until the service is receiving as many requests as the other services in the configuration. During the ramp-up period for the new service, the appliance uses the configured load balancing method.

This functionality is not available globally. It has to be configured for each virtual server. The functionality is available only for virtual servers that use one of the following load balancing methods:

- Round robin
- Least connection
- Least response time
- Least bandwidth
- Least packets
- LRTM (Least Response Time Method)
- Custom load

For this functionality, you need to set the following parameters:

- The new service request rate, which is the amount by which to increase the number or percentage of requests sent to a new service each time the rate is incremented. That is, you specify the size of the increment in terms of either the number of requests per second or the percentage of the load being borne, at the time, by the existing services. If this value is set to `0` (zero), slow start is not performed on new services.

  Note: In automated slow start mode, the final increment is smaller than the specified value if the specified value would place a heavier load on the new service than on the other services.

- The increment interval, in seconds. If this value is set to 0 (zero), the load is not incremented automatically. You have to increment it manually.

With automated slow start, a service is taken out of the slow start phase when one of the following conditions applies:

- The actual request rate is less than the new service request rate.
- The service does not receive traffic for three successive increment intervals.
- The request rate has been incremented 200 times.
- The percentage of traffic that the new service must receive is greater than or equal to 100.

With manual slow start, the service remains in the slow start phase until you take it out of that phase.

Manual Slow Start

If you want to manually increase the load on a new service, do not specify an increment interval for the load balancing virtual server. Specify only the new service request rate and the units. With no interval specified, the appliance does not increment the load periodically. It maintains the load on the new service at the value specified by the combination of the new service request rate and units until you manually modify either parameter. For example, if you set the new service request rate and unit parameters to 25 and "per second," respectively, the appliance maintains the load on the new service at 25 requests per second until you change either parameter. When you want the new service to exit the slow start mode and receive as many requests as the existing services, set the new service request rate parameter to `0`.

As an example, assume that you are using a virtual server to load balance 2 services, `Service1` and `Service2`, in round robin mode. Further assume that the virtual server is receiving 240 requests per second, and that it is distributing the load evenly across the services. When a new service, `Service3`, is added to the configuration, you might want to increase the load on it manually through values of 10, 20, and 40 requests per second before sending it its full share of the load. The following table shows the values to which you set the three parameters.

Table 1. Parameter Values

Parameter	Value
Interval in seconds	0
New service request rate	10, 20, 40, and 0, at intervals that you choose
Units for the new service request rate	Requests per second

When you set the new service request rate parameter to 0, `Service3` is no longer considered a new service, and receives its full share of the load.

Assume that you add another service, `Service4`, during the ramp-up period for `Service3`. In this example, `Service4` is added when the new service request rate parameter is set to `40`. Therefore, `Service4` begins receiving 40 requests per second.

The following table shows the load distribution on the services during the period described in this example.

Table 2. Load Distribution on Services when Manually Stepping Up the Load

	new service request rate = 10 req/sec (Service3added)	new service request rate = 20 req/sec	new service request rate = 40 req/sec (Service4added)	new service request rate = 0 req/sec (new services exit slow start mode)
Service1	115	110	80	60

Service2	115	110	80	60
Service3	10	20	40	60
Service4	-	-	40	60
Total req/sec (load on the virtual server)	240	240	240	240

Automated Slow Start

If you want the appliance to increase the load on a new service automatically at specified intervals until the service can be considered capable of handling its full share of the load, set the new service request rate parameter, the units parameter, and the increment interval. When all the parameters are set to values other than 0, the appliance increments the load on a new service by the value of the new service request rate, at the specified interval, until the service is receiving it's full share of the load.

As an example, assume that four services, `Service1`, `Service2`, `Service3`, and `Service4`, are bound to a load balancing virtual server, `vserver1`. Further assume that `vserver1` receives 100 requests per second, and that it distributes the load evenly across the services (25 requests per second per service). When you add a fifth service, `Service5`, to the configuration, you might want the appliance to send the new service 4 requests per second for the first 10 seconds, 8 requests per second for the next 10 seconds, and so on, until it is receiving 20 requests per second. For this requirement, the following table shows the values to which you set the three parameters:

Table 1. Parameter Values

Parameter	**Value**
Interval in seconds	10
Increment value	4
Units for the new service request rate	Requests per second

With this configuration, the new service begins receiving as many requests as the existing services 50 seconds after it is added or its state has changed from `DOWN` to `UP`. During each interval in this period, the appliance distributes to the existing servers the excess of requests that would have been sent to the new service in the absence of stepwise increments. For example, in the absence of stepwise increments, each service, including `Service5`, would have received 20 requests each per second. With stepwise increments, during the first 10 seconds, when `Service5` receives only 4 requests per second, the appliance distributes the excess of 16 requests per second to the existing services, resulting in the distribution pattern shown in the following table and figure over the 50-second period. After the 50-second period, `Service5` is no longer considered a new service, and it receives its normal share of traffic.

Table 2. Load Distribution Pattern on All Services for the 50-second Period Immediately after `Service5` is Added

	0 sec	10 sec	20 sec	30 sec	40 sec	50 sec
Req/sec forService1	25	24	23	22	21	20
Req/sec forService2	25	24	23	22	21	20
Req/sec forService3	25	24	23	22	21	20

Req/sec forService4	25	24	23	22	21	20
Req/sec forService5	0	4	8	12	16	20
Total req/sec (load on the virtual server)	100	100	100	100	100	100

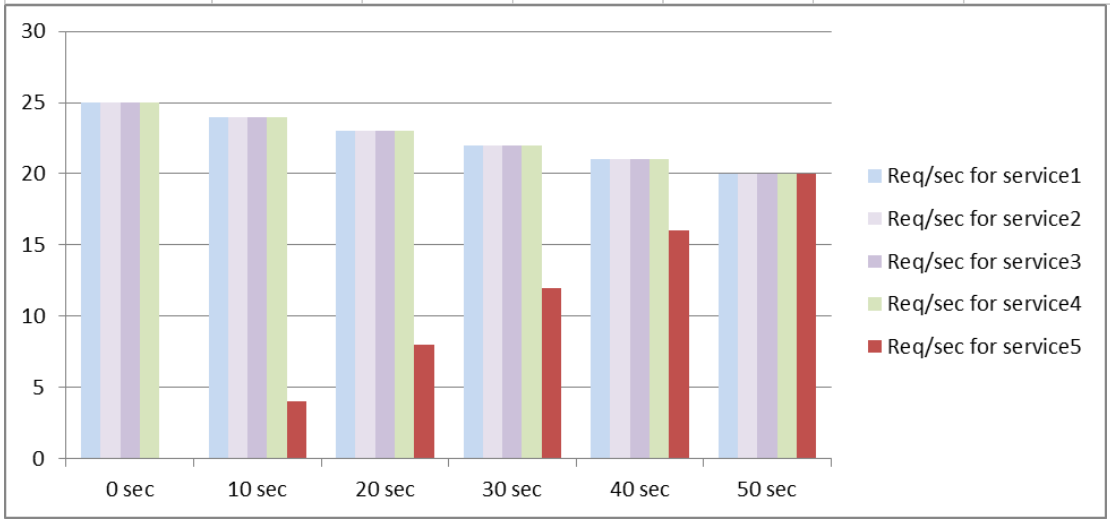


Figure 1. A Graph of the Load Distribution Pattern on All Services for the 50-second Period Immediately after `Service5` is Added

An alternative requirement might be for the appliance to send `Service5` 25% of the load on the existing services in the first 5 seconds, 50% in the next 5 seconds, and so on, until it is receiving 20 requests per second. For this requirement, the following table shows the values to which you set the three parameters.

Table 3. Parameter Values

Parameter	Value
Interval in seconds	5
Increment value	25
Units for the new service request rate	Percent

With this configuration, the service begins receiving as many requests as the existing services 20 seconds after it is added or its state has changed from `DOWN` to `UP`. The traffic distribution during the ramp-up period for the new service is identical to the one described earlier, where the unit for the step increments was “requests per second.”

Setting the Slow Start Parameters

You set the slow start parameters by using either the `set lb vserver` or the `add lb vserver` command. The following command is for setting slow start parameters when adding a virtual server.

To configure stepwise load increments for a new service by using the command line interface

At the command prompt, type the following commands to configure stepwise increments in the load for a service and verify the configuration:

- add lb vserver <name> <serviceType> <IPAddress> <port> [-newServiceRequest <positive_integer>] [<newServiceRequestUnit>] [-newServiceRequestIncrementInterval <positive_integer>]
- show lb vserver <name>

Example

```
> set lb vserver BR_LB -newServiceRequest 5 PER_SECOND -newServiceRequestIncrementInterval 10
 Done
> show lb vserver BR_LB
   BR_LB (192.0.2.33:80) - HTTP    Type: ADDRESS
   State: UP
            ...
            ...
   New Service Startup Request Rate: 5 PER_SECOND, Increment Interval: 10
            ...
            ...
Done
>
```

Parameters for configuring stepwise load increments for a new service

newServiceRequest (New Service Startup Request Rate)

Number of requests, or percentage of the load on existing services, by which to increase the load on a new service at each interval in slow-start mode. A non-zero value indicates that slow-start is applicable. A zero value indicates that the global RR startup parameter is applied. Changing the value to zero will cause services currently in slow start to take the full traffic as determined by the LB method. Subsequently, any new services added

will use the global RR factor.

newServiceRequestUnit

The unit for the step increment in load. Possible values: `PER_SECOND` (number of requests per second), `PERCENT` (percentage of the load on existing services).

newServiceRequestIncrementInterval (Increment Interval)

The interval, in seconds, between successive increments in the load on a new service or a service whose state has just changed from `DOWN` to `UP`. A value of `0` (zero) specifies manual slow start.

To configure stepwise load increments for a new service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, do one of the following:
   - To configure stepwise increments for a new load balancing virtual server, click Add.
   - To configure stepwise increments for an existing load balancing virtual server, select the virtual server, and then click Open.
3. In the Create Virtual Server or Configure Virtual Server dialog box, on the Method and Persistence tab, set the following parameters:
   - New Service Startup Request Rate. Also, from the list next to the text box, select the unit (`PER_SECOND` or `PERCENT`).
   - Increment Interval.
4. Click Create or OK, and then click Close.

The No-Monitor Option for Services

If you use an external system to perform health checks on the services and do not want the NetScaler appliance to monitor the health of a service, you can set the no-monitor option for the service. If you do so, the appliance does not send probes to check the health of the service but shows the service as UP. Even if the service goes DOWN, the appliance continues to send traffic from the client to the service as specified by the load balancing method.

The monitor can be in the ENABLED or DISABLED state when you set the no-monitor option, and when you remove the no-monitor option, the earlier state of the monitor is resumed.

You can set the no-monitor option for a service when creating the service. You can also set the no-monitor option on an existing service.

The following are the consequences of setting the no-monitor option:

- If a service for which you enabled the no-monitor option goes down, the NetScaler continues to show the service as UP and continues to forward traffic to the service. A persistent connection to the service can worsen the situation. In that case, or if many services shown as UP are actually DOWN, the system may fail. To avoid such a situation, when the external mechanism that monitors the services reports that a service that is DOWN, remove the service from the NetScaler configuration.

- If you configure the no-monitor option on a service, you cannot configure load balancing in the Direct Server Return (DSR) mode. For an existing service, if you set the no-monitor option, you cannot configure the DSR mode for the service.

To set the no-monitor option for a new service by using the command line interface

At the command prompt, type the following commands to create a service with the health monitor option, and verify the configuration:

add service <serviceName> <IP | serverName> <serviceType> <port> -healthMonitor (YES|NO)

Example

```
 >add service nomonsrvc 10.102.21.21 http 80
 -healthMonitor no
 Done
 > show service nomonsrvc
nomonsrvc (10.102.21.21:80) - HTTP
State: UP
Last state change was at Mon Nov 15 22:41:29 2010
Time since last state change: 0 days, 00:00:00.970
```

```
Server Name: 10.102.21.21
 Server ID : 0 Monitor Threshold : 0
...
Access Down Service: NO
...
Down state flush: ENABLED
Health monitoring: OFF

1 bound monitor:
1) Monitor Name: tcp-default
State: UNKNOWN Weight: 1
Probes: 3 Failed [Total: 3 Current: 3]
Last response: Probe skipped - Health monitoring is turned off.
Response Time: N/A
Done
```

To set the no-monitor option for an existing service by using the command line interface

At the command prompt, type the following command to set the health monitor option:

set service <name> -healthMonitor (YES|NO)

Example

By default, the state of a service and the state of the corresponding monitor are UP.

```
 >show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP


1) Monitor Name: http-ecv
 State: UP Weight: 1
Probes: 99992 Failed [Total: 0 Current: 0]
Last response: Success - Pattern found in response.
Response Time: 3.76 millisec
Done
```

When the no-monitor option is set on a service, the state of the monitor changes to UNKNOWN.

```
> set service LB-SVC1 -healthMonitor NO
Done
> show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP
Last state change was at Fri Dec 10 10:17:37 2010.
Time since last state change: 5 days, 18:55:48.710
Health monitoring: OFF

1) Monitor Name: http-ecv
   State: UNKNOWN Weight: 1
```

```
        Probes: 100028 Failed [Total: 0 Current: 0]
    Last response: Probe skipped - Health monitoring is turned off.
      Response Time: 0.0 millisec
  Done
When the no-monitor option is removed, the earlier state of the monitor is resumed.
> set service LB-SVC1 -healthMonitor YES
Done
>show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP
Last state change was at Fri Dec 10 10:17:37 2010
Time since last state change: 5 days, 18:57:47.880
1) Monitor Name: http-ecv
   State: UP Weight: 1
   Probes: 100029 Failed [Total: 0 Current: 0]
   Last response: Success - Pattern found in response.
   Response Time: 5.690 millisec
   Done
```

Parameters for configuring a service

serviceName

Name of the service. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

ipAddress

IP address of the server that is associated with the service, in either IPv4 or IPv6 format.

serverName

Name of the server that is associated with the service. The name must not exceed 127 characters, and the leading character must be a number or a letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serviceType

Protocol supported by the service. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, DNS_TCP, ADNS_TCP, RADIUS, MYSQL, MSSQL, and RDP.

port

The port number used for the service.

healthMonitor

The monitoring option for the service. Possible values: YES, NO. Default: YES.

To set the no-monitor option for a service by using the configuration utility

1. In the navigation pane, click Load Balancing and then click Services.
2. In the details pane, do one of the following:
   - To create a new service, click Add.
   - To modify an existing service, select the service and then click Open.
3. In the Create Service or Configure Service dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a service” as shown:
   - Service Name*–serviceName
   - Protocol*–serviceType
   - Server*–ipAddress
   - Port*–port
   - Health Monitor–healthMonitor

   * A required parameter
4. Click Create. The service you created appears in the Services pane.
5. From the Services pane, open the service that you added, and verify the health monitor setting.

Protecting Applications on Protected Servers Against Traffic Surges

The NetScaler provides the surge protection option to maintain the capacity of a server or cache. The NetScaler regulates the flow of client requests to servers and controls the number of clients that can simultaneously access the servers. The NetScaler blocks any surges passed to the server, thereby preventing overloading of the server.

For surge protection to function correctly, you must enable it globally. For more information about surge protection, see "Surge Protection."

To set surge protection on the service by using the command line interface

At the command prompt, type:

set service <name>@ -sp <Value>

Example

set service Service-HTTP-1 -sp ON

Parameters for configuring surge protection on the service

ServiceName

The name of the service that you are configuring.

sp

State of surge protection for the service. Possible values: ON and OFF. Default: OFF.

To set surge protection on the service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to configure surge protection, and then click Open.
3. In the Configure Service dialog box, click the Advanced tab, scroll down, and under Others, select the Surge Protection check box.
4. Click OK.

Enabling Cleanup of Service Connections

When cleanup of service connections is enabled, the NetScaler performs a cleanup of the connections on a service that is down. This setting is described in Enabling Cleanup of Virtual Server Connections.

To set down state flush on the service by using the command line interface

At the command prompt, type:

set service <name> -downStateFlush <Value>

Example

set service Service-HTTP-1 -downStateFlush enabled

Parameters for configuring down state flush on the service

ServiceName

The name of the service that you are configuring.

downStateFlush

Flush all active transactions associated with a service whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions. Possible values: ENABLED and DISABLED. Default: ENABLED.

To set down state flush on the service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to configure down state flush, and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Scroll down, and under Others, select the Down state flush check box.
5. Click OK.

Directing Requests to a Custom Web Page

For SureConnect to function correctly, you must set it globally. The NetScaler provides the SureConnect option to ensure the response from an application. For more information about the SureConnect option, see "Sure Connect."

To set SureConnect on the service by using the command line interface

At the command prompt, type:

set service <name>@ -sc <Value>

Example

set service Service-HTTP-1 -sc ON

Parameters for configuring SureConnect on the service

ServiceName

The name of the service that you are configuring.

sc

State of SureConnect for the service. This parameter is supported for legacy purposes only. It has no effect on the NetScaler, and its only valid value is OFF. Possible values: ON and OFF. Default: OFF.

To set SureConnect on the service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to configure SureConnect, and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Scroll down, and under Others, select the Sure Connect check box.
5. Click OK.

Enabling Access to Services When Down

You can enable access to a service when it is disabled or in a DOWN state by configuring the NetScaler appliance to use Layer 2 mode to bridge the packets sent to the service. Normally, when requests are forwarded to services that are DOWN, the request packets are dropped. When you enable the Access Down setting, however, these request packets are sent directly to the load balanced servers.

For more information about Layer 2 and Layer 3 modes, see IP Addressing.

For the appliance to bridge packets sent to the DOWN services, enable Layer 2 mode with the accessDown parameter.

To enable access down on a service by using the command line interface

At the command prompt, type:

set service <name>@ -accessDown <Value>

Example

set service Service-HTTP-1 -accessDown YES

Parameters for configuring Access Down

ServiceName

The name of the service that you are configuring.

accessDown

Access to disabled or DOWN services. If this option is enabled, and the service goes DOWN, all packets to the service are bridged. If this option is disabled, and the service goes DOWN, the packets are dropped. Possible values: YES and NO. Default: NO.

To enable access down on a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to configure access down, click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Scroll down, and under Others, select the Access Down check box.
5. Click OK.

Enabling TCP Buffering of Responses

The NetScaler appliance provides a TCP buffering option that buffers only responses from the load balanced server. This enables the appliance to deliver server responses to the client at the maximum speed that the client can accept them. The appliance allocates from 0 through 4095 megabytes (MB) of memory for TCP buffering, and from 4 through 20480 kilobytes (KB) of memory per connection.

Note: TCP buffering set at the service level takes precedence over the global setting. For more information about configuring TCP buffering globally, see "TCP Buffering."

To enable TCP Buffering on a service by using the command line interface

At the command prompt, type:

set service <name>@ -TCPB <Value>

Example

set service Service-HTTP-1 -TCPB YES

Parameters for configuring TCP buffering

ServiceName

The name of the service that you are configuring.

TCPB

State of the TCP buffering feature for the service. Possible values: YES and NO. Default: NO.

To enable TCP Buffering on a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to configure TCP buffering (for example, Service-HTTP-1), and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Scroll down, and under Settings, select the TCP Buffering check box.
5. Click OK.

Enabling Compression

The NetScaler appliance provides a compression option to transparently compress HTML and text files by using a set of built-in compression policies. Compression reduces bandwidth requirements and can significantly improve server responsiveness in bandwidth-constrained setups. The compression policies are associated with services bound to the virtual server. The policies determine whether a response can be compressed and send compressible content to the appliance, which compresses it and sends it to the client.

Note: For compression to function correctly, you must enable it globally. For more information about configuring compression globally, see Compression.

To enable compression on a service by using the command line interface

At the command prompt, type:

set service <name> -CMP <YES | NO>

Example

set service Service-HTTP-1 -CMP YES

Parameters for configuring compression

ServiceName

The name of the service that you are configuring.

CMP

State of the HTTP compression feature for the service. Possible values: YES, NO. Default: NO.

To enable compression on a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to configure compression (for example, Service-HTTP-1), and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Under Settings, select the Compression check box.
5. Click OK.

Maintaining Client Connection for Multiple Client Requests

You can set the client keep-alive parameter to configure an HTTP or SSL service to keep a client connection to a Web site open across multiple client requests. If client keep-alive is enabled, even when the load balanced Web server closes a connection, the NetScaler appliance keeps the connection between the client and itself open. This setting allows services to serve multiple client requests on a single client connection.

If you do not enable this setting, the client will open a new connection for every request that it sends to the Web site. The client keep-alive setting saves the packet round trip time required to establish and close connections. This setting also reduces the time to complete each transaction. Client keep-alive can be enabled only on HTTP or SSL service types.

Client keep-alive set at the service level takes precedence over the global client keep-alive setting. For more information about client keep-alive, see Client Keep-Alive.

To enable client keep-alive on a service by using the command line interface

At the command prompt, type:

set service <name>@ -CKA <Value>

Example

set service Service-HTTP-1 -CKA YES

Parameters to configure client keep-alive

ServiceName

The name of the service that you are configuring.

CKA

State of the Client Keep-Alive feature. Possible values: YES, NO. Default: NO.

To enable client keep-alive on a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to configure client keep-alive, and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Under Settings, select the Client Keep-Alive check box.
5. Click OK.

Inserting the IP Address of the Client in the Request Header

A NetScaler uses the mapped IP address (MIP) to connect to the server. The server need not be aware of the client.

However, in some situations, the server needs to be aware of the client it has to serve. When you enable the client IP setting, the NetScaler inserts the client's IPv4 or IPv6 address while forwarding the requests to the server. The server inserts this client IP in the header of the responses. The server is thus aware of the client.

To insert client IP address in the client request by using the command line interface

At the command prompt, type:

set service <name>@ -CIP <Value> <cipHeader>

Example

set service Service-HTTP-1 -CIP enabled X-forwarded-for

Parameters for inserting client IP address in the client request

ServiceName

The name of the service that you are configuring.

CIP

Client IP address header addition option for the service. Possible values: ENABLED and DISABLED. Default: DISABLED.

This option works with IPv4 and IPv6 addresses.

cipHeader

The name of the HTTP header that the NetScaler inserts and to which it adds the IP address of the client as the header value. If client IP insertion is enabled, and the client IP header is not specified, then the NetScaler sets the client IP header. The default is blank (NetScaler uses a blank HTTP header).

To insert client IP address in the client request by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to add the client IP address in the request, and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Under Settings, select the Client IP check box.
5. In the Header text box, type the header tag (for example, X-Forwarded-for).
6. Click OK.

Using the Source IP Address of the Client When Connecting to the Server

You can configure the NetScaler appliance to forward packets from the client to the server without changing the source IP address. This is useful when you cannot insert the client IP address into a header, such as when working with non-HTTP services.

For more information about configuring USIP globally, see "Enabling Use Source IP Mode."

For information about using the port of the client when connecting to the server, see Using the Client Port When Connecting to the Server.

To enable USIP mode for a service by using the command line interface

At the command prompt, type:

set service <name>@ -usip (**YES** | **NO**)

Example

set service Service-HTTP-1 -usip YES

Parameters to configure USIP mode

ServiceName

The name of the service that you are configuring.

usip

Determines the source IP address used when the NetScaler appliance connects to the server. If this option is set to YES, the NetScaler uses the client IP address. Possible values: YES, NO. Default: NO.

Note: USIP does not work when you bind an IPv6 service with USIP enabled to an IPv4 virtual server, or when you bind an IPv4 service with USIP enabled to an IPv6 virtual server.

To enable USIP mode for a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to enable the USIP mode, and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Under Settings, select the Use Source IP check box.
5. Click OK.

Configuring the Source Port for Server-Side Connections

When the NetScaler appliance connects to a physical server, it can use the source port from client's request, or it can use a proxy port as the source port for the connection. You can set the Use Proxy Port parameter to YES to handle situations such as the following scenario:

- The NetScaler appliance is configured with two load balancing virtual servers, LBVS1 and LBVS2.
- Both the virtual servers are bound to the same service, S-ANY.
- Use (the client's) source IP address (USIP) is enabled on the service.
- Client C1 sends two requests, Req1 and Req2, for the same service.
- Req1 is received by LBVS1 and Req2 is received by LBVS2.
- LBVS1 and LBVS2 forward the request to S-ANY, and when S-ANY sends the response, they forward the response to the client.
- Consider two cases:
    - Use the client port. When the NetScaler uses the client port, both the virtual servers use the client's IP address (because USIP is ON) and the client's port when connecting to the server. Therefore, when the service sends the response, the NetScaler cannot determine which virtual server should receive the response.
    - Use proxy port. When the NetScaler uses a proxy port, the virtual servers use the client's IP address (because USIP is ON), but different ports when connecting to the server. Therefore, when the service sends the response, the port number identifies the virtual server that should receive the response.

The Use Proxy Port option becomes relevant if the use source IP (USIP) option is enabled. For TCP-based service types, such as TCP, HTTP, and SSL, the option is enabled by default. For UDP-based service types, such as UDP and DNS, including ANY, the option is disabled by default. For more information about the USIP option, see "Enabling Use Source IP Mode."

You can configure the Use Proxy Port setting either globally or on a given service.

To configure the Use Proxy Port setting on a service by using the command line interface

At the command prompt, type:

set service <ServiceName> -useProxyPort (**YES** | **NO**)

Example

```
> set service svc1 -useproxyport YES
 Done > show service svc1
   svc1 (10.102.29.30:80) - HTTP
   State: UP
   . . .
   Use Source IP: YES      Use Proxy Port: YES
   . . .
 Done
>
```

Parameters for configuring proxy port mode on a service

ServiceName

The name of the service that you are configuring.

useProxyPort

If USIP is enabled, use a proxy port, instead of the source port in the client's request, as the source port when connecting to a physical server. Possible values: YES, NO. Default: YES for TCP based service types, NO for UDP based service types.

To configure the Use Proxy Port setting on a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to use the source IP address, and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Under Others, in the Use Proxy Port drop-down list, select YES.
5. Click OK.

Setting a Limit on the Number of Client Connections

You can specify a maximum number of client connections that each load balanced server can handle. The NetScaler appliance then opens client connections to a server only until this limit is reached. When the load balanced server reaches its limit, monitor probes are skipped, and the server is not used for load balancing until it has finished processing existing connections and frees up capacity.

For more information on the Maximum Client setting, see "Load Balancing Domain-Name Based Services."

Note: Connections that are in the process of closing are not considered for this limit.

To set a limit to the number of client connections by using the command line interface

At the command prompt, type:

set service <name> -maxclient <Value>

Example

set service Service-HTTP-1 -maxClient 1000

Parameters for configuring the maximum clients setting

ServiceName

The name of the service that you are configuring.

maxClient

Maximum number of open connections to the service. The default value is 0. The maximum value is 4294967294.

To set a limit to the number of client connections by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to configure the maximum number of client connections (for example, Service-HTTP-1), and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Under Thresholds, in the Max Clients text box, type the maximum number of client connections (for example, 100).
5. Click OK.

Setting a Limit on Number of Requests Per Connection to the Server

The NetScaler appliance can be configured to reuse connections to improve performance. In some scenarios, however, load balanced Web servers may have issues when connections are reused for too many requests. For HTTP or SSL services, use the max request option to limit the number of requests sent through a single connection to a load balanced Web server.

Note: You can configure the max request option for HTTP or SSL services only.

To limit the number of client requests per connection by using the command line interface

At the command prompt, type:

set service <ServiceName> -maxReq <Value>

Example

set service Service-HTTP-1 -maxReq 100

Parameters for configuring the maximum requests setting

ServiceName

The name of the service that you are configuring.

maxReq

Maximum number of requests that can be sent on a persistent connection to the service. The default value is 0. The minimum value is 0 and maximum value is 65535. ‘0’ specifies that there is no limit on the maximum requests that are sent on a persistent connection.

To limit the number of client requests per connection by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to configure the maximum number of client requests, and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Under Thresholds, in the Max Requests text box, type the maximum number of client requests (for example, 100).
5. Click OK.

Setting a Threshold Value for the Monitors Bound to a Service

The NetScaler appliance designates a service as UP only when the sum of the weights of all monitors bound to it and that are UP is equal to or greater than the threshold value configured on the service. The weight for a monitor specifies how much that monitor contributes to designating the service to which it is bound as UP.

For example, assume that three monitors, named Monitor-HTTP-1, Monitor-HTTP-2, and Monitor-HTTP-3 respectively, are bound to Service-HTTP-1, and that the threshold configured on the service is three. Suppose the following weights are assigned to each monitor:

- The weight of Monitor-HTTP-1 is 1.
- The weight of Monitor-HTTP-2 is 3.
- The weight of Monitor-HTTP-3 is 1.

The service is marked UP only when one of the following is true:

- Monitor-HTTP-2 is UP.
- Monitor-HTTP-2 and Monitor-HTTP-1 or Monitor-HTTP-3 are UP
- All three monitors are UP.

To set the monitor threshold value on a service by using the command line interface

At the command prompt, type:

set service <name> -monThreshold <Value>

Example

set service Service-HTTP-1 -monThreshold 100

Parameters for configuring the monitor threshold on a service

ServiceName

The name of the service that you are configuring.

monThreshold

Monitoring threshold. The default value is 0. The minimum value is 0 and maximum value is 65535.

To set the monitor threshold value on a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to configure monitor threshold (for example, Service-HTTP-1), and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. In the Monitor Threshold text box, type the monitor threshold.
5. Click OK.

Setting a Timeout Value for Idle Client Connections

You can configure the service with a time-out value to terminate any idle client connections when the configured time elapses. If the client is idle during the configured time, the NetScaler closes the client connection.

To set a timeout value for idle client connections by using the command line interface

At the command prompt, type:

set service <name> -cltTimeout <Value>

Example

set service Service-HTTP-1 -cltTimeout 100

Parameters for setting a timeout value for idle client connections

ServiceName

The name of the service that you are configuring.

cltTimeout

Idle time (in seconds) after which the client connection is terminated. The default value is 180sec for HTTP/SSL-based services and 9000sec for TCP-based services.

To set a timeout value for idle client connections by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to configure the time-out value for client connections, and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Under Idle Time-out (secs), in the Client text box, type the timeout value.
5. Click OK.

Setting a Timeout Value for Idle Server Connections

You can configure a service with a timeout value to terminate any idle server connections when the configured time elapses. If the server is idle for the configured amount of time, the NetScaler appliance closes the server connection.

To set a timeout value for idle server connections by using the command line interface

At the command prompt, type:

set service <name>@ -svrTimeout <Value>

Example

set service Service-HTTP-1 -svrTimeout 100

Parameters for configuring idle server timeout on services

ServiceName

The name of the service that you are configuring.

svrTimeout

Idle time (in seconds) after which the server connection is terminated. The default value is 360. The maximum value is 31536000.

To set a timeout value for idle server connections by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to configure the timeout value for server connections (for example, Service-HTTP-1), and click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Under Idle Time-out (secs), in the Server text box, type a timeout value as a number of seconds (for example, 100).
5. Click OK.

Setting a Limit on the Bandwidth Usage by Clients

In some cases, servers may have limited bandwidth to handle client requests and may become overloaded. To prevent overloading a server, you can specify a maximum limit on the bandwidth processed by the server. The NetScaler appliance forwards requests to a load balanced server only until this limit is reached.

To set a maximum bandwidth limit on a service by using the command line interface

At the command prompt, type:

set service <name> -maxBandwidth <Value>

Example

set service Service-HTTP-1 -maxBandwidth 100

Parameters for configuring a maximum bandwidth on a service

ServiceName

The name of the service that you are configuring.

maxBandwidth

Maximum bandwidth, in Kbps, allowed for forwarding incoming requests to a service. Possible Values: 0-limit of memory. Default: limit of memory.

To set a maximum bandwidth limit on a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details page, select the service for which you want to configure maximum bandwidth usage (for example, Service-HTTP-1), and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Under Thresholds, in the Max Bandwidth (kbits) text box, type the maximum bandwidth (for example, 100).
5. Click OK.

Redirecting Client Requests to a Cache

You can configure a service to redirect client requests to a cache, and forward only those requests that are cache misses to a service chosen by the configured load balancing method.

To set cache redirection on a service by using the command line interface

At the command prompt, type:

set service <name>@ -cacheable <Value>

Example

set service Service-HTTP-1 -cacheable YES

Parameters for configuring caching of client requests

ServiceName

The name of the service that you are configuring.

cacheable

Use the transparent cache redirection virtual server to forward requests to the cache server.

Note: Do not specify this parameter if you set the Cache Type parameter.

Possible values: YES and NO. Default: NO.

To set cache redirection on a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to configure cache redirection, and then click Open.
3. In the Configure Service dialog box, click the Advanced tab.
4. Scroll down, and under Cache Redirection Options, in Cache Type list, select the type of cache (for example, Regular Server).
5. Click OK.

Monitors

To manage a high-traffic load balancing setup, the NetScaler appliance needs to track the state of each load balanced server in near real time, so that it can divert traffic from any load balanced server that is not responding and send that traffic to a load balanced server that is responding. Therefore, a monitor is bound to each service. The monitor is configured to test the service by sending periodic probes to the service. (This is sometimes referred to as performing a health check.) If the monitor receives a timely response to its probes, it marks the service as UP. If it does not receive a timely response to the designated number of probes, it marks the service as DOWN.

The load balancing virtual server does not route requests to services that are DOWN. Those services are removed from its list of available services until they become available again and respond to monitor probes.

You can bind a single monitor or multiple monitors to the same service. If you bind multiple monitors to a service, they each evaluate responses to different types of traffic.

The NetScaler appliance supports built-in monitors to monitor common types of services. It also supports user-created monitors based on the built-in monitors, and allows you to create and configure custom monitors.

The Built-in Monitors

The NetScaler appliance contains a number of built-in monitors that you can use to monitor your services. These built-in monitors handle most of the common protocols. You cannot modify or remove the built-in monitors; you can only bind a built-in monitor to a service and unbind it from the service.

Note: You can create a custom monitor based on a built-in monitor. To learn how to create custom monitors, see Configuring Monitors in a Load Balancing Setup.

Monitoring TCP-based Applications

The NetScaler appliance has two built-in monitors that monitor TCP-based applications: tcp-default and ping-default. When you create a service, the appropriate default monitor is bound to it automatically, so that the service can be used immediately if it is UP. The tcp-default monitor is bound to all TCP services; the ping-default monitor is bound to all non-TCP services.

You cannot delete or modify default monitors. When you bind any other monitor to a TCP service, the default monitor is unbound from the service. The following table lists the monitor types, and the parameters and monitoring processes associated with each type.

Monitor type	Specific parameters	Process
tcp	Not applicable	The NetScaler appliance establishes a 3-way handshake with the monitor destination, and then closes the connection. If the appliance observes TCP traffic to the destination, it does not send TCP monitoring requests. This occurs if LRTM is disabled. By default, LRTM is disabled on this monitor.
http	httprequest [“HEAD /”] - HTTP request that is sent to the service. respcode [200] - A set of HTTP response codes are expected from the service.	The NetScaler appliance establishes a 3-way handshake with the monitor destination. After the connection is established, the appliance sends HTTP requests, and then compares the response code with the configured set of response codes.

tcp-ecv	send [""] - is the data that is sent to the service. The maximum permissible length of the string is 512 K bytes. recv [""] - expected response from the service. The maximum permissible length of the string is 128 K bytes.	The NetScaler appliance establishes a 3-way handshake with the monitor destination. When the connection is established, the appliance uses the send parameter to send specific data to the service and expects a specific response through the receive parameter.
http-ecv	send [""] - HTTP data that is sent to the service recv [""] - the expected HTTP response data from the service	The NetScaler appliance establishes a 3-way handshake with the monitor destination. When the connection is established, the appliance uses the send parameter to send the HTTP data to the service and expects the HTTP response that the receive parameter specifies. (HTTP body part without including HTTP headers). Empty response data matches any response. Expected data may be anywhere in the first 24K bytes of the HTTP body of the response.
ping	Not Applicable	The NetScaler appliance sends an ICMP echo request to the destination of the monitor and expects an ICMP echo response.

To configure built-in monitors for TCP-based applications, see Configuring Monitors in a Load Balancing Setup.

Monitoring SSL Services

The NetScaler appliance has built-in secure monitors, TCPS and HTTPS. You can use the secure monitors to monitor HTTP as well as non-HTTP traffic. The secure monitors work as described below:

- **TCPS.** The NetScaler appliance establishes a TCP connection. After the connection is established, the appliance performs an SSL handshake with the server. After the handshake is over, the appliance closes the connection.
- **HTTPS.** The NetScaler appliance establishes a TCP connection. After the connection is established, the appliance performs an SSL handshake with the server. When the SSL connection is established, the appliance sends HTTP requests over the encrypted channel and checks the response codes.

The following table describes the available built-in monitors for monitoring SSL services.

Monitor type	Probe	Success criteria (Direct condition)
TCP	TCP connection SSL handshake	Successful TCP connection established and successful SSL handshake.
HTTP	TCP connection SSL handshake Encrypted HTTP request	Successful TCP connection is established, successful SSL handshake is performed, and expected HTTP response code in server HTTP response is encrypted.
TCP-ECV	TCP connection SSL handshake (Data sent to a server is encrypted.)	Successful TCP connection is established, successful SSL handshake is performed, and expected TCP data is received from the server.
HTTP-ECV	TCP connection SSL handshake (Encrypted HTTP request)	Successful TCP connection is established, successful SSL handshake is performed, and expected HTTP data is received from the server.

Monitoring FTP Services

To monitor FTP services, the NetScaler appliance opens two connections to the FTP server. It first connects to the control port, which is used to transfer commands between a client and an FTP server. After it receives the expected response, it connects to the data port, which is used to transfer files between a client and an FTP server. Only when the FTP server responds as expected on both connections is it marked UP.

The NetScaler appliance has two built-in monitors for FTP services: the FTP monitor and the FTP-EXTENDED monitor. The FTP monitor checks basic functionality; the FTP-EXTENDED monitor also verifies that the FTP server is able to transmit a file correctly.

Parameter	Specifies
userName	User name used in the probe. Applies to both the FTP and FTP-EXTENDED monitor.
password	Password used in monitoring. Applies to both the FTP and FTP-EXTENDED monitor
fileName	File name to be used for FTP-EXTENDED monitor only.

To configure built-in monitors to check the state of FTP services, see Configuring Monitors in a Load Balancing Setup.

Monitoring SIP Services

A NetScaler ADC has two built-in monitors that you can use to monitor SIP services: the **SIP-UDP** and **SIP-TCP** monitors. A SIP monitor periodically checks the SIP service to which the SIP monitor is bound, by sending SIP request methods to the SIP service. If the SIP service replies with a response code, the monitor marks the service as UP. If the SIP service does not respond, or responds incorrectly, it is marked as DOWN.

Parameter	Specifies
sipURI	SIP addressing schema of the SIP server.
sipmethod	Type of SIP request used to probe the SIP service. Specify one of the following methods: · INVITE · OPTION (the default) · REGISTER
respcode	SIP response code with which the SIP service responds the probe request. Default: 200.

The Session Initiation Protocol (SIP) is designed to initiate, manage, and terminate multimedia communications sessions. It has emerged as the standard for Internet telephony (VoIP). SIP messages can be transmitted over TCP or UDP. SIP messages are of two types: request messages and response messages.

The following table summarizes the structure of SIP messages.

Message type	Components	Components
Request	Method	Invite, Ack, Options, Bye, Cancel, Register
	Request URI	Represents the subject, media type, or urgency of sessions initiated. The common format is: sip:user:password@host:port;uri-parameters?headers
	SIP version	The SIP version being used
Response	SIP version	The SIP version that is being used.

	Status code	A 3-digit integer result code. The possible values are: 1xx: Information Responses. For example: 180, Ringing 2xx: Successful Responses. For example: 200, OK 3xx: Redirection Responses. For example: 302, Moved Temporarily 4xx: Request Failures Responses. For example: 403, Forbidden 5xx: Server Failure Responses. For example: 504, Gateway Time-out 6xx: Global Failure Responses. For example: 600, Busy Everywhere
	Reason-phrase	Textual description of the status code.

The traffic in an SIP-based communication system is routed through dedicated devices and applications (entities). In a multimedia communication session, these entities exchange messages.

One of the most common uses for SIP is VoIP, where SIP is used to set up the session. The following diagram illustrates how the messages and entities in a SIP-based communication system interoperate.

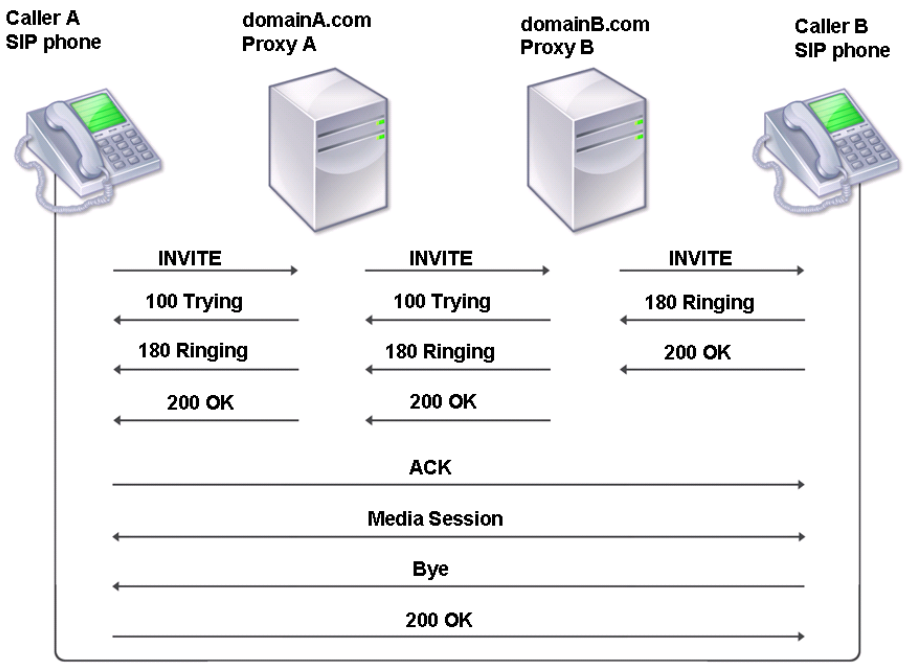


Figure 1. How SIP Works

The entity that initiates the call is referred to as the user agent (UA). The UA can be an SIP softphone (a PC-based application) or a SIP phone.

To initiate a call, the user agent sends an INVITE request to the previously configured SIP proxy server. The INVITE request contains the details of the destination, such as the destination uniform resource identifier (URI) and Call ID. In the diagram, the Caller A (user agent) sends an INVITE request to Proxy A.

When the proxy server receives the INVITE request, it sends a 100 (Trying) response to the user agent, Caller A. It also performs a DNS lookup to locate the SIP proxy server of the destination domain. After the SIP proxy server of the destination domain is located, the SIP proxy at the source domain sends the INVITE request to it. Here, Proxy A sends a 100 (Trying) response to Caller A and an INVITE request to Proxy B.

When the SIP proxy server of the destination domain receives the INVITE request from the SIP proxy server of the source domain, it responds with a 100 (Trying) response. It then sends the INVITE request to the destination user agent. In this case, Proxy B sends a 100 (Trying) response to Proxy A and an INVITE request to Caller B.

When the destination user agent receives the INVITE request, it alerts Caller B and responds with a 180 (ringing) response. This response is routed back to the source user agent through the proxies.

When caller B accepts the call, the destination user agent responds with a 200 (OK) response. This signifies that caller B has answered the call. This response is routed back to the source user agent through the proxies. After the call is set up, the user agents communicate directly without the proxies.

The following table describes the entities of a SIP-based communication system and their roles.

Entity	Role
User Agent (UA)	SIP user agents generate requests and respond to incoming requests. A user agent that generates requests is known as a User Agent Client (UAC). The user agent that responds to requests is known as the User Agent Server (UAS). In the preceding example, Caller A was the UAC and Caller B was the UAS.
Proxy Server	Proxies receive and route SIP requests based on the URI. They can selectively rewrite parts of the request message before forwarding it. They also handle registrations and invitations to user agents, and apply call policies.
Redirect Server	Redirect servers send routing information to the SIP proxy servers.
Registrar Server	Registrar servers provide location information to user agents and proxy servers.
Back-to-Back User Agent (B2BUA)	Back-to-Back User Agents (B2BUA) are combination of UAS and UAC.

You can configure the NetScaler appliance to load balance SIP requests to a group of SIP proxy servers. To do so, you need to create a load balancing virtual server with the load balancing method set to Call-ID hash, and then bind to it the services that are bound to the SIP proxies.

For load balancing to work, you must also configure the SIP proxies so that they do not add private IP addresses or private domains to the SIP header/payload. SIP proxies must add to the SIP header a domain name that resolves to the IP address of the SIP virtual server. Also, the SIP proxies must communicate with a common database to share registration information.

The NetScaler appliance can load balance SIP proxies in either a one-arm DSR configuration or an inline direct server return (DSR) configuration. In a one-arm DSR configuration, the appliance receives SIP requests from user agents and routes the requests to the appropriate SIP proxy by using the configured load balancing method. The SIP proxies send their responses to the destination SIP proxies, bypassing the appliance, as illustrated in the following diagram.

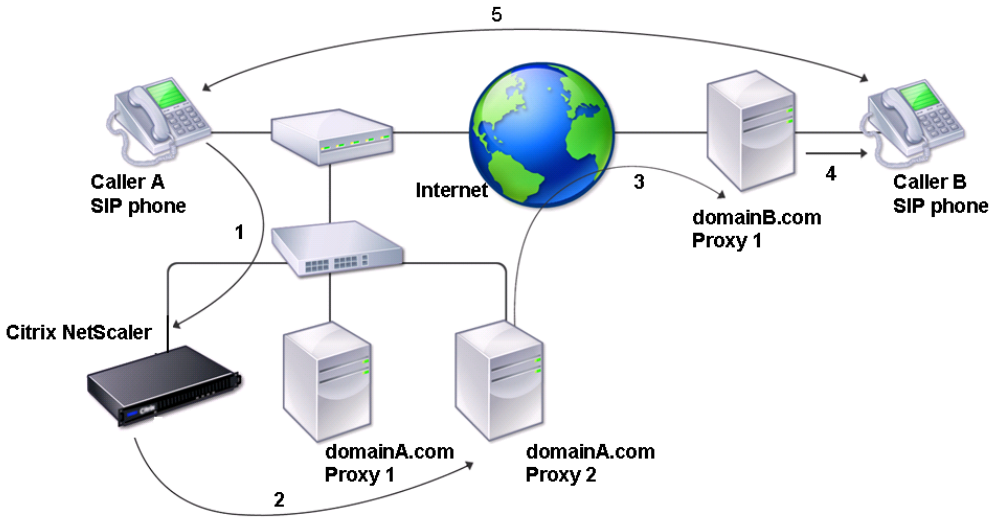


Figure 2. SIP in One-Arm Mode

The flow of requests and responses in this configuration is as follows:

- The user agent, Caller A, sends an INVITE request to the NetScaler. The NetScaler, using a load balancing method, routes the request to Proxy 2.
- Proxy 2 receives the INVITE request from the NetScaler and responds with a 100 (Trying) message.
- Proxy 2 performs a DNS lookup to obtain the IP address of the destination SIP proxy at domainB.com. It then sends the INVITE request to the destination proxy.

- The destination proxy responds with a 100 (Trying) message and sends the INVITE request to the destination user agent, Caller B. The destination user agent, Caller B, begins to ring and responds with a 180 (Ringing) message. This message is sent to Caller A through the NetScaler and the Proxy 2. After the user accepts the call, Caller B responds with a 200 (OK) message that is propagated to Caller A through the NetScaler and the Proxy 2.

- After Caller B accepts the call, the user agents (Caller A and Caller B) communicate independently.

In an inline DSR configuration, the appliance is placed between the router and the SIP proxy, as illustrated in the following diagram.

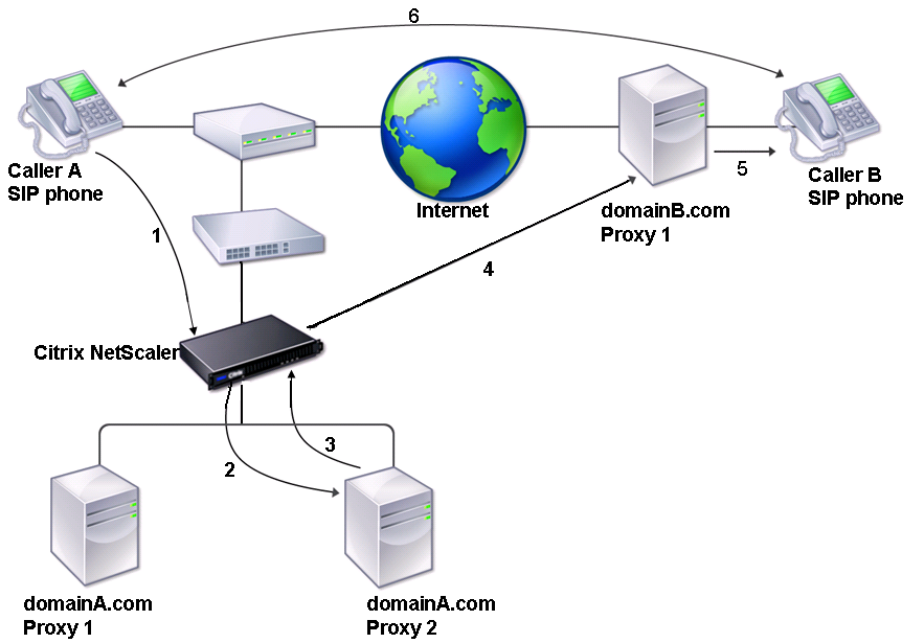


Figure 3. SIP in Inline Mode

The flow of requests and responses is as follows:

- The user agent, Caller A, sends an INVITE request to the appliance. The NetScaler, using a load balancing method, routes the request to Proxy 2.

- Proxy 2 receives the INVITE request from the appliance and responds with a 100 (Trying) message.

- Proxy 2 performs a DNS lookup to obtain the IP address of the destination SIP proxy at domainb.com. It then propagates the INVITE request to the destination proxy through the appliance.

- The appliance performs RNAT, and replaces the source IP address in the INVITE request with the NAT IP address, and then forwards the INVITE request to the destination SIP proxy.

- The destination proxy responds with a 100 (Trying) message and sends the INVITE request to the destination user agent, Caller B. Caller B begins to ring and responds with a 180 (Ringing) message. This message is sent to Caller A through the NetScaler and the Proxy 2. After the user accepts the call, Caller B responds with a 200 (OK) message that is propagated to Caller A through the appliance and Proxy 2.

- After the user accepts the call, the user agents (Caller A and Caller B) communicate independently.

Parameter	Specifies
maxForwards	SIP packet max-forwards. Possible Values: 0-255. Default: 1.
sipMethod	SIP method to be used for the query. Possible values: OPTIONS, INVITE, REGISTER Default value: OPTIONS.
sipURI	SIP method string, sent to the server. For example “OPTIONS sip:sip.test.”
sipregURI	SIP user to be registered.

To configure built-in monitors to check the state of SIP server, see Configuring Monitors in a Load Balancing Setup.

Monitoring RADIUS Services

The NetScaler appliance RADIUS monitor periodically checks the state of the RADIUS service to which it is bound by sending an authentication request to the service. The RADIUS server authenticates the RADIUS monitor and sends a response. By default, the monitor expects to receive a response code of 2, the default Access-Accept response, from the RADIUS server. As long as the monitor receives the appropriate response, it marks the service UP.

Note: RADIUS monitor supports only PAP type authentication.

- If the client authenticated successfully, the RADIUS server sends an Access-Accept response. The default access-accept response code is 2, and this is the code that the appliance uses.
- If the client fails to authenticate successfully (such as when there is a mismatch in the user name, password, or secret key), the RADIUS server sends an Access-Reject response. The default access-reject response code is 3, and this is the code that the appliance uses.

Parameter	Specifies
userName	User name on the RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3 server. This user name is used in the probe.
password	Password used in monitoring RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/LDAP servers.
radKey	Shared secret key value that the RADIUS server uses during client authentication.
radNASid	NAS-ID that is encapsulated in the payload when an access request is made.
radNASip	The IP address that is encapsulated in the payload when an access-request is made. When radNASip is not configured, the NetScaler sends the mapped IP address (MIP) to the RADIUS server as the NAS IP address.

To monitor a RADIUS service, you must configure the RADIUS server to which it is bound as follows:

1. Add the user name and password of the client that the monitor will use for authentication to the RADIUS authentication database.
2. Add the IP address and secret key of the client to the appropriate RADIUS database.
3. Add the IP addresses that the appliance uses to send RADIUS packets to the RADIUS database. If the NetScaler appliance has more than one mapped IP address, or if a subnet IP address (SNIP) is used, you must add the same secret key for all of the IP addresses.

   Caution: If the IP address used by the appliance are not added to the RADIUS database, the RADIUS server will discard all packets.

To configure built-in monitors to check the state of RADIUS server, see Configuring Monitors in a Load Balancing Setup.

Monitoring DNS and DNS-TCP Services

The NetScaler appliance has two built-in monitors that can be used to monitor DNS services: DNS and DNS-TCP. When bound to a service, either monitor periodically checks the state of that DNS service by sending a DNS query to it. The query resolves to an IPv4 or IPv6 address. That IP address is then checked against the list of test IP addresses that you configure. The list can contain up to five IP addresses. If the resolved IP address matches at least one IP address on the list, the DNS service is marked as up. If the resolved IP does not match any IP addresses on the list, the DNS service is marked as down.

Parameter	Parameter
query	The DNS query (domain name) sent to the DNS service that is being monitored. Default value: “\007” If the DNS query succeeds, the service is marked as UP; otherwise, it is marked as DOWN. For a reverse monitor, if the DNS query succeeds, the service is marked as DOWN; otherwise, it is marked as UP. If no response is received, the service is marked as DOWN.
queryType	The type of DNS query that is sent. Possible values: Address, Zone.
IPAddress	List of IP addresses that are checked against the response to the DNS monitoring probe.
IPv6	Select this check box if the IP address uses IPv6 format.

To configure the built-in DNS or DNS-TCP monitors, see Configuring Monitors in a Load Balancing Setup.

Monitoring LDAP Services

The NetScaler appliance has one built-in monitor that can be used to monitor LDAP services: the LDAP monitor. It periodically checks the LDAP service to which it is bound by authenticating and sending a search query to it. If the search is successful, the service is marked UP. If the LDAP server does not locate the entry, a failure message is sent to the LDAP monitor, and the service is marked DOWN.

You configure the LDAP monitor to define the search that it should perform when sending a query. You can use the Base DN parameter to specify a location in the directory hierarchy where the LDAP server should start the test query. You can use the Attribute parameter to specify an attribute of the target entity.

Parameter	Specifies
baseDN	Base name for the LDAP monitor from where the LDAP search must start. If the LDAP server is running locally, the default value of base is dc=netscaler, dc=com.
bindDN	BDN name for the LDAP monitor.
filter	Filter for the LDAP monitor.
password	Password used in monitoring LDAP servers.
attribute	Attribute for the LDAP monitor.

To configure the built-in LDAP monitor, see Configuring Monitors in a Load Balancing Setup.

Monitoring MySQL Services

The NetScaler appliance has one built-in monitor that can be used to monitor MySQL services: the MySQL monitor. It periodically checks the MySQL service to which it is bound by sending a search query to it. If the search is successful, the service is marked UP. If the MySQL server does not respond or the search fails, a failure message is sent to the MySQL monitor, and the service is marked DOWN.

Parameter	Specifies
database	Database that is used for the MySQL monitor.
sqlQuery	SQL query that is used for the MySQL monitor.

To configure built-in MySQL monitor, see Configuring Monitors in a Load Balancing Setup.

Monitoring SNMP Services

The NetScaler appliance has one built-in monitor that can be used to monitor SMNP services: the SNMP monitor. It periodically checks the SNMP agent on the service to which it is bound by sending a query for the enterprise identification ID (OID) that you configure for monitoring. If the query is successful, the service is marked UP. If the SNMP service finds the OID that you specified, the query succeeds and the SNMP monitor marks the service UP. If it does not find the OID, the query fails and the SNMP monitor marks service DOWN.

Parameter	Specifies
SNMPOID	OID that is used for the SNMP monitor.
snmpCommunity	Community that is used for the SNMP monitor.
snmpThreshold	Threshold that is used for the SNMP monitor.
snmpVersion	SNMP version that is used for load monitoring. Possible Values: V1, V2.

To configure the built-in SNMP monitor, see Configuring Monitors in a Load Balancing Setup.

Monitoring NNTP Services

The NetScaler appliance has one built-in monitor that can be used to monitor NNTP services: the NNTP monitor. It periodically checks the NNTP service to which it is bound by connecting to the service and checking for the existence of the newsgroup that you specify. If the newsgroup exists, the search is successful and the service is marked UP. If the NNTP service does not respond or the search fails, the service is marked DOWN.

The NNTP monitor can optionally be configured to post a test message to the newsgroup as well.

Parameter	Specifies
userName	User name on the RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3 server. This user name is used in the probe.
password	Password used in monitoring RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/LDAP servers.
group	Group name to be queried for NNTP monitor.

To configure the built-in NNTP monitor, see Configuring Monitors in a Load Balancing Setup.

Monitoring POP3 Services

The NetScaler appliance has one built-in monitor that can be used to monitor POP3 services: the POP3 monitor. It periodically checks the POP3 service to which it is bound by opening a connection with a POP3 server. If the POP3 server responds with the correct response codes within the configured time period, it marks the service UP. If the POP3 service does not respond, or responds incorrectly, it marks the service DOWN.

Parameter	Specifies
userName	User name POP3 server. This user name is used in the probe.
password	Password used in monitoring POP3 servers.
scriptName	The path and name of the script to execute.
dispatcherIP	The IP address of the dispatcher to which the probe is sent.
dispatcherPort	The port of the dispatcher to which the probe is sent.

To configure the built-in POP3 monitor, see Configuring Monitors in a Load Balancing Setup.

Monitoring SMTP Services

The NetScaler appliance has one built-in monitor that can be used to monitor SMTP services: the SMTP monitor. It periodically checks the SMTP service to which it is bound by opening a connection with it and conducting a series of handshakes to ensure that the server is operating correctly. If the SMTP service completes the handshakes properly, the monitor marks the service UP. If the SMTP service does not respond, or responds incorrectly, it marks the service DOWN.

Parameter	Specifies
userName	User name SMTP server. This user name is used in the probe.
password	Password used in monitoring SMTP servers.
scriptName	The path and name of the script to execute.
dispatcherIP	The IP Address of the dispatcher to which the probe is sent.
dispatcherPort	The port of the dispatcher to which the probe is sent.

To configure the built-in SMTP monitor, see Configuring Monitors in a Load Balancing Setup.

Monitoring RTSP Servers

The NetScaler appliance has one built-in monitor that can be used to monitor RTSP services: the RTSP monitor. It periodically checks the RTSP service to which it is bound by opening a connection with the load balanced RTSP server. The type of connection that it opens, and the response that it expects, differs depending upon the network configuration. If the RTSP service responds as expected within the configured time period, it marks the service UP. If the service does not respond, or responds incorrectly, it marks the service DOWN.

The NetScaler appliance can be configured to load balance RTSP servers using two topologies: NAT-off and NAT-on. RTSP servers send their responses directly to the client, bypassing the appliance. The appliance must be configured to monitor RTSP services differently depending upon which topology your network uses. The appliance can be deployed either in inline or non-inline mode in both NAT-off and NAT-on mode.

In NAT-off mode, the appliance operates as a router: it receives RTSP requests from the client and routes them to the service that it selects using the configured load balancing method. If your load balanced RTSP servers are assigned publicly accessible FQDNs in DNS, the load balanced servers send their responses directly to the client, bypassing the appliance. The following figure demonstrates this configuration.

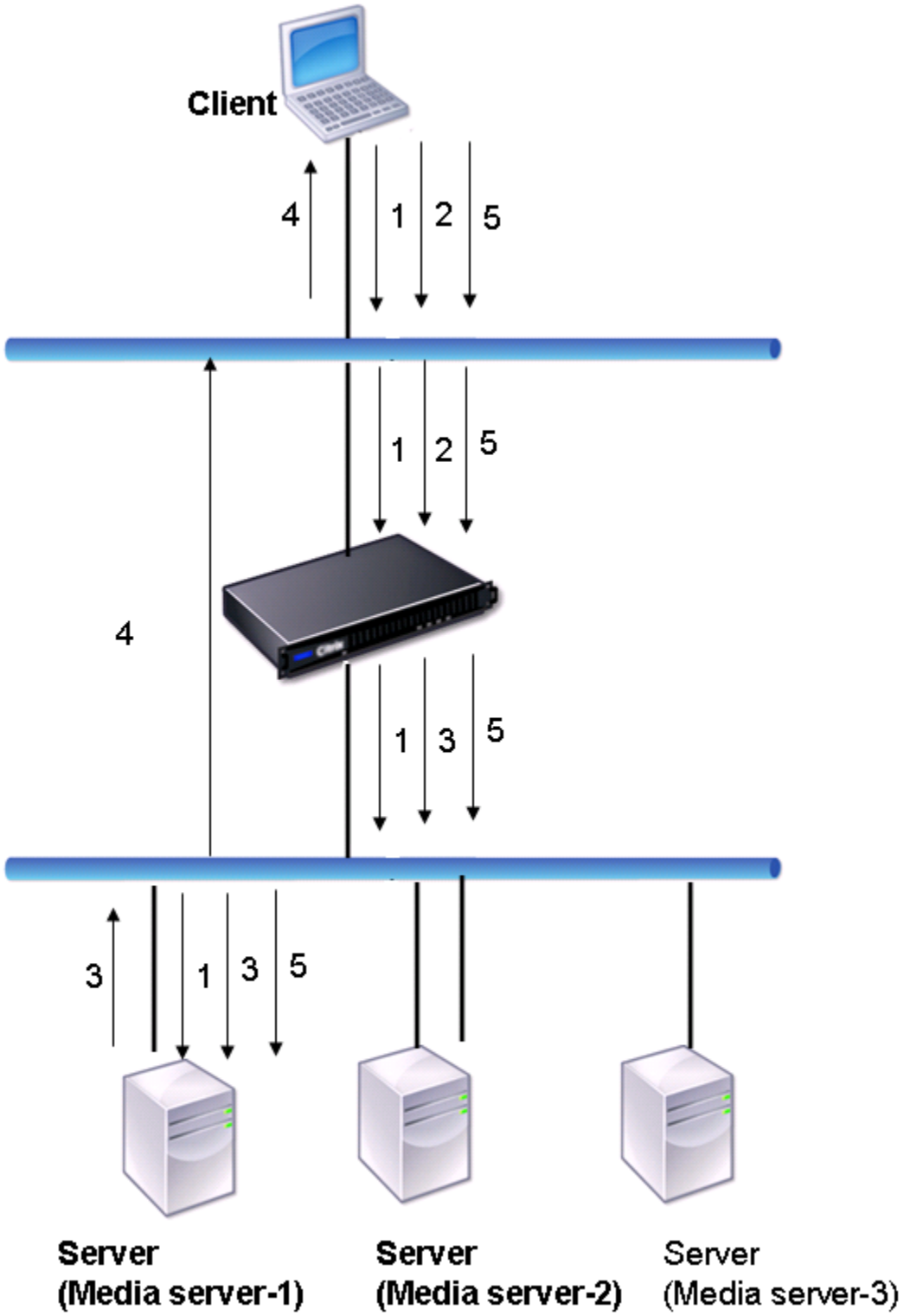


Figure 1. RTSP in NAT-off Mode

The flow of requests and responses in this scenario is as follows:

1. The client sends a DESCRIBE request to the appliance. The appliance uses the configured load balancing method to choose a service, and routes the request to Media Server-1.

2. The client sends a SETUP request to the appliance. If the RTSP session ID is exchanged in the DESCRIBE request, the appliance, using RTSPSID persistence, routes the request to Media Server-1. If the RTSP session ID is exchanged in the SETUP request, the appliance does one of the following:

   - If the RTSP request comes on the same TCP connection, it routes the request to Media Server-1, maintaining persistence.

   - If the request arrives on a different TCP connection, it uses the configured load balancing method to choose a service, and sends the request to that service, not maintaining persistence. This means that the request may be sent to a different service.
3. Media Server-1 receives the SETUP request from the appliance, allocates resources to process the RTSP request, and sends the appropriate session ID to the client.

   Note: The appliance does not perform NAT to identify the RTSP connection, because the RTSP connections bypass it.

4. For subsequent requests, the client then uses the session ID to identify the session and send control messages to the media server. Media Server-1 performs the requested actions, such as play, forward, or rewind.

In NAT-on mode, the appliance receives RTSP requests from the client and routes those requests to the appropriate media server using the configured load balancing method. The media server then sends its responses to the client through the appliance, as illustrated in the following diagram.

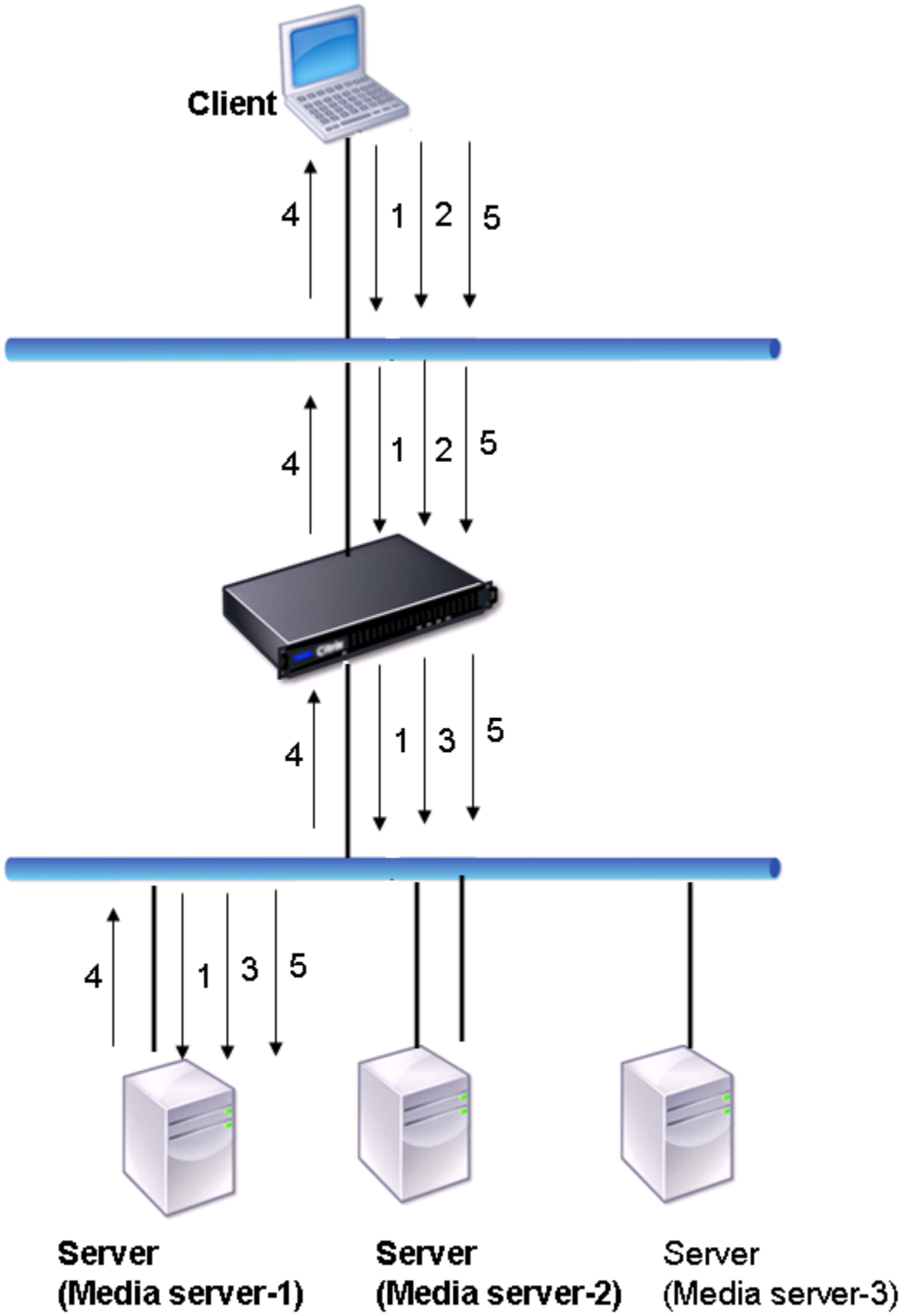


Figure 2. RTSP in NAT-on Mode

The flow of requests and responses in this scenario is as follows:

1. The client sends a DESCRIBE request to the appliance. The appliance uses the configured load balancing method to choose a service, and routes the request to Media Server-1.

2. The client sends a SETUP request to the appliance. If the RTSP session ID is exchanged in the DESCRIBE request, the appliance, using the RTSPSID persistence, routes the request to Media Server-1. If the RTSP session ID is exchanged in the SETUP request, the appliance does one of the following:

   - If the RTSP request comes on the same TCP connection, it routes the request to Media Server-1, maintaining persistence.

   - If the request arrives on a different TCP connection, it uses the configured load balancing method to choose a service, and sends the request to that service, not maintaining persistence. This means that the request may be sent to a different service.
3. Media Server-1 receives the SETUP request from the appliance, allocates resources to process the RTSP request, and sends the appropriate session ID to the client.

4. The appliance performs NAT to identify the client for RTSP data connections, and the RTSP connections pass through the appliance and are routed to the correct client.

5. For subsequent requests, the client then uses the session ID to identify the session and send control messages to the appliance. The appliance uses RTSPSID persistence to identify the appropriate service, and routes the request to Media Server-1. Media Server-1 performs the requested action, such as play, forward, or rewind.

The RTSP monitor uses the RTSP protocol to evaluate the state of the RTSP services. The RTSP monitor connects to the RTSP server and conducts a sequence of handshakes to ensure that the server is operating correctly.

Parameter	Specifies
rtspRequest	The RTSP request string that is sent to the RTSP server (for example, OPTIONS *). The default value is 07. The length of the request must not exceed 163 characters.
respCode	Set of response codes that are expected from the service.

For instructions on configuring an RTSP monitor, see Configuring Monitors in a Load Balancing Setup.

Monitoring the XML Broker Services

The NetScaler appliance has a built-in monitor type, CITRIX-XML-SERVICE, with which you can create monitors to monitor the XML Broker services. The XML Broker services are used by Citrix XenApp. The monitor opens a connection to the service and periodically probes the XML services to which it is bound. If the server responds as expected within the configured time period, the monitor marks the service UP. If the service does not respond, or responds incorrectly, the monitor marks the service DOWN.

To configure a CITRIX-XML-SERVICE monitor, you need to specify the application name in addition to setting the standard parameters. The application name is the name of the application that has to be run to monitor the state of the XML Broker service. The default application is Notepad.

To configure monitors for XML Broker services, see "Configuring Monitors in a Load Balancing Setup."

Monitoring ARP Requests

The NetScaler appliance has one built-in monitor that can be used to monitor ARP requests: the ARP monitor. This monitor periodically sends an ARP request to the service to which it is bound, and listens for the expected response. If it receives the expected response, it marks the service UP. If it receives no response or the wrong response, it marks the service DOWN.

ARP locates a hardware address for a load balanced server when only the network layer address is known. ARP works with IPv4 to translate IP addresses to Ethernet MAC addresses. ARP monitoring is not relevant to IPv6 networks, and is therefore not supported on those networks.

There are no special parameters for the ARP monitor.

For instructions on configuring an ARP monitor, see Configuring Monitors in a Load Balancing Setup.

Monitoring the Access Gateway

The NetScaler appliance has one built-in monitor that can be used to monitor a load-balanced Access Gateway: the CITRIX-AG monitor. This is in addition to two monitors for the Advanced Access Control login page and agent service page, which are described separately. The CITRIX-AG monitor periodically logs on to the Access Gateway service to which it is bound, and awaits the expected responses to its requests. If it receives the expected responses, it marks the service UP. If it receives no response or the wrong responses, it marks the service DOWN.

To configure monitoring of an Access Gateway, you must first create a local user and password for the monitor on the load balanced Access Gateway server that the service is bound to. After you configure the Access Gateway, you then configure the monitor. The monitor logs on to the Access Gateway using the realm and user name. For example, if you configured a realm of LDAP and a user name of user1, the Access Gateway logs on as LDAP/user1.

Note: RSA SecurID authentication is not supported for this monitor. RSA SecurID requires an RSA-generated token as a password, which is not supported on the NetScaler appliance.

Parameter	Specifies
userName	A user name.
password	A password for the username.
secondaryPassword	A secondary password for the username.

For instructions on configuring the CITRIX-AG monitor, see Configuring Monitors in a Load Balancing Setup.

Monitoring the Advanced Access Control Login Page

The NetScaler appliance has one built-in monitor that can be used to monitor the Advanced Access Control (AAC) login page on a load-balanced Access Gateway: the CITRIX-AAC-LOGINPAGE monitor. This monitor periodically logs on to the AAC login page via the Access Gateway service to which it is bound, and awaits the expected response. If it receives the expected response, it marks the service UP. If it receives no response or the wrong response, it marks the service DOWN.

Parameter	Specifies
logonpointName	The URL from which users access corporate resources using the Access Gateway Advanced Edition. This setting controls access to server farms, the Access Interface configuration, and other session-specific settings. It can also be used as a filter within Access Gateway policies.

For instructions on configuring the CITRIX-AAC-LOGINPAGE monitor, see Configuring Monitors in a Load Balancing Setup.

Monitoring the Advanced Access Control Logon Agent Service Page

The NetScaler appliance has one built-in monitor that can be used to monitor the Advanced Access Control (AAC) agent service page on a load-balanced Access Gateway: the CITRIX-AAC-LAS monitor. The Logon Agent Service (LAS) is a service component of Advanced Access Control that requests authentication to the Authentication Service. This monitor periodically logs on to the AAC agent service page via the Access Gateway service to which it is bound, and awaits the expected response. If it receives the expected response, it marks the service UP. If it receives no response or the wrong response, it marks the service DOWN.

Parameter	Specifies
logonpointName	The URL from which users access corporate resources using the Access Gateway advanced edition. This setting controls access to server farms, the Access Interface configuration, and other session-specific settings. It can also be used as a filter within Access Gateway policies.
lasVersion	The version number of the agent.

For instructions on configuring the CITRIX-AAC-LAS monitor, see Configuring Monitors in a Load Balancing Setup.

Monitoring the XenDesktop Delivery Controller Services

In desktop virtualization, the NetScaler appliance can be used to load balance the Web Interface (WI) servers and the XenDesktop Delivery Controller servers deployed by Citrix XenDesktop environment. The NetScaler provides a built-in monitor, CITRIX-XD-DDC monitor, which monitors the XenDesktop Delivery Controller servers. In addition to the health check, you can also verify whether the probe is sent by a valid user of the XenDesktop Delivery Controller server.

The monitor sends a probe to the XenDesktop Delivery Controller server in the form of an XML message. If the server responds to the probe with the identity of the server farm, the probe is considered to be successful and the server's status is marked as UP. If the HTTP response does not have a success code or the identity of the server farm is not present in the response, the probe is considered to be a failure and the server's status is marked as DOWN.

The Validate Credentials option determines the probe to be sent by the monitor to the XenDesktop Delivery Controller server, that is, whether to request only the server name or to also validate the login credentials.

Note: Regardless of whether or not the user credentials (user name, password and domain) are specified on the CITRIX-XD-DDC monitor, the XenDesktop Delivery Controller server validates the user credentials only if the option to validate credentials is enabled on the monitor.

If you use the wizard for configuring the load balancing of the XenDesktop servers, the CITRIX-XD-DDC monitor is automatically created and bound to the XenDesktop Delivery Controller services. If you do not use the wizard, add a monitor of the type CITRIX-XD-DDC.

- For instructions on using the wizard, see Configuring the load balancing of XenDesktop.
- For instructions on adding a monitor, see Creating Monitors.
- For instructions on binding a monitor to a service, see Binding Monitors to Services.

To add an XD-DDC monitor with the validate credentials option by using the command line interface

At the command prompt, type the following commands to add an XD-DDC monitor and verify the configuration:

- add lb monitor <monitorName> <monitorType> -userName <userName> -password <password> -ddcDomain <ddc_domain_name> -validateCred YES
- show lb monitor <monitorName>

Example

```
 > add lb monitor xdddcmon Citrix-xd-ddc -userName Administrator -password E12Dc35450a1 -ddcDomain dh
 Done
> show lb monitor xdddcmon
1) Name......:xdddcmon Type......:CITRIX-XD-DDC State......: ENABLED

Standard parameters:
Interval.....:..5 sec...Retries.....:..3
Response timeout.....:..2 sec...Down time.....:..30 sec
Reverse.....:..NO...Transparent.....:..NO
Secure.....:..NO...LRTM.....:..ENABLED
Action.....:..Not applicable...Deviation.....:..0 sec
Destination IP.....:..Bound service
Destination port.....:..Bound service
Iptunnel.....:..NO
TOS.....:..NO...TOS ID.....:..0
SNMP Alert Retries.....:..0...Success Retries.....:..1
Failure Retries.....:..0

Special parameters:
User Name.....:"Administrator"
Password.....:*****
DDC Domain.....: "dhop"
Done
```

To specify the validate credentials option on an XD-DDC monitor by using the command line interface

At the command prompt, type:

set lb monitor <monitorName> <monitorType> -userName -password -ddcDomain <ddc_domain_name> -validateCred YES

Example

```
 > set lb monitor XD_DDC_21.21.21.22_443_mn CITRIX-xd-ddc -userName Administrator -password D123S1R2A
Done
```

Parameters for configuring a monitor

monitorName

Name to identify the monitor.

monitorType

Type of the monitor. For monitoring XenDesktop Delivery Controller servers, specify CITRIX-XD-DDC.

userName

User name of the user account authorized to log into the XenDesktop Delivery Controller server.

password

Password for the user account.

ddcDomain

Domain in which the XenDesktop Delivery Controller server is present.

validateCred

Verify the validity of the user credentials. Possible values: YES, NO. Default: NO

To configure an XD-DDC monitor with the validate credentials option by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. In the details pane, do one of the following:
   - To add an XD-DDC monitor, click Add.
   - To modify an XD-DDC monitor, select the monitor, and click Open.
3. Type a name for the monitor.
4. Select the monitor type as CITRIX-XD-DDC.
5. On the Special Parameters tab, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring a monitor" as shown:
   - Validate Credentials—validateCred (To specify YES, select the check box.)
   - Name*—monitorName
   - Type*—monitorType
   - User Name*—userName
   - Password*—password
   - Domain Name*—ddcDomain

   *A required parameter
6. Click Create.
7. Select the new monitor, click Open, and verify the settings.

Monitoring Web Interface Services

In desktop virtualization, the NetScaler appliance can be used to load balance the Web Interface (WI) servers and Dynamic Desktop Controller (DDC) servers deployed in the Citrix XenApp and Citrix XenDesktop and environments. The NetScaler appliance has two built-in monitor types for monitoring the WI servers used in these environments.

A CITRIX-WEB-INTERFACE monitor can monitor the Web Interface services efficiently because it monitors a dynamic page at the location specified by the site path. The monitor checks for critical failures in resource availability.

When you configure a CITRIX-WEB-INTERFACE monitor, specify the site path to the location of the http page that displays the data collected by the monitor. To monitor the status of the service, in the specified site path, you can view the data updated dynamically by the monitoring script auth/nocookies.aspx.

Note: End the site path with a slash (/) to indicate that the monitored resource is dynamic.

Note: When you configure the WI-EXTENDED monitor, when specifying the site path, do not enter a slash (/) at the end of the path as the software internally adds a slash at the end of the path. For example, note the following command:

```
add monitor wi CITRIX-WI-EXTENDED -sitepath "/Citrix/DesktopWeb" -username aaa -password bbb -domain c
```

A CITRIX-WI-EXTENDED monitor verifies the logging process with the Web Interface service. This monitor accesses the login page and passes the user name, password, domain, and site path that were specified while configuring the monitor. It verifies the validity of the login credentials, correct configuration of the monitor (for example, the site path), and the connection with the IIS server.

Note: The CITRIX-WI-EXTENDED monitor is supported only for the .NET version of the WI servers. This monitor will not work for the JSP version of the WI servers.

If you use the wizard for configuring load balancing of the XenDesktop servers, a CITRIX-WEB-INTERFACE monitor is automatically created and bound to the WI services. The wizard adds and binds a CITRIX-WEB-INTERFACE monitor by default. If you want to add and bind a CITRIX-WI-EXTENDED monitor, select the Validate Credentials check box and type the necessary data. If you do not use the wizard, add a monitor corresponding to the WI services and bind it to each WI service that you create.

- For instructions on using the wizard, see Configuring XenDesktop for Load Balancing or Configuring XenApp for Load Balancing.
- For instructions on adding a CITRIX-WEB-INTERFACE monitor, see Creating Monitors.
- For instructions on binding a monitor to a service, see Binding Monitors to Services.

To add a WI monitor by using the command line interface

At the command prompt, type:

add lb monitor <monitorName> <monitorType> -sitePath <site_path> -dispatcherIP 127.0.0.1 -dispatcherPort 3013 -userName <username> -password <password> -domain <domain_name>

Examples

add lb monitor mwie CITRIX-WEB-INTERFACE -sitePath "/Citrix/XDWI/"

add lb monitor mwie CITRIX-WI-EXTENDED -sitePath "/Citrix/XDWI/" -dispatcherIP 127.0.0.1 -dispatcherPort 3013 -userName administrator -password d83d154575d426 -encrypted -domain wi

Parameters for configuring WI monitors

monitorName

Name of the monitor.

monitorType

Type of the monitor. Type of monitor. For monitoring WI servers, specify CITRIX-WEB-INTERFACE or CITRIX_WI_EXTENDED.

sitePath

URL of the logon page.

password

Password for the user account. To view the dynamic page, this site path must end with a slash (/).

userName

User name of the user account authorized to log on to the WI server.

password

Password for the user account.

domain

Domain in which the WI server is present.

To add a WI monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. In the details pane, do one of the following:
   - To add a WI monitor, click Add.
   - To modify a WI monitor, select the monitor, and click Open.
3. Type a name for the monitor.
4. Select the monitor type as CITRIX-WEB-INTERFACE or CITRIX-WI-EXTENDED.
5. On the Special Parameters tab, type the site path. To configure the CITRIX-WI-EXTENDED monitor, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring a monitor" as shown:
   - User Name*—userName
   - Password*—password
   - Domain Name*—domain
6. Click Create.
7. Select the new monitor, click Open, and verify the settings.

Custom Monitors

In addition to built-in monitors, you can use custom monitors to check the state of your services. The NetScaler appliance provides several types of custom monitors based on scripts that are included with NetScaler operating system that can be used to determine the state of services based on the load on the service or network traffic sent to the service. These are the inline monitors, user monitors, and load monitors.

With any of these types of monitors, you can use the supplied functionality, or you can create your own scripts and use those scripts to determine the state of the service to which the monitor is bound.

Configuring Inline Monitors

Inline monitors analyze and probe the responses from the services to which they are bound only when those services receive client requests. The inline monitor is of type HTTP-INLINE and can only be configured to work with HTTP and HTTPS services. An inline monitor determines that the service to which it is bound is UP by checking its responses to the requests that are sent to it. When no client requests are sent to the service, the inline monitor probes the service by using the configured URL.

Note: Inline monitors cannot be bound to HTTP or HTTPS Global Server Load Balancing (GSLB) remote or local services because these services represent virtual servers rather than actual load balanced Web servers.

Inline monitors have a time-out value and a retry count when probes fail. You can select any of the following action types for the NetScaler appliance to take when a failure occurs:

- **NONE.** No explicit action is taken. You can view the service and monitor, and the monitor indicates the number of current contiguous error responses and cumulative responses checked.
- **LOG.** Logs the event in ns/syslog and displays the counters.
- **DOWN.** Marks the service down and does not direct any traffic to the service. This setting breaks any persistent connections to the service. This action also logs the event and displays counters.

After the service is down, the service remains DOWN for the configured down time. After the DOWN time elapses, the inline monitor uses the configured URL to probe the service to see if it is available again. If the probe succeeds, the state of the service is changed to UP. Traffic is directed to the service, and monitoring resumes as before.

To configure inline monitors, see Configuring Monitors in a Load Balancing Setup.

Understanding User Monitors

User monitors extend the scope of custom monitors. You can create user monitors to track the health of customized applications and protocols that the NetScaler appliance does not support. The following diagram illustrates how the user monitor works.

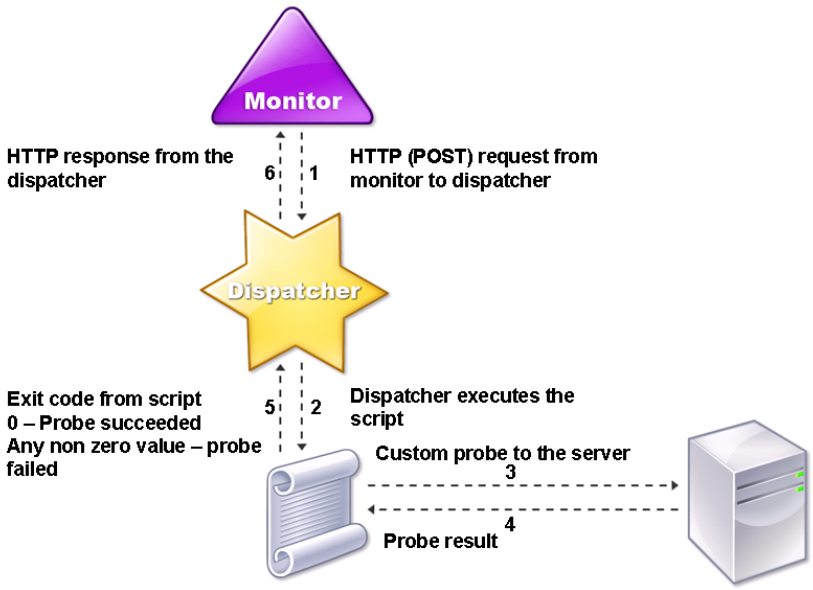


Figure 1. User Monitors

A user monitor requires the following components.

- **Dispatcher.** A process on the appliance that listens to monitoring requests. A dispatcher can be on the loopback IP address (127.0.0.1) and port 3013. Dispatchers are also known as internal dispatchers. A dispatcher can also be a Web server that supports Common Gateway Interface (CGI). Such dispatchers are also known as external dispatchers. They are used for custom scripts that do not run on the FreeBSD environment, such as .NET scripts.

  Note: You can configure the monitor and the dispatcher to use HTTPS instead of HTTP if you enable the “secure” option on the monitor and configure it as an external dispatcher. However, an internal dispatcher understands only HTTP, and cannot use HTTPS.

  In a HA setup, the dispatcher runs on both the primary and secondary NetScaler appliances. The dispatcher remains inactive on the secondary appliance.

- **Script.** The script is a program that sends custom probes to the load balanced server and returns the response code to the dispatcher. The script may return any value to the dispatcher, but if a probe succeeds, the script must return a value of zero (0). The dispatcher considers any other value as probe failure.

  The NetScaler appliance is bundled with sample scripts for commonly used protocols. The scripts exist in the /nsconfig/monitors directory. If you want to add a new script, you add the script there. If you want to customize an existing script, you copy the script with a new name and modify the script.

  For the scripts to function correctly, the name of the script file must not exceed 63 characters, and the maximum number of script arguments is 512. To debug the script, you must run it using the nsumon-debug.pl script from the NetScaler command line. You use the script name (with its arguments), IP address, and the port as the arguments of the nsumon-debug.pl script. Users must use the script name, IP address, port, time-out, and the script arguments for the nsumon-debug.pl script.

To track the status of the server, the monitor sends an HTTP POST request to the configured dispatcher. This POST request contains the IP address and port of the server, and the script that must be executed. The dispatcher executes the script as a child process, with user-defined parameters (if any). Then, the script sends a probe to the server. The script sends the status of the probe (response code) to the dispatcher. The dispatcher converts the response code to an HTTP response and sends it to the monitor. Based on the HTTP response, the monitor marks the service as up or down.

The appliance logs the error messages to the /var/nslog/nsumond.log file when user monitor probes fail. The following table lists the user monitors and the possible reasons for failure.

User monitor type	Probe failure reasons
SMTP	Monitor fails to establish a connection to the server.
NNTP	Monitor fails to establish a connection to the server.
	Missing or invalid script arguments, which may include an invalid number of arguments or argument format.
	Monitor fails to find NNTP group.
LDAP	Monitor fails to establish a connection to the server.
	Missing or invalid script arguments, which may include an invalid number of arguments or argument format.
	Monitor fails to bind to the LDAP server.
	Monitor fails to locate an entry for the target entity in the LDAP server.
FTP	The connection to the server times out.
	Missing or invalid script arguments, which may include an invalid number of arguments or argument format.

	Login fails.
	Monitor fails to find the file on the server.
POP3	Monitor fails to establish a connection to the database.
	Missing or invalid script arguments, which may include an invalid number of arguments or argument format.
	Login fails.
POP3	Monitor fails to establish a connection to the database.
	Missing or invalid script arguments, which may include an invalid number of arguments or argument format.
	Login fails.
	Preparation of SQL query fails.
	Execution of SQL query fails.
SNMP	Monitor fails to establish a connection to the database.
	Missing or invalid script arguments, which may include an invalid number of arguments or argument format.
	Login fails.
	Monitor fails to create SNMP session.
	Monitor fails to find the object identifier.
	The monitor threshold value setting is greater than or equal to the actual threshold of the monitor.
RDP (Windows Terminal Server)	Missing or invalid script arguments, which may include an invalid number of arguments or argument format.
	Monitor fails to create a socket.
	Mismatch in version.
	Monitor fails to confirm connection.

You can view the log file from the NetScaler command line by using the following commands, which open a BSD shell, display the log file on the screen, and then close the BSD shell and return you to the NetScaler command prompt:

```
> shell
root@ns# cat /var/nslog/nsumond.log
root@ns# exit
>
```

User monitors also have a time-out value and a retry count on failure of probes. You can use user monitors with non-user monitors. During high CPU utilization, a non-user monitor enables faster detection of a server failure.

Note: If the user monitor probe times out during high CPU usage, the state of the service remains unchanged.

How to Use a User Monitor to Check Web Sites

You can configure a user monitor to check for specific Web site problems that are reported by HTTP servers using specific HTTP codes. The following table lists the HTTP response codes that this user monitor expects.

HTTP response code	Meaning
200 - success	Probe success.
503 - service unavailable	Probe failure.
404 - not found	Script not found or cannot execute.
500 - Internal server error	Internal error/resource constraints in dispatcher (out of memory, too many connections, unexpected system error, or too many processes). The service is not marked DOWN.
400 - bad request	Error parsing HTTP request.
502 - bad gateway	Error decoding script's response.

You configure the user monitor for HTTP by using the following parameters.

Parameter	Specifies
scriptName	The path and name of the script to execute.
scriptArgs	The strings that are added in the POST data. They are copied to the request verbatim.
dispatcherIP	The IP address of the dispatcher to which the probe is sent.
dispatcherPort	The port of the dispatcher to which the probe is sent.
localfileName	The name of a monitor script file on the local system.
destPath	A particular location on the NetScaler appliance where the uploaded local file is stored.

To create a user monitor to monitor HTTP, see Configuring Monitors in a Load Balancing Setup.

Understanding the Internal Dispatcher

You can use a custom user monitor with the internal dispatcher. Consider a case where you need to track the health of a server based on the presence of a file on the server. The following diagram illustrates this scenario.

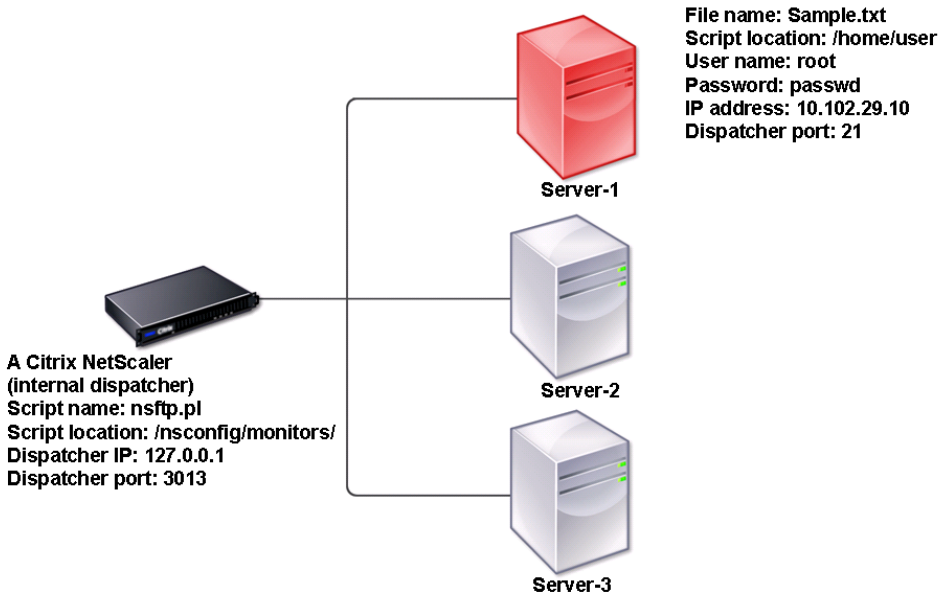
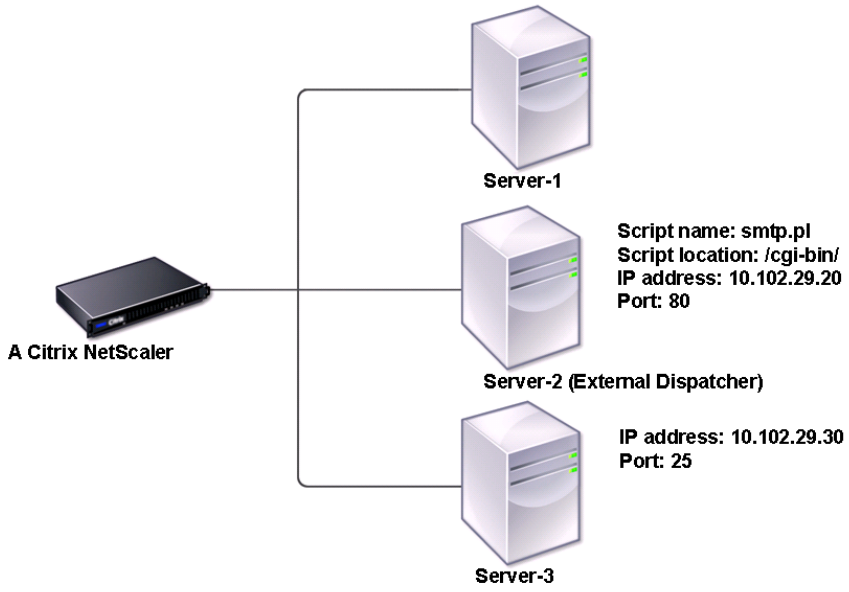


Figure 1. Using a User Monitor with the Internal Dispatcher

A possible solution is to use a Perl script that initiates an FTP session with the server and checks for the presence of the file. You can then create a user monitor that uses the Perl script. The NetScaler includes such a Perl script (nsftp.pl), in the /nsconfig/monitors/ directory.

You can use a user monitor with an external dispatcher. Consider a case where you must track the health of a server based on the state of an SMTP service on another server. This scenario is illustrated in the following diagram.

Figure 2. Using a User Monitor with an External Dispatcher



A possible solution would be to create a Perl script that checks the state of the SMTP service on the server. You can then create a user monitor that uses the Perl script.

Configuring a Custom User Monitor

To configure a custom user monitor, you must first write the script that performs the action that the monitor will use to check the service that is bound to it, and upload the script to the /home/user directory on the NetScaler appliance. Then you create the monitor on the appliance, as described below.

To configure a user monitor by using the command line interface

At the command prompt, type:

add lb monitor <monitorName> USER -scriptname <NameOfScript> –scriptargs <Arguments>

Example

add monitor Monitor-User-1 USER -scriptname nsftp.pl –scriptargs "file=/home/user/sample.txt;user=root;password=passwd"

Understanding Load Monitors

Load monitors use SNMP polled OIDs to calculate load. The load monitor uses the IP address of the service to which it is bound (the destination IP address) for polling. It sends an SNMP query to the service, specifying the OID for a metric. The metrics can be CPU, memory, or number of server connections. The server responds to the query with a metric value. The metric value in the response is compared with the threshold value. The NetScaler appliance considers the service for load balancing only if the metric is less than the threshold value. The service with the lowest load value is considered first.

The following diagram illustrates a load monitor configured for the services described in the basic load balancing setup discussed in Setting Up Basic Load Balancing.

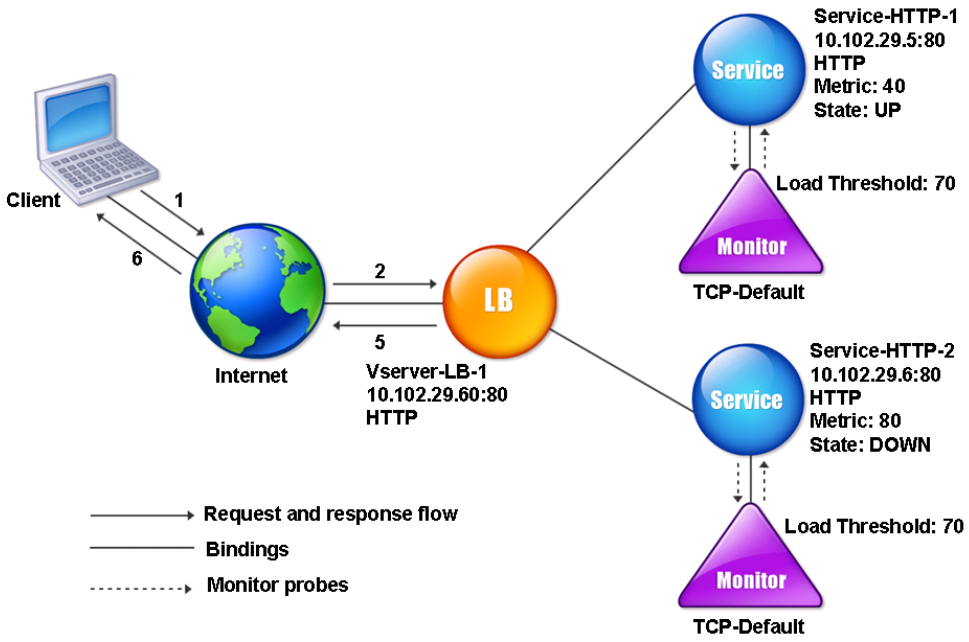


Figure 1. Operation of Load Monitors

Note: The load monitor does not determine the state of the service. It only enables the appliance to consider the service for load balancing.

After you configure the load monitor, you must then configure the metrics that the monitor will use. For load assessment, the load monitor considers server parameters known as metrics, which are defined within the metric tables in the appliance configuration. Metric tables can be of two types:

- **Local.** By default, this table exists in the appliance. It consists of four metrics: connections, packets, response time, and bandwidth. The appliance specifies these metrics for a service, and SNMP queries are not originated for these services. These

metrics cannot be changed.

- **Custom.** A user-defined table. Each metric is associated with an OID.

By default, the appliance generates the following tables:

- NetScaler
- RADWARE
- CISCO-CSS
- LOCAL
- FOUNDRY
- ALTEON

You can either add the appliance-generated metric tables, or you can add tables of your own choosing, as shown in the following table. The values in the metric table are provided only as examples. In an actual scenario, consider the real values for the metrics.

Metric name	OIDs	Weight	Threshold
CPU	1.2.3.4	2	70
Memory	4.5.6.7	3	80
Connections	5.6.7.8	4	90

To calculate the load for one or more metrics, you assign a weight to each metric. The default weight is 1. The weight represents the priority given to each metric. If the weight is high, the priority is high. The appliance chooses a service based on the SOURCEIPDESTIP hash algorithm.

You can also set the threshold value for each metric. The threshold value enables the appliance to select a service for load balancing if the metric value for the service is less than the threshold value. The threshold value also determines the load on each service.

Configuring Load Monitors

To configure a load monitor, first create the load monitor. For instructions on creating a monitor, see Creating Monitors. Next, select or create the metric table to define a set of metrics that determine the state of the server, and (if you create a metric table) bind each metric to the metric table.

To create a metric table by using the command line interface

At the command prompt, type the following commands:

- add lb metricTable <metricTableName>
- bind lb metricTable <metricTableName> <metric> <SNMPOID>

Example

add metricTable Table-Custom-1

bind metricTable Table-Custom-1 1.3.6.1.4.1.5951.4.1.1.41.1.5 11

Parameters for configuring load balancing metric tables

metricTableName

Name of the metric table. This alphanumeric string is required and cannot be changed after the metric table is created. The name must not exceed 31 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

metric

The name of the metric that you are binding to the metric table.

SNMPOID

The SNMP OID for the metric that you are binding to the metric table.

To create a metric table and bind metrics to it by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Metric Tables.
2. In the details pane, click Add.
3. In the Create Metric Table dialog box, in the Metric Table Name text box, type the name of the metric table (for example, Table-Custom-1).
4. Click Create.
5. In the details pane, select the metric table that you just created (for example, Table-Custom-1), and then click Open.
6. In the Configure Metric Table dialog box, in the Metric and SNMP OID text boxes, type the metric and SNMP OID for the metric table (for example, 1.3.6.1.4.1.5951.4.1.1.41.1.5 and 11).
7. Click Add.
8. Click Close. The metric table you created appears in the Metric Tables pane.

Unbinding Metrics from a Metrics Table

You can unbind metrics from a metrics table if the metrics need to be changed, or if you want to remove the metrics table entirely.

To unbind metrics from a metric table by using the command line interface

At the command prompt, type:

unbind lb metricTable <metricTable> <metric>

Example

unbind metricTable Table-Custom-1 1.3.6.1.4.1.5951.4.1.1.41.1.5

To unbind metrics from a metric table by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Metric Tables.
2. In the details pane, select the metric table from which you want to unbind the metrics (for example, Table-Custom-1), click Open.
3. In the Configure Metric Table dialog box, in the Bound Metrics list box, select the metric that you want to unbind from the table (for example, 1.3.6.1.4.1.5951.4.1.1.41.1.5).
4. Click Remove, and then click OK.

You can view the detail of all configured metric tables, such as name and type, to determine whether the metric table is internal or created and configured.

Removing a Load Monitoring Metric Table

You can remove a metric table from the NetScaler configuration.

Note: Before you can remove a metric table, you must unbind all metrics from it.

To remove a metric table by using the command line interface

At the command prompt, type:

rm lb metricTable <metricTable>

Example

rm metricTable <Table-Custom-1>

To remove a metric table by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Metric Tables.
2. In the details pane, select the metric table that you want to remove (for example, Table-Custom-1), and click Remove.
3. In the Remove dialog box, and then click Yes.

You can unbind a metric from a metric table to remove that metric from consideration.

Viewing Metrics Tables

You can view a metrics table and the metrics bound to it.

To view the metric tables by using the command line interface

At the command prompt, type:

show lb metricTable <metricTable>

Example

show metricTable Table-Custom-1

To view the metric tables by using the configuration utility

1. In the navigation pane, expand Load Balancing.
2. Click Metric Tables. The details of the available metric table appear on the Metric Tables pane.

Configuring Monitors in a Load Balancing Setup

To configure monitors on a Web site, you first decide whether to use a built-in monitor or create your own monitor. If you create a monitor, you can choose between creating a monitor based on a built-in monitor, or creating a custom monitor that uses a script that you write to monitor the service. (For more information about creating custom monitors, see Custom Monitors.) Once you have chosen or created a monitor, you then bind it to the appropriate service. The following conceptual diagram illustrates a basic load balancing setup with monitors.

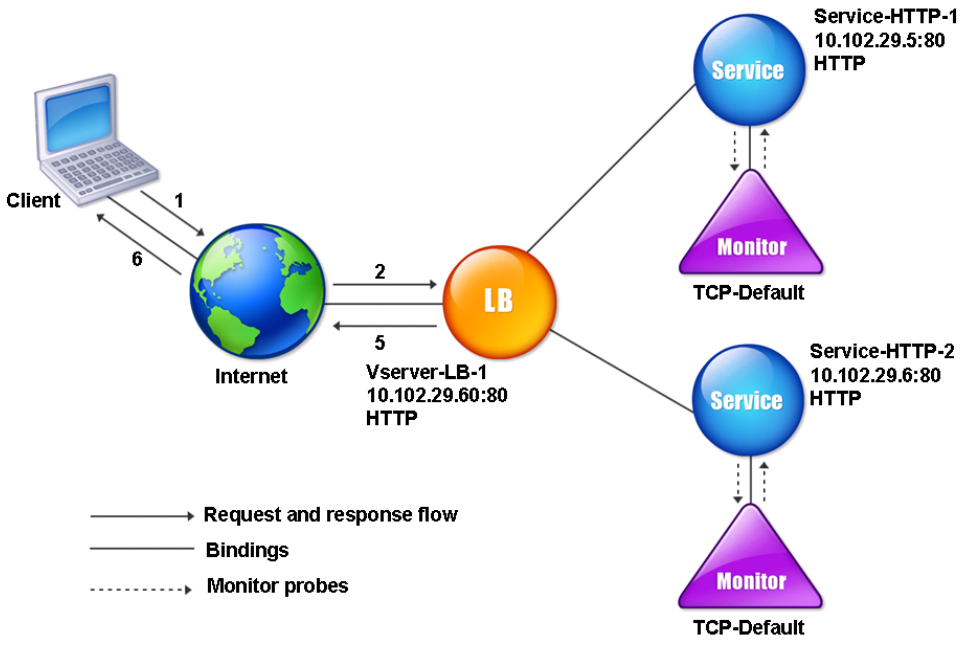


Figure 1. How Monitors Operate

As shown above, each service has a monitor bound to it. The monitor probes the load balanced server via its service. As long as the load balanced server responds to the probes, the monitor marks it UP. If the load balanced server should fail to respond to the designated number of probes within the designated time period, the monitor marks it DOWN.

Creating Monitors

The NetScaler appliance provides a set of built-in monitors. It also allows you to create custom monitors, either based on the built-in monitors or from scratch.

To create a monitor by using the command line interface

At the command prompt, type:

add lb monitor <monitorName> <monitorType> [<interval>]

Example

add lb mon monitor-HTTP-1 HTTP

add lb mon monitor-HTTP-2 TCP 2

Parameters for configuring monitors

monitorName

Name of the monitor. This alphanumeric string is required and cannot be changed after the monitor is created. The name must not exceed 31 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

Type

Type of monitor. The valid options for this parameter are: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, MYSQL-ECV | MSSQL-ECV, CITRIX-WI-EXTENDED.

interval

Frequency at which the probe is sent to a service. The interval must be greater than the response time-out. Possible values: 1 millisecond-160 seconds. Default: 5 seconds.

To create a monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. On the Monitors pane, click Add.
3. In the Create Monitor dialog box, in the Name and Interval text boxes type the name and interval value of the monitor.
4. In the Type list, select the type of the monitor.
5. In the list next to the Interval text box, select Seconds.
6. Click Create, and then click Close. The monitor that you created appears in the Monitors pane.

Binding Monitors to Services

After creating a monitor, you bind it to a service. You can bind one or multiple monitors to a service. If you bind one monitor to a service, that monitor determines whether the service is marked UP or DOWN. If you bind multiple monitors to a service, the NetScaler appliance checks all monitors bound to that service using a calculation that you control, and marks the service UP or DOWN depending on the results.

Note: The destination IP address of a monitor probe can be different than the server IP address and port.

To bind a monitor to a service by using the command line interface

At the command prompt, type:

bind lb monitor <monitorName> <ServiceName>

Example

bind mon monitor-HTTP-1 Service-HTTP-1

To bind a monitor to a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service for which you want to bind the monitor (for example, Service-HTTP-1), and then click Open.
3. On the Monitors tab, in the Available list box, select the monitor you want to bind the service (for example, monitor-HTTP-1), and then click Add.
4. In the Configured box, click OK.

Modifying Monitors

You can modify the settings for any monitor that you created.

Note: Two sets of parameters apply to monitors: those that apply to all monitors, regardless of type, and those that are specific to a monitor type. For information on parameters for a specific monitor type, see the description for that type of monitor.

To modify an existing monitor by using the command line interface

At the command prompt, type:

set lb monitor <monitorName> <type> -interval <interval> -resptimeout <resptimeout>

Example

set mon monitor-HTTP-1 HTTP -interval 50 milli
-resptimeout 20 milli

Parameters for modifying monitor settings

LRTM

State of the response time calculation of probes. Possible values: ENABLED and DISABLED. Default: DISABLED.

deviation

Deviation from the learned response time for dynamic response time monitoring. The maximum value is 348 minutes.

interval

Duration of the interval for which the NetScaler appliance waits before it marks the probe as failed. The response time-out must be less than the value specified in the interval parameter.

The UDP-ECV monitor type does not decide the probe failure using the response time-out. The appliance considers the probe as successful for the UDP-ECV monitor type when the server response matches the criteria that the send and receive options set, or if the response is not received from the server.

The send option specifies the data that must be sent to the server in the probe, and the receive option specifies the server response criteria for the probe to succeed. The

unreachable error from the service causes probe failure. The minimum value is 10 milliseconds. The maximum value is 159 seconds. The default value is 2 seconds.

resptimeout

Monitor response time-out threshold. If the response time for the monitoring probes exceeds the threshold, a trap is sent. The response time-out is given as a percentage. The minimum value is 1 and the maximum value is 100.

retries

Number of consecutive probe failures after which the NetScaler appliance determines the service as DOWN. Possible Values: 3 -127. Default: 3.

successRetries

Number of consecutive successful retries that are required to mark the state of the service as UP. For example, if you set the success retries to 3, when 3 probes succeed consecutively, the service is marked as UP. Possible Values: 1-32. Default: 1.

failureRetries

Number of failed probes that are required to mark the state of the service as DOWN. By default, the NetScaler appliance requires a specific number of consecutive retry failures to mark the state of the service as DOWN. The minimum value for this parameter is 0 and maximum value is 32. The default value is 0. For example, if you set the retries to 10 and the failure retries to 3, when 3 retry probes fail, the service is marked as DOWN.

alertRetries

The number of probe failures after which the NetScaler appliance generates an SNMP trap named MonProbeFailed. This parameter is closely linked to the Retries parameter. For example, if you set Retries to ten and SNMP Alert Retries to three, the appliance generates a MonProbeFailed trap when it detects a third probe failure. You can then take corrective action. However, if the problem is not corrected, the appliance marks the service as DOWN after the tenth probe failure.

You need to set the SNMP Alert Retries parameter to a value lower than the Retries parameter.

Note: The monitor probe failures need not be consecutive.

Possible Values: 0-32. Default: 0.

downTime

Wait duration until the next probe after the service is marked down. Possible Values: 10-160 seconds. Default: 30 seconds.

destIP

IP address to which the probe is sent. If the destination IP address is set to 0, the destination IP address is set to the bound service. Default: 0.0.0.0.

destPort

TCP/UDP port to which the probe is sent. If the destination port is set to 0, the destination port is the port of the service to which the monitor is bound. For a USER monitor, this port is the port sent in the HTTP request to the dispatcher. This option is ignored if the monitor is of the PING type. For information about user monitors, see Understanding User Monitors.

state

State of the monitor. If the monitor is disabled, this monitor type probe is not sent for the services. If the monitor is bound, the state of this monitor is not considered when the state of the service is determined. Possible values: ENABLED and DISABLED. Default: ENABLED.

reverse

Mark a service as DOWN, instead of UP, when probe criteria are satisfied, and as UP instead of DOWN when probe criteria are not satisfied. Possible values: YES, NO. Default: NO.

transparent

The monitor is bound to a transparent device such as a firewall or router. The state of a transparent device depends on the responsiveness of the services behind it. If a transparent device is being monitored, a destination IP address must be specified. The probe is sent to the specified IP address by using the MAC address of the transparent device. Possible values: YES, NO. Default: NO.

secure

State of the secure monitoring of services. SSL handshake is performed on the established TCP connection. Applicable for TCP-based monitors only. Possible values: YES and NO. Default: NO.

application

Name of the application that must be executed to check the state of the service.

sitePath

URL of the logon page.

To modify an existing monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. In the details pane, select the monitor that you want to modify (for example, monitor-HTTP-1), and then click Open.
3. On the Standard Parameters tab, in the Interval and Response Time-out text boxes, type the interval and response timeout values (for example, 50 and 20).
4. In the list next to Interval text box, select the interval (for example, Milli Seconds).
5. In the list next to Response Time-out text box, select the interval (for example, Milli Seconds).
6. Click OK.

Enabling and Disabling Monitors

By default, monitors bound to services and service groups are enabled. When you enable a monitor, the monitor begins probing the services to which it is bound. If you disable a monitor bound to a service, the state the service is determined using the other monitors bound to the service. If the service is bound to only one monitor, and if you disable the monitor, the state of the service is determined using the default monitor.

To enable a monitor by using the command line interface

At the command prompt, type:

enable lb monitor <monitorName>

Example

enable lb mon monitor-HTTP-1

To enable a monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. On the Monitors pane, select the monitor that you want to enable (for example, monitor-HTTP-1), and then click Enable.
3. In the Enable dialog box, click Yes.

To disable a monitor by using the command line interface

At the command prompt, type:

disable lb monitor <monitorName>

Example

disable lb mon monitor-HTTP-1

To disable a monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. On the Monitors pane, select the monitor that you want to disable (for example, monitor-HTTP-1), and then click Disable.
3. In the Disable dialog box, click Yes.

Unbinding Monitors

You can unbind monitors from a service and service group. When you unbind a monitor from the service group, the monitors are unbound from the individual services that constitute the service group. When you unbind a monitor from a service or a service group, the monitor does not probe the service or the service group.

Note: When you unbind all user-configured monitors from a service or a service group, the default monitor is bound to the service and the service group. The default monitors then probes the service or the service groups.

To unbind a monitor from a service by using the command line interface

At the command prompt, type:

unbind lb monitor <monitorName>

Example

unbind mon monitor-HTTP-1 Service-HTTP-1

To unbind a monitor from a service by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, select the service from that you want to unbind the monitor (for example, Service-HTTP-1), click Open.
3. In the Configure Service dialog box, under Configured, select the monitor that you want to unbind from the service (for example, monitor-HTTP-1), and then click Remove.
4. Click OK.

Removing Monitors

After you unbind a monitor that you created from its service, you can remove that monitor from the NetScaler configuration. (If a monitor is bound to a service, it cannot be removed.)

Note: When you remove monitors bound to a service, the default monitor is bound to the service. You cannot remove default monitors.

To remove a monitor by using the command line interface

At the command prompt, type:

rm lb monitor <monitorName> <type>

Example

rm lb monitor monitor-HTTP-1 HTTP

To remove a monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. On the Monitors pane, select the monitor that you want to remove (for example, monitor-HTTP-1), and then click Remove.
3. In the Remove dialog box, click Yes.

Viewing Monitors

You can view the services and service groups that are bound to a monitor. You can verify the settings of a monitor to troubleshoot your NetScaler configuration. The following procedure describes the steps to view the bindings of a monitor to the services and service groups.

To view monitor bindings by using the command line interface

At the command prompt, type:

show lb monbindings <MonitorName>

Example

show lb monbindings monitor-HTTP-1

To view monitor bindings by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. On the Monitors pane, select the monitor for which you want to view the binding information (for example, monitor-HTTP-1), and then click Show Bindings. The binding information for the monitor that you selected appears in the Binding Info for Monitor: monitor-HTTP-1 dialog box.

To view monitors by using the command line interface

At the command prompt, type:

show lb monitor <monitorName>

Example

show lb mon monitor-HTTP-1

To view monitors by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors. The details of the available monitors appear on the Monitors pane.

Closing Monitor Connections

The NetScaler appliance sends probes to the services through the monitors bound to the services. By default, the monitor on the NetScaler and the physical server follow the complete handshake procedure even for monitor probes. However, this procedure adds overhead to the monitoring process and may not be always necessary.

For the TCP monitors, you can configure the NetScaler to close a monitor-probe connection after receiving SYN-ACK from the service. To do so, set the value of the monitorConnectionClose parameter to RESET. If you want the monitor-probe connection to go through the complete procedure, set the value to FIN.

Note: The monitorConnectionClose setting is applicable to all the monitors bound to all the services configured on the NetScaler appliance.

To configure monitor-connection closure by using the command line interface

At the command prompt, type:

set lb parameter -monitorConnectionClose <monitor_conn_close_option>

Example

set lb parameter -monitorConnectionClose RESET

Parameter for configuring monitor-connection closure

monitorConnectionClose

Close (reset) a monitor-probe connection after receiving SYN-ACK from the service, or complete (finish) the handshake before closing the connection. Possible values: RESET, and FIN. Default: FIN.

To configure monitor-connection closure by using the configuration utility

1. In the navigation pane, click Load Balancing.
2. Under Settings, click Configure Load Balancing Parameters.
3. In the Configure Load Balancing Parameters dialog box, for Connection Close for Monitor, select FIN or RESET.
4. Click OK.

Ignoring the Upper Limit on Client Connections for Monitor Probes

Depending on considerations such as the capacity of a physical server, you can specify a limit on the maximum number of client connections made to any service. If you have set such a limit on a service, the NetScaler appliance stops sending requests to the service when the threshold is reached and resumes sending connections to the service after the number of existing connections falls to within the limits. You can configure the NetScaler to skip this check when it sends monitor-probe connections to a service.

Note: You cannot skip the maximum-client-connections check for an individual service. If you specify this option, it applies to all the monitors bound to all the services configured on the NetScaler appliance.

To set the Skip MaxClients for Monitor Connections option by using the command line interface

At the command prompt, type:

set lb parameter -monitorSkipMaxClient (ENABLED|DISABLED)

Example

set lb parameter -monitorSkipMaxClient enabled

Parameter for skipping the maximum-client-connections check

monitorSkipMaxClient

For monitor-probe connections, ignore any maximum-client-connections limits that have been specified for the services being monitored. Possible values: ENABLED and DISABLED. Default: DISABLED.

To set the Skip MaxClients for Monitor Connections option by using the configuration utility

1. In the navigation pane, click Load Balancing.
2. Under Settings, click Configure Load Balancing Parameters.
3. To ignore the upper limit on client connections for monitor probes, in the Configure Load Balancing Parameters dialog box, select the Skip MaxClients for Monitor Connections checkbox.
4. Click OK.

Troubleshooting

I created a user script for monitoring but it is not working.

Resolution: Check the number of arguments in the script. The maximum number of arguments that a script can have is 512. If the number of arguments is more than 512, the script may not work properly. Use the nsumon-debug.pl script from the NetScaler command line to debug the script.

I see a lot of monitor probes and they seem to be increasing the network traffic unnecessarily. Is there a way to turn off the monitor probes?

Resolution: You can turn off the monitor probe connections. To turn off the monitor probe connections, set the value of the monitorConnectionClose parameter to RESET. If you want the monitor probe connection to go through the complete process, set the value to FIN.

I have monitors setup for services, still connections are directed to servers which are DOWN.

Resolution: This probably happens because the probe interval of monitors is long. If a service goes down between two probes, NetScaler appliance does not know about the state of the service and hence would still direct the connection to the service. You, can reduce the time interval for monitor probe.

Managing a Large Scale Deployment

The NetScaler appliance contains several features that are helpful when you are configuring a large load balancing deployment. Instead of configuring virtual servers and services individually, you can create groups of virtual servers and services. You can also create a range of virtual servers and services, and you can translate or mask virtual server and service IP addresses.

You can set persistence for a group of virtual servers. You can bind monitors to a group of services. Creating a range of virtual servers and services of identical type allows you to set up and configure those servers in a single procedure, which significantly shortens the time required to configure those virtual servers and services.

By translating or masking IP addresses, you can take down virtual servers and services, and make changes to your infrastructure, without extensive reconfiguration of your service and virtual server definitions.

Ranges of Virtual Servers and Services

When you configure load balancing, you can create ranges of virtual servers and services, eliminating the need to configure virtual servers and services individually. For example, you can use a single procedure to create three virtual servers with three corresponding IP addresses. When more than one argument uses a range, all of the ranges must be of the same size.

The following are the types of ranges you can specify when adding services and virtual servers to your configuration:

- **Numeric ranges.** Instead of typing a single number, you can specify a range of consecutive numbers.

  For example, you can create a range of virtual servers by specifying a starting IP address, such as 10.102.29.30, and then typing a value for the last byte that indicates the range, such as 34. In this example, five virtual servers will be created with IP addresses that range between 10.102.29.30 and 10.102.29.34.

  Note: The IP addresses of the virtual servers and services must be consecutive.

- **Alphabetic ranges.** Instead of typing a literal letter, you can substitute a range for any single letter, for example, [C-G]. This results in all letters in the range being included, in this case C, D, E, F, and G.

  For example, if you have three virtual servers named Vserver-x, Vserver-y, and Vserver-z, instead of configuring them separately, you can type vserver [x-z] to configure them all.

Creating a Range of Virtual Servers

You create a range of virtual servers as described below.

To create range of virtual servers by using the command line interface

At the command prompt, type one of the following commands:

- add lb vserver <name>@ <protocol> -range <rangeValue> <IPAddress> [<port>]
- add lb vserver <name>@**[**<rangeValue>**]**> <protocol> <IPAddress[<rangeValue>]> [<port>]

Example

add lb vserver Vserver-LB-2 http -range 6 10.102.29.30 80

OR

> add lb vserver vserver[P-R] http 10.102.29.[26-28] 80
vserver "vserverP" added
vserver "vserverQ" added
vserver "vserverR" added
Done

Parameters for configuring virtual server ranges

vServerName

Name of the first virtual server in the range. If you use the second form of this command, you bracket the portion of the vServerName that contains the range.

Note: This command returns an error if the vServerName and IPAddress ranges that you define differ in number of entities.

protocol

The protocol of the virtual server.

rangeValue

The number of entities in the range that you are creating.

Note: Do not use -range and the [ ] range operator in the same command.

IPAddress

The IP address at the beginning of the range that you are defining. If you use the second form of this command, you bracket the portion of the IP address that contains the range.

port

The port of the virtual servers.

To create range of virtual servers by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click Add Range.
3. In the Create Virtual Server (Load Balancing) - Range dialog box, in the Name Prefix, IP Address Range, and Port text boxes, type the virtual server name, IP address with which to begin the range, and port.
4. Select the Network VServer check box, and in Range, type the last value of the virtual server range.
5. In the Protocol drop-down list box, select the protocol type.
6. Click Create, and then click Close. The range of virtual servers you created appears in the Load Balancing Virtual Servers pane.

Creating a Range of Services

You create a range of services as described below. If you specify a range for the service name, specify a range for the IP address too.

To create range of services by using the command line interface

At the command prompt, type the command:

add service <name>@ <IP>@ <protocol> <port>

Example

```
> add service serv[1-3] 10.102.29.[102-104] http 80
service "serv1" added
service "serv2" added
service "serv3" added
 Done
```

Parameters for configuring service ranges

serviceName

Name of the first service in the range. If you use the second form of this command, you bracket the portion of the serviceName that contains the range.

Note: This command returns an error if the serviceName and IPAddress ranges that you define differ in number of entities.

protocol

The protocol of the service.

rangeValue

The number of entities in the range that you are creating.

Note: Do not use -range and the [ ] range operator in the same command.

IPAddress

The IP address at the beginning of the range that you are defining. If you use the second form of this command, you bracket the portion of the IP address that contains the range.

port

The port of the services.

To create range of services by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add Range.
3. In the Create Service (Range) dialog box, in the IP Address Range and Port text boxes, type the start value of the IP address range and the port.
4. In the text box next to the IP Address Range text box, type the last value of the last service (for example, 104).
5. In the Protocol drop-down list box, select the protocol type.
6. Click Create, and then click Close. The range of services you created appears in the Services pane.

Configuring Service Groups

Configuring a service group enables you to manage a group of services as easily as a single service. For example, if you enable or disable any option, such as compression, health monitoring or graceful shutdown, for a service group, the option gets enabled for all the members of the service group.

After creating a service group, you can bind it to a virtual server, and you can add services to the group. You can also bind monitors to service groups.

The members of a service group can be identified by IP address or server name.

Using domain-name based service (DBS) group members is advantageous because you need not reconfigure the member on the NetScaler appliance if the IP address of the member changes. The appliance automatically senses such changes through the configured name server. This feature is particularly useful in cloud scenarios, where the service provider can change a physical server or change the IP address for a service. If you specify a DBS group member, the NetScaler learns the IP address dynamically.

You can bind both IP-based and DBS members to the same service group.

Note: If you use DBS service group members, make sure that either a name server is specified or a DNS server is configured on the NetScaler. A domain name will be resolved into an IP address only if the corresponding address record is present on the NetScaler or the name server.

Creating Service Groups

You can configure up to 4096 service groups on the NetScaler appliance.

To create a service group by using the command line

At the command prompt, type:

add servicegroup <ServiceGroupName> <Protocol>

Example

add servicegroup Service-Group-1 HTTP

Parameters for creating service groups

serviceGroupName

Name of the service group. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

Protocol

Type of service in this group. The valid options are: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, DNS_TCP, ADNS_TCP, RADIUS, MYSQL, MSSQL, RDP.

To create a service group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.
2. In the details pane, click Add.
3. In the Create Service Group dialog box, in the Service Group Name text box, type name of the service group.
4. In the Protocol list, select the protocol type.
5. Click Create, and then click Close. The service group you created appears in the Service Groups pane.

Binding a Service Group to a Virtual Server

When you bind a service group to a virtual server, the member services are bound to the virtual server.

To bind a service group to a virtual server by using the command line interface

At the command prompt, type:

bind lb vserver <name>@ <serviceGroupName>

Example

bind lb vserver Vserver-LB-1 Service-Group-1

To bind a service group to a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server to which you want to bind the service group, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, click the Services Groups tab.
4. In the Active column, select check box next to the service group that you want to bind to the virtual server (for example, Service-Group-1), and then click OK.

Binding a Member to a Service Group

Adding services to a service group enables the service group to manage the servers. You can add the servers to a service group by specifying the IP addresses or the names of the servers.

To add members to a service group by using the command line interface

To configure a service group, at the command prompt, type:

bind servicegroup <serviceGroupName> (<IP>@ | <serverName>) <port>

Examples

bind servicegroup Service-Group-1 10.102.29.30 80

bind servicegroup Service-Group-2 1000:0000:0000:0000:0005:0600:700a:888b 80

bind servicegroup CitrixEdu s1.citrite.net

To add members to a service group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.

2. In the details pane, select the service group to which you want to bind members, and then click Open.

3. In the Configure Service Group dialog box, under Specify Member(s), do one of the following:

   - To add a new IP based service group member, select IP Based.

   - To add a server-name based service group member, select Server Based.

   If you want to add a domain-name based service group member, select **Server Based**. With this option, you can add any server that has been assigned a name, regardless of whether the name is an IP address or a user-assigned name.

4. If adding a new IP based member, in the IP Address text box, type the IP address. If the IP address uses IPv6 format, select the IPv6 check box and then enter the address in the IP Address text box.

   Note: You can add a range of IP addresses. The IP addresses in the range must be consecutive. Specify the range by entering the starting IP address in the IP Address text box (for example, 10.102.29.30). Specify the end byte of the IP address range in the text box under Range (for example, 35). In the Port text box type the port (for example, 80), and then click Add.

5. Click OK.

Binding a Monitor to a Service Group

When you create a service group, the default monitor of the type appropriate for the group is automatically bound to it. Monitors periodically probe the servers in the service group to which they are bound and update the state of the service groups.

You can bind a different monitor of your own choice to the service group.

To bind a monitor to a service group by using the command line interface

At the command prompt, type:

bind serviceGroup <serviceGroupName> -monitorName <string> -monState (ENABLED | DISABLED)

Example

bind serviceGroup Service-Group-1 -monitorName monitor-HTTP-1

To a bind monitor to a service group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.
2. In the details pane, select the service group for which you want to bind monitors, and then click Open.
3. On the Monitors tab, under Available, select a monitor name.
4. Click Add, and then click OK.

Managing Service Groups

You can change the settings of the services in a service group, and you can perform tasks such as enabling, disabling, and removing service groups. You can also unbind members from a service group.

Modifying a Service Group

You can modify attributes of service group members. You can set several attributes of the service group, such as maximum client, SureConnect, and compression. The attributes are set on the individual servers in the service group. You cannot set parameters on the service group such as transport information (IP address and port), weight, and server ID.

Note: A parameter you set for a service group is applied to the member servers in the group, not to individual services.

To modify a service group by using the command line interface

At the command prompt, type the following command with one or more of the optional parameters:

set servicegroup <serviceGroupName> [-type <type>] [-maxClient <maxClient>] [-maxReq <maxReq>] [-cacheable (YES|NO)] [-cip (ENABLED|DISABLED)] [-cipHeader <cipHeader>] [-usip (YES|NO)] [-sc (ON|OFF)] [-sp (ON|OFF)] [-cltTimeout <cltTimeout>] [-svrTimeout <svrTimeout>] [-cka (YES|NO)] [-TCPB (YES|NO)] [-CMP (**YES**|**NO**)] [-maxBandwidth <maxBandwidth>] [-maxThreshold <maxThreshold>] [-state (ENABLED|DISABLED)] [-downStateFlush (ENABLED|DISABLED)

Example

set servicegroup Service-Group-1 -type TRANSPARENT

set servicegroup Service-Group-1 -maxClient 4096

set servicegroup Service-Group-1 -maxReq 16384

set servicegroup Service-Group-1 -cacheable YES

Parameters for modifying service groups

type

Cache server supports the cache type option. Possible values: TRANSPARENT, REVERSE, and FORWARD.

maxClient

Maximum number of open connections to each service in the service group. The default value is 0. The maximum value is 4294967294.

maxReq

Maximum number of requests that can be sent over a persistent connection to a service in the service group. The default value is 0. The minimum value is 0. The maximum value is 65535.

cacheable

Whether a virtual server used for load balancing or content switching feature routes a request to the virtual server (used in transparent cache redirection) on the same appliance before sending it to the configured servers. The virtual server used for transparent cache redirection determines if the request is directed to the cache servers or the configured servers. Do not specify this argument if a cache type is specified. By default, this argument is disabled. Possible values: YES and NO. Default: NO.

cip

Enables or disables insertion of the Client IP header for services in the service group. Possible values: ENABLED and DISABLED. Default: DISABLED.

cipHeader

Client IP header. If client IP insertion is enabled and the client IP header is not specified, then the NetScaler sets the value of the Client IP header.

usip

Use of the client IP address as the source IP address while connecting to the server. By default, the appliance uses a mapped IP address for its server connection. However, with this option, you can tell the appliance to use the client's IP address when it communicates with the server. Possible values: yes and no. Default: no.

sc

The state of SureConnect on this service group. This parameter is supported for legacy purposes only; it has no effect, and the only valid value is OFF. Possible values: ON and OFF. Default: OFF.

sp

Whether surge protection needs to be enabled on this service group. Possible values: ON and OFF. Default: OFF

cltTimeout

Idle time in seconds after which the client connection is terminated. Default: 180. Maximum value: 31536000.

svrTimeout

Idle time in seconds after which the server connection is terminated. The default value is 360. The maximum value is 31536000.

CKA

State of the client keep-alive feature for the services in the service group. Possible values: YES and NO. Default: NO.

TCPB

State of the TCP Buffering feature for the services in the service group. Possible values: YES and NO. Default: NO.

CMP

State of the HTTP Compression feature for the services in the service group. Possible values: YES and NO. Default: NO.

maxBandwidth

Positive integer that identifies the maximum bandwidth in kilobits allowed for the services in the service group.

maxThreshold

Monitoring threshold. The default value is 0. The minimum value is 0 and maximum value is 65535.

state

State of the service group after it is added. Possible values: ENABLED and DISABLED. Default: ENABLED.

DownStateFlush

Delayed cleanup of connections on this service group. Possible values: ENABLED and DISABLED. Default: ENABLED.

Note: Any parameter you set on the service group is applied to the member servers in the group, not to individual services.

To modify a service group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.
2. In the details pane, select the service group that you want to modify (for example, Service-Group-1), and then click Open.
3. Change any of the parameters described in "Parameters for modifying service groups," and then click OK.

Removing a Service Group

When you remove a service group, the servers bound to the group retain their individual settings and continue to exist on the NetScaler.

To remove a service group by using the command line interface

At the command prompt, type:

rm servicegroup <ServiceGroupName>

Example

rm servicegroup Service-Group-1

To remove a service group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.
2. In the details pane, select the service group that you want to remove (for example, Service-Group-1), and then click Remove.
3. In the Remove dialog box, click Yes.

Unbinding a Member from a Service Group

When you unbind a member from the service group, the attributes set on the service group will no longer apply to the member that you unbound. The member services retains its individual settings, however, and continues to exist on the NetScaler.

To unbind members from a service group by using the command line interface

At the command prompt, type:

unbind servicegroup <serviceGroupName> <IP>@ [<port>]

Example

unbind servicegroup Service-Group-1 10.102.29.30 80

To unbind members from a service group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.
2. In the details pane, select the service group from which you want to unbind members, and then click Open.
3. In the Configure Service Group dialog box, in the Configured Members list box, select a service.
4. Click Remove, and then click OK.

Unbinding a Service Group from a Virtual Server

When you unbind a service group from a virtual server, the member services are unbound from the virtual server and continue to exist on the NetScaler appliance.

To unbind a service group from a virtual server by using the command line interface

At the command prompt, type:

unbind lb vserver <name>@ <ServiceGroupName>

Example

unbind lb vserver Vserver-LB-1 Service-Group-1

To unbind a service group from a virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server from which you want to unbind the service group, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, click the Services Group tab.
4. Clear the Active check box next to the service group that you want to unbind from the virtual server (for example, Service-Group-1).
5. Click OK.

Unbinding Monitors from Service Groups

When you unbind a monitor from a service group, the monitor that you unbound no longer monitors the individual services that constitute the group.

To unbind a monitor from a service group using the command line interface

At the command prompt, type:

unbind serviceGroup <serviceGroupName> -monitorName <string>

Example

unbind serviceGroup Service-Group-1 -monitorName monitor-HTTP-1

To unbind a monitor from a service group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.
2. In the details pane, select the service group from which you want to unbind the monitor, click Open.
3. In the Configure Service Group dialog box, click the Monitors tab.
4. Under Configured, select the monitor that you want to unbind from the service group, and then click Remove.
5. Click OK.

Enabling or Disabling a Service Group

When you enable a service group and the servers, the services belonging to the service group are enabled. Similarly, when a service belonging to a service group is enabled, the service group and the service are enabled. By default, service groups are enabled.

After disabling an enabled service, you can view the service using the configuration utility or the command line to see the amount of time that remains before the service goes DOWN.

To disable a service group by using the command line interface

At the command prompt, type:

disable servicegroup <ServiceGroupName>

Example

disable servicegroup Service-Group-1

To disable a service group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.
2. In the Service Groups pane, select the service group that you want to disable, and then click Disable.
3. In the Wait Time dialog box type the wait time value.
4. Click Enter.

To enable a service group by using the command line interface

At the command prompt, type:

enable servicegroup <ServiceGroupName>

Example

```
enable servicegroup Service-Group-1
```

To enable a service group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.
2. In the Service Groups pane, select the service group that you want to enable (for example, Service-Group-1), and then click Enable.
3. In the Enable dialog box, click Yes.

Viewing the Properties of a Service Group

You can view the following settings of the configured service groups: name, IP address, state, protocol, maximum client connections, maximum requests per connection, maximum bandwidth, and monitor threshold. Viewing the details of the configuration can be helpful for troubleshooting your configuration.

To view the properties of a service group by using the command line interface

At the command prompt, type one of the following commands to display the group properties or the properties and the group members:

- show servicegroup <ServiceGroupName>
- show servicegroup <ServiceGroupName> -includemembers

Example

show servicegroup Service-Group-1

To view the properties of a service group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.
2. In the details pane, click the name of the service group whose properties you want to view, and then click Open.

Viewing Service Group Statistics

You can view service-group statistical data, such as rate of requests, responses, request bytes, and response bytes. The NetScaler appliance uses the statistics of a service group, such as these, to balance the load on the services.

To view the statistics of a service group by using the command line interface

At the command prompt, type:

stat servicegroup <ServiceGroupName>

Example

stat servicegroup Service-Group-1

To view the statistics of a service group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.
2. In the details pane, select the service group for which statistics you want to view (for example, Service-Group-1), and then click Statistics. The statistics of the service group you selected appear in a new window.

Load Balancing Virtual Servers Bound to a Service Group

In large-scale deployments, the same service group can be bound to multiple load balancing virtual servers. In such a case, instead of viewing each virtual server to see the service group it is bound to, you can view a list of all the load balancing virtual servers bound to a service group. You can view the following details of each virtual server:

- Name
- State
- IP address
- Port

To display the virtual servers bound to a service group by using the command line interface

At the command prompt, type the following command to display the virtual servers bound to a service group:

show servicegroupbindings <serviceGroupName>

Example

```
> show servicegroupbindings SVCGRPDTLS
SVCGRPDTLS - State :ENABLED
1) Test-pers (10.10.10.3:80) - State : DOWN
2) BRVSERV (10.10.1.1:80) - State : DOWN
3) OneMore (10.102.29.136:80) - State : DOWN
4) LBVIP1 (10.102.29.66:80) - State : UP
Done
>
```

Parameters

serviceGroupName

Indicates the name of the service group whose bindings you want to view.

To display the virtual servers bound to a service group by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.

2. Select a service group, and then click Show Bindings. The Binding details for Service Group box then displays all the load balancing virtual servers bound to the selected service group.

Configuring Automatic Domain Based Service Group Scaling

A domain based service group consists of members whose IP addresses are obtained by resolving the domain names of servers that are bound to the service group. The domain names are resolved by a name server whose details you configure on the appliance. A domain based service group can also include IP-address based members.

The process of name resolution for a domain based server might return more than one IP address. The number of IP addresses in the DNS response is determined by the number of address (A) records configured for the domain name, on the name server. Even if the name resolution process returns multiple IP addresses, only one IP address is bound to the service group. To scale up or scale down a service group, you need to manually bind and unbind additional domain based servers to and from the service group, respectively.

However, you can configure a domain based service group to scale automatically on the basis of the complete set of IP addresses returned by a DNS name server for a domain based server. To configure automatic scaling, when binding a domain based server to a service group, enable the automatic scaling option. Following are the steps for configuring a domain based service group that scales automatically:

- Add a name server for resolving domain names. For more information about configuring a name server on the appliance, see Adding a Name Server.
- Add a domain based server. For information about adding a domain based server, see Adding a Server.
- Add a service group and associate the domain based server to the service group, with the autoscale option set to DNS. For information about adding a service group, see Configuring Service Groups.

When a domain based server is bound to a service group and the automatic scaling option is set on the binding, a UDP monitor and a TCP monitor are automatically created and bound to the domain based server. The two monitors function as resolvers. The TCP monitor is disabled by default, and the appliance uses the UDP monitor to send DNS queries to the name server to resolve the domain name. If the DNS response is truncated (has the TC flag set to 1), the appliance falls back to TCP and uses the TCP monitor to send the DNS queries over TCP. Thereafter, the appliance continues to use only the TCP monitor.

The DNS response from the name server might contain multiple IP addresses for the domain name. With the automatic scaling option set, the appliance polls each of the IP addresses by using the default monitor, and then includes in the service group only those IP addresses that are up and available. After the IP address records expire, as defined by their time-to-live (TTL) values, the UDP monitor (or the TCP monitor, if the appliance has fallen back to using the TCP monitor) queries the name server for domain resolution and includes any new IP addresses in the service group. If an IP address that is part of the service group is not present in the DNS response, the appliance removes that address from the service group after gracefully closing existing connections to the group member, a process during which it does not allow any new connections to be established with the member. If a domain name that resolved successfully in the past results in an NXDOMAIN response, all

the service group members associated with that domain are removed.

Static (IP-address based) members and dynamically scaling domain based members can coexist in a service group. You can also bind members with different domain names to a service group with the automatic scaling option set. However, each domain name associated with a service group must be unique within the service group. You must enable the automatic scaling option for each domain based server that you want to use for automatic service group scaling. If an IP address is common to one or more domains, the IP address is added to the service group only once.

To configure a service group to scale automatically by using the command line interface

At the command prompt, type the following commands to configure the service group and verify the configuration:

- bind serviceGroup <serviceGroupName> <serverName> <port> -autoScale (**YES** | **NO**)
- show serviceGroup <serviceGroupName>

Example

In the following example, `server1` is a domain based server. The DNS response contains multiple IP addresses. Five addresses are available and are added to the service group.

```
> bind serviceGroup servGroup server1 80 -autoScale YES
 Done
> sh servicegroup servGroup
      servGroup - HTTP
       State: ENABLED  Monitor Threshold : 0
           . . .
           . . .
      1)  192.0.2.31:80   State: UP      Server Name: server1 (Auto scale)   Server ID: None Weight: 1

            Monitor Name: tcp-default      State: UP
            Probes: 2      Failed [Total: 0 Current: 0]
            Last response: Success - TCP syn+ack received.

      2)  192.0.2.32:80   State: UP      Server Name: server1 (Auto scale)   Server ID: None Weight: 1

            Monitor Name: tcp-default      State: UP
            Probes: 2      Failed [Total: 0 Current: 0]
            Last response: Success - TCP syn+ack received.

      3)  192.0.2.36:80   State: UP      Server Name: server1 (Auto scale)   Server ID: None Weight: 1

            Monitor Name: tcp-default      State: UP
            Probes: 2      Failed [Total: 0 Current: 0]
            Last response: Success - TCP syn+ack received.

      4)  192.0.2.55:80   State: UP      Server Name: server1 (Auto scale)   Server ID: None Weight: 1
```

```
        Monitor Name: tcp-default       State: UP
        Probes: 2       Failed [Total: 0 Current: 0]
        Last response: Success - TCP syn+ack received.

    5)  192.0.2.80:80   State: UP       Server Name: server1 (Auto scale)    Server ID: None Weight: 1

        Monitor Name: tcp-default       State: UP
        Probes: 2       Failed [Total: 0 Current: 0]
        Last response: Success - TCP syn+ack received.
Done
```

Parameters for configuring a service group to scale automatically

serviceGroupName

The name of the service group to which you want to bind the domain based server.

serverName

The name of the domain based server that you want to bind to the service group.

Port (Port)

The port to which clients must connect.

Autoscale (Auto Scale)

Scale the size of a service group automatically on the basis of the IP addresses that are returned by name resolution process for the domain based server.

To configure a service group to scale automatically by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Service Groups.
2. In the details pane, do one of the following:
   - To create a domain based service, click Add.
   - To bind a domain based server to an existing service group, click the name of the service group, and then click Open.
3. In the Create Service Group or Configure Service Group dialog box, set the following parameters:
   - Server Based (Specifies that you want to bind a domain based server to the service group. A list that contains all the IP addresses and servers configured on the NetScaler appliance appears. Select the domain based server that you want.)
   - Port
   - Auto Scale

   After you set the parameters, to bind the server to the service group, click Add.
4. Click Create or OK, and then click Close.

Translating the IP Address of a Domain-Based Server

To simplify maintenance on the NetScaler appliance and on the domain-based servers that are connected to it, you can configure IP address masks and translation IP addresses. These functions work together to parse incoming DNS packets and substitute a new IP address for a DNS-resolved IP address.

When configured for a domain-based server, IP address translation enables the appliance to locate an alternate server IP address in the event that you take the server down for maintenance or if you make any other infrastructure changes that affect the server.

When configuring the mask, you must use standard IP mask values (a power of two, minus one) and zeros, for example, 255.255.0.0. Non-zero values are only permitted in the starting octets.

When you configure a translation IP for a server, you create a 1:1 correspondence between a server IP address and an alternate server that shares leading or trailing octets in its IP address. The mask blocks particular octets in the original server's IP address. The DNS-resolved IP address is transformed to a new IP address by applying the translation IP address and the translation mask.

For example, you can configure a translation IP address of 10.20.0.0 and a translation mask of 255.255.0.0. If a DNS-resolved IP address for a server is 40.50.27.3, this address is transformed to 10.20.27.3. In this case, the translation IP address supplies the first two octets of the new address, and the mask passes through the last two octets from the original IP address. The reference to the original IP address, as resolved by DNS, is lost. Monitors for all services to which the server is bound also report on the transformed IP address.

When configuring a translation IP address for a domain-based server, you specify a mask and an IP address to which the DNS-resolved IP address is to be translated.

Note: Translation of the IP address is only possible for domain-based servers. You cannot use this feature for IP-based servers. The address pattern can be based on IPv4 addresses only.

To configure a translation IP address for a server by using the command line interface

At the command prompt, type:

add server <name>@ <serverDomainName> -translationIp <translationIPAddress> -translationMask <netMask> -state <ENABLED|DISABLED>

Example

```
add server myMaskedServer www.example.com -translationIp 10.10.10.10 -translationMask
255.255.0.0 -state ENABLED
```

Parameters for configuring translation IP addresses

serverName

Name of the domain-based server.

serverDomainName

Server's domain name (for example, www.example.com).

Note that for IP address translation, the domain name is required.

translationIP

IP address (relevant octets only) to which the resolved ip for the server needs to be translated (for example, 11.12.0.0).

translationMask

Mask determines the number of bits in the translation IP address that are to be considered when applying the transformation.

For example, if you want an original server IP of 10.20.30.40 to be translated to 11.12.30.40, you could specify the mask 255.255.0.0.

To configure a translation IP address for a server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Servers.
2. In the details pane, click Add.
3. In the Create Server dialog box, in the Server Name field, enter a name.
4. In the IP Address / Domain Name field, enter the server's domain name.

   Note: Do not enter an IP address if you are entering a mask.
5. In the Translation IP Address field, enter the IP address of a server on the same subnet.
6. In the Translation Mask field, enter a valid mask (for example, 255.255.0.0).
7. Click Create.

Masking a Virtual Server IP Address

You can configure a mask and a pattern instead of a fixed IP address for a virtual server. This enables traffic that is directed to any of the IP addresses that match the mask and pattern to be rerouted to a particular virtual server. For example, you can configure a mask that allows the first three octets of an IP address to be variable, so that traffic to 111.11.11.198, 22.22.22.198, and 33.33.33.198 is all sent to the same virtual server.

By configuring a mask for a virtual server IP address, you can avoid reconfiguration of your virtual servers due to a change in routing or another infrastructure change. The mask allows the traffic to continue to flow without extensive reconfiguration of your virtual servers.

The mask for a virtual server IP address works somewhat differently from the IP pattern definition for a server described in Translating the IP Address of a Domain-Based Server. For a virtual server IP address mask, a non-zero mask is interpreted as an octet that is considered. For a service, the non-zero value is blocked.

Additionally, for a virtual server IP address mask, either leading or trailing values can be considered. If the virtual server IP address mask considers values from the left of the IP address, this is known as a forward mask. If the mask considers the values to the right side of the address, this is known as a reverse mask.

Note: The NetScaler appliance evaluates all forward mask virtual servers before evaluating reverse mask virtual servers.

When masking a virtual server IP address, you also need to create an IP address pattern for matching incoming traffic with the correct virtual server. When the appliance receives an incoming IP packet, it matches the destination IP address in the packet with the bits that are considered in the IP address pattern, and after it finds a match, it applies the IP address mask to construct the final destination IP address.

Consider the following example:

- Destination IP address in the incoming packet: 10.102.27.189
- IP address pattern: 10.102.0.0
- IP mask: 255.255.0.0
- Constructed (final) destination IP address: 10.102.27.189.

In this case, the first 16 bits in the original destination IP address match the IP address pattern for this virtual server, so this incoming packet is routed to this virtual server.

If a destination IP address matches the IP patterns for more than one virtual server, the longest match takes precedence. Consider the following example:

- Virtual Server 1: IP pattern 10.10.0.0, IP mask 255.255.0.0
- Virtual Server 2: IP pattern 10.10.10.0, IP mask 255.255.255.0
- Destination IP address in the packet: 10.10.10.45.

- Selected virtual server: Virtual Server 2.

The pattern associated with Virtual Server 2 matches more bits than that associated with Virtual Server 1, so IPs that match it will be sent to Virtual Server 2.

Note: Ports are also considered if a tie-breaker is required.

To configure a virtual server IP address mask by using the command line interface

At the command prompt, type:

add lb vserver <name>@ http -ipPattern <ipAddressPattern> -ipMask <ipMask> <listenPort>

Example

Pattern matching based on prefix octets:

add lb vserver myLBVserver http -ippattern 10.102.0.0 -ipmask 255.255.0.0 80

Pattern matching based on trailing octets:

add lb vserver myLBVserver1 http -ippattern 0.0.22.74 -ipmask 0.0.255.255 80

Modify a pattern-based virtual server:

set lb vserver myLBVserver1 -ippattern 0.0.22.74 -ipmask 0.0.255.255

Parameters for masking virtual server IP addresses

name

Name of the load balancing virtual server.

http

Value of HTTP

port

Listen port for the virtual server.

Pattern Based

(Configuration utility only.) Option to select if the virtual server is to be pattern-based.

ippattern

IP address pattern for the virtual server. You must supply either the initial or the trailing octets (for example, 11.11.00.00).

ipmask

Network mask for the IP address. Non-zero values indicate the IP address octets that are to be passed through. (For example, for an IP address pattern of 11.11.00.00, you might specify a mask of 255.255.0.0).

Note: You cannot convert a virtual server with a fixed IP address to a pattern-based virtual server, and you cannot convert a pattern-based virtual server to one with a fixed IP address.

To configure a virtual server IP address mask by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server dialog box, in the Name field, enter a name.
4. In the Protocol field, select the protocol.
5. In the Port field, enter the listen port.
6. In the IP Pattern field, enter a pattern for an IP address. The fixed part of the pattern must be entered in contiguous octets. Enter zeros for the pattern values that can vary in the IP address.
7. In the IP Mask field, enter a standard network mask. Use non-zero mask values for the portion of the IP address that constitutes the fixed part of the pattern.

Configuring Load Balancing for Commonly Used Protocols

In addition to Web sites and Web-based applications, other types of network-deployed applications that use other common protocols often receive large amounts of traffic and therefore benefit from load balancing. Several of these protocols require specific configurations for load balancing to work properly. Among them are FTP, DNS, SIP, and RTSP.

If you configure your NetScaler appliance to use domain names for your servers rather than IPs, you may also need to set up IP translation and masking for those servers.

Load Balancing for a Group of FTP Servers

The NetScaler appliance can be used to load balance FTP servers. FTP requires that the user initiate two connections on two different ports to the same server: the control connection, through which the client sends commands to the server, and the data connection, through which the server sends data to the client. When the client initiates an FTP session by opening a control connection to the FTP server, the appliance uses the configured load balancing method to select an FTP service, and forwards the control connection to it. The load balanced FTP server then opens a data connection to the client for information exchange.

The following diagram describes the topology of a load balancing configuration for a group of FTP servers.

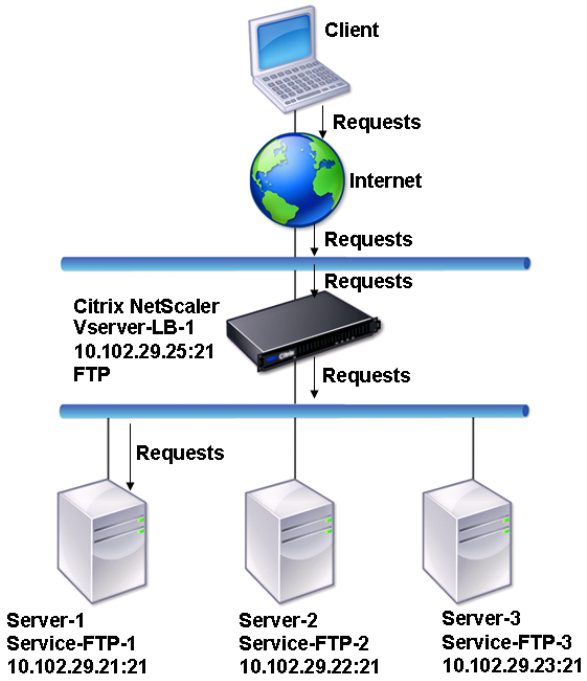


Figure 1. Basic Load Balancing Topology for FTP Servers

In the diagram, the services Service-FTP-1, Service-FTP-2, and Service-FTP-3 are bound to the virtual server Vserver-LB-1. Vserver-LB-1 forwards the client's connection request to one of the services using the least connection load balancing method. Subsequent requests are forwarded to the service that the appliance initially selected for load balancing.

The following table lists the names and values of the basic entities configured on the appliance.

Entity type	Name	IP address	Port	Protocol
Vserver	Vserver-LB-1	10.102.29.25	21	FTP
Services	Service-FTP-1	10.102.29.21	21	FTP
	Service-FTP-2	10.102.29.22	21	FTP
	Service-FTP-3	10.102.29.23	21	FTP
Monitors	FTP	None	None	None

The following diagram shows the load balancing entities, and the values of the parameters that need to be configured on the appliance.

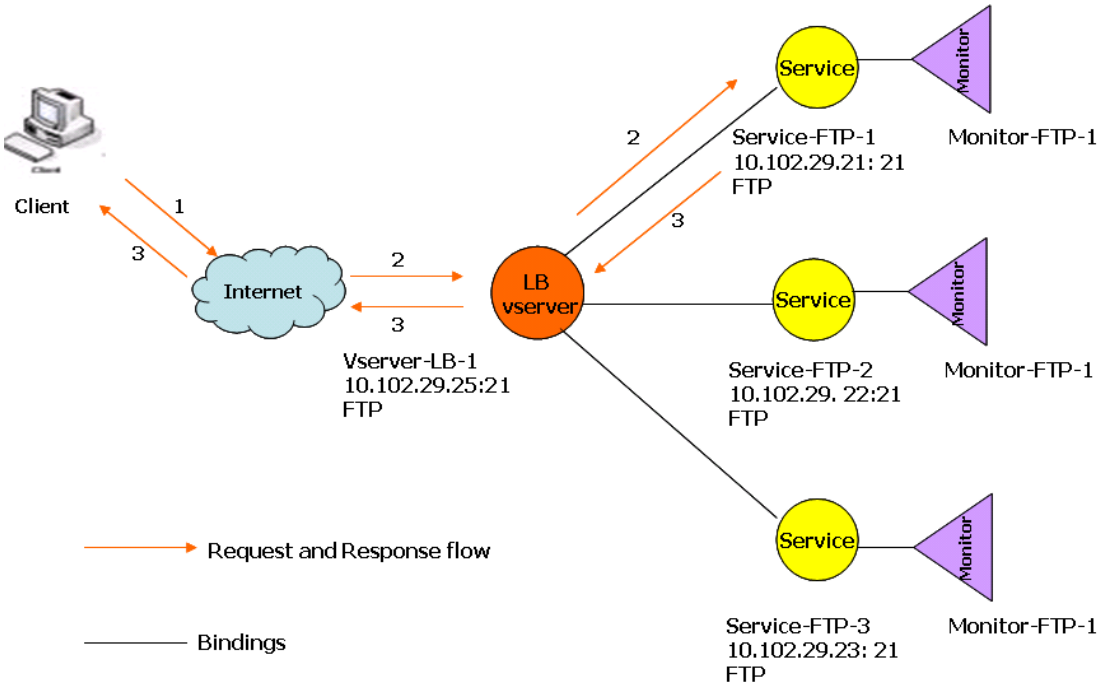


Figure 2. Load Balancing FTP Servers Entity Model

The appliance can also provide a passive FTP option to access FTP servers from outside of a firewall. When a client uses the passive FTP option and initiates a control connection to the FTP server, the FTP server also initiates a control connection to the client. It then initiates a data connection to transfer a file through the firewall.

To create services and virtual servers of type FTP, see Setting Up Basic Load Balancing. Name the entities and set the parameters to the values described in the columns of the previous table. When you configure a basic load balancing setup, a default monitor is bound to the services.

Next, bind the FTP monitor to the services by following the procedure described in the section Binding Monitors to Services.

To create FTP monitors by using the command line interface

At the command prompt, type:

add lb monitor <FTPMonitorName> -interval <Interval> -userName <UserName> -password <Password>

Example

add lb monitor monitor-FTP-1 FTP -interval 360 -userName User -password User

To create FTP monitors by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. In the details pane, click Add.
3. On the Standards Parameters tab, in the Name and Interval text boxes, type the monitor name and interval.
4. In the Type list, select FTP.
5. On the Special Parameters tab, in the User Name and Password text boxes, type User.
6. Click Create, and then click Close. The monitor that you created appears in the Monitors pane.

Load Balancing DNS Servers

When you request DNS resolution of a domain name, the NetScaler appliance uses the configured load balancing method to select a DNS service. The DNS server to which the service is bound then resolves the domain name and returns the IP address as the response. The appliance can also cache DNS responses and use the cached information to respond to future requests for resolution of the same domain name. Load balancing DNS servers improves DNS response times.

The following diagram describes the topology of a load balancing configuration that load balances a group of DNS services.

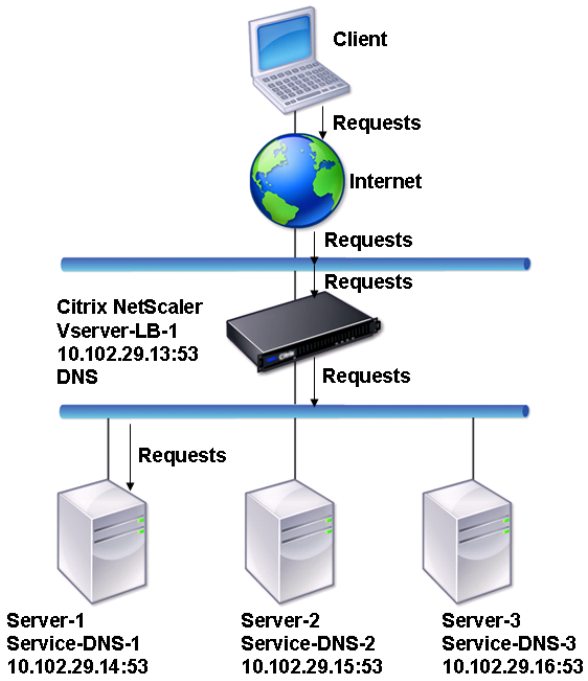


Figure 1. Basic Load Balancing Topology for DNS Servers

In the diagram, the services Service-DNS-1, Service-DNS-2, and Service-DNS-3 are bound to the virtual server Vserver-LB-1. The virtual server Vserver-LB-1 forwards client requests to a service using the least connection load balancing method. The following table lists the names and values of the basic entities configured on the appliance.

Entity type	Name	IP address	Port	Protocol
Virtual Server	Vserver-LB-1	10.102.29.13	53	DNS
Services	Service-DNS-1	10.102.29.14	53	DNS
	Service-DNS-2	10.102.29.15	53	DNS
	Service-DNS-3	10.102.29.16	53	DNS

Monitors	monitor-DNS-1	None	None	None

The following diagram shows the load balancing entities and the values of the parameters that need to be configured on the appliance.

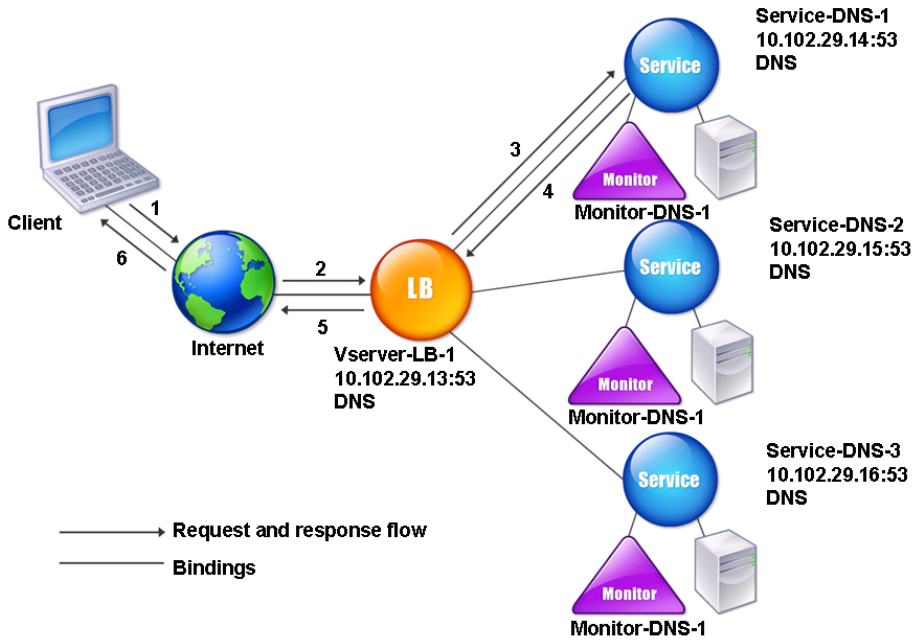


Figure 2. Load Balancing DNS Servers Entity Model

To configure a basic DNS load balancing setup, see Setting Up Basic Load Balancing. Follow the procedures to create services and virtual servers of type DNS, naming the entities and setting the parameters using the values described in the previous table. When you configure a basic load balancing setup, the default ping monitor is bound to the services. For instructions on binding a DNS monitor to DNS services, you can also see Binding Monitors to Services.

The following procedure describes the steps to create a monitor that maps a domain name to the IP address based on a query.

To configure DNS monitors by using the command line interface

At the command prompt, type:

add lb monitor <monitorName> DNS -query <domainName> -queryType <**Address**|**ZONE**> -IPAddress <ipAddress>

Example

```
add lb monitor monitor-DNS-1 DNS -query www.citrix.com -queryType Address -IPAddress 10.102.29.66

add lb monitor monitor-DNS-2 DNS -query www.citrix2.com -queryType Address -IPAddress
1000:0000:0000:0000:0005:0600:700a::888b-888d
```

To configure DNS monitors by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. In the details pane, click Add.
3. In the Create Monitor dialog box, in the Name and Interval text boxes, type a monitor name and a monitoring interval.
4. Select the unit of time for the interval in the drop-down menu.
5. In the Type list, select DNS.
6. Click the Special Parameters tab, in the Query text box type the domain name query to send to the DNS service (for example, www.mycompany.com), and in the Query Type list box, select ADDRESS or ZONE.
7. In the text box below the Query Type list box, type an IP address that is to be checked against the response to the DNS monitoring query (for example, 10.102.29.66), and click Add.

   Note: If you want to enter an IPv6 address, select the IPv6 check box before entering the address.
8. Click Create, and then click Close. The monitor that you created appears in the Monitors pane.

Load Balancing Domain-Name Based Services

When you create a service for load balancing, you can provide an IP address. Alternatively, you can create a server using a domain name. The server name (domain name) can be resolved using an IPv4 or IPv6 name server, or by adding an authoritative DNS record (A record for IPv4 or AAAA record for IPv6) to the NetScaler configuration.

When you configure services with domain names instead of IPs, if you change the IP address of a server in your load balancing setup, the name server resolves the domain name to the new IP address. The monitor runs a health check on the new IP address, and updates the service IP address only when the IP address is found to be healthy.

Note: When you change the IP address of a server, the corresponding service is marked down for the first client request. The name server resolves the service IP address to the changed IP address for the next request, and the service is marked UP.

Domain-name based services have the following restrictions:

- The maximum domain name length is 255 characters.
- The Maximum Client parameter is used to configure a service that represents the domain name-based server. For example, a maxClient of 1000 is set for the services bound to a virtual server. When the connection count at the virtual server reaches 2000, the DNS resolver changes the IP address of the services. However, because the connection counter on the service is not reset, the virtual server cannot take any new connections until all the old connections are closed.
- When the IP address of the service changes, persistence is difficult to maintain.
- If the domain name resolution fails due to a timeout, the appliance uses the old information (IP address).
- When monitoring detects that a service is down, the appliance performs a DNS resolution on the service (representing the domain name-based server) to obtain a new IP address.
- Statistics are collected on a service and are not reset when the IP address changes.
- If a DNS resolution returns a code of “name error” (3), the appliance marks the service down and changes the IP address to zero.

When the appliance receives a request for a service, it selects the target service. This way, the appliance balances load on your services. The following diagram describes the topology of a load balancing configuration that load balances a group of domain-name based servers (DBS).

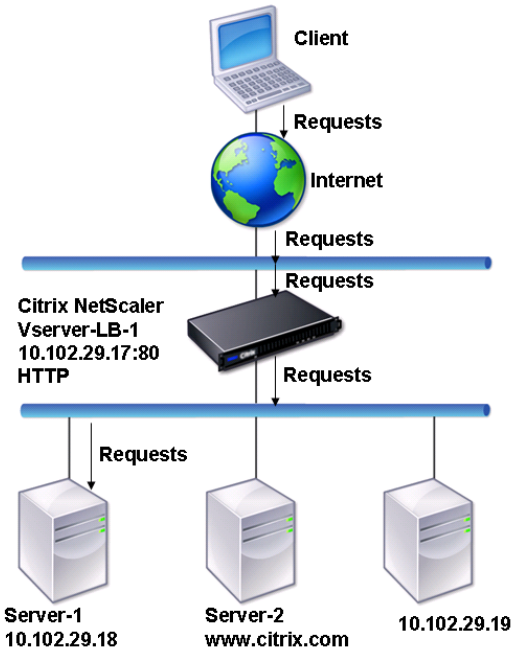


Figure 1. Basic Load Balancing Topology for DBS Servers

The services Service-HTTP-1, Service-HTTP-2, and Service-HTTP-3 are bound to the virtual server Vserver-LB-1. The vserver Vserver-LB-1 uses the least connection load balancing method to choose the service. The IP address of the service is resolved using the name server Vserver-LB-2.

The following table lists the names and values of the basic entities configured on the appliance.

Entity type	Name	IP address	Port	Protocol
Virtual Server	Vserver-LB-1	10.102.29.17	80	HTTP
	Vserver-LB-2	10.102.29.20	53	DNS
Servers	server-1	10.102.29.18	80	HTTP
	server-2	www.citrix.com	80	HTTP
Services	Service-HTTP-1	server-1	80	HTTP
	Service-HTTP-2	server-2	80	HTTP
	Service-HTTP-2	10.102.29.19	80	HTTP
Monitors	Default	None	None	None
Name Server	None	10.102.29.19	None	None

The following diagram shows the load balancing entities and the values of the parameters that need to be configured on the appliance.

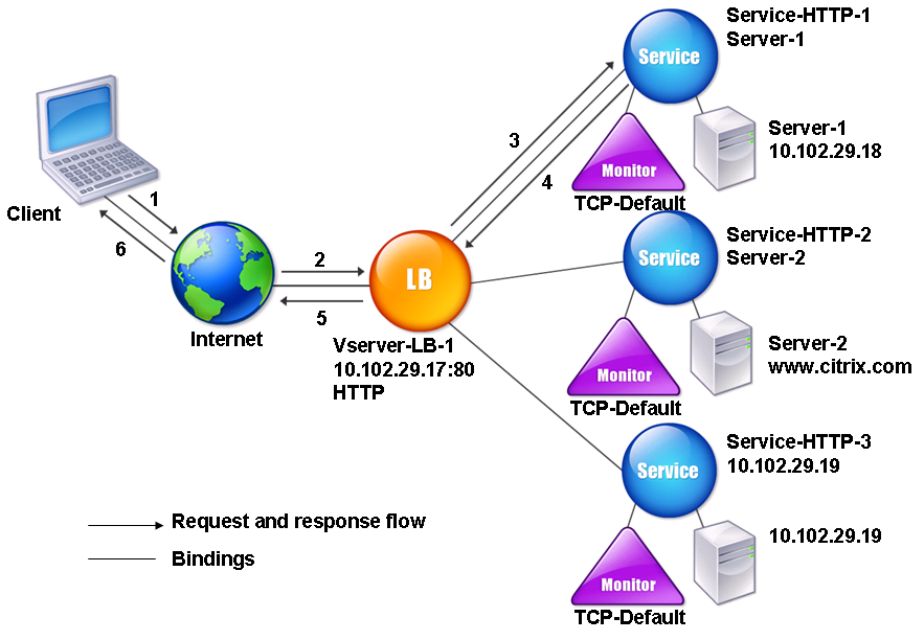


Figure 2. Load Balancing DBS Servers Entity Model

To configure a basic load balancing setup, see Setting Up Basic Load Balancing. Create the services and virtual servers of type HTTP, and name the entities and set the parameters using the values described in the previous table.

You can add, remove, enable, and disable external name servers. You can create a name server by specifying its IP address, or you can configure an existing virtual server as the name server.

To add a name server by using the command line interface

At the command prompt, type:

add dns nameServer <dnsVserverName>

Example

add dns nameServer Vserver-LB-2

To add a name server by using the configuration utility

1. In the navigation pane, expand DNS, and then click Name Servers.
2. In the details pane, click Add.
3. In the Create Name Server dialog box, select DNS Virtual Server.
4. In the DNS Virtual Server drop-down list, select the server name.

   Note: Click New if you want to create a new load balancing vserver. The Create Virtual Server (Load Balancing) dialog box appears.
5. Click Create, and then click Close.

You can also add an authoritative name server that resolves the domain name to an IP address.

Load Balancing a Group of SIP Servers

The Session Initiation Protocol (SIP) is designed to initiate, manage, and terminate multimedia communications sessions. It has emerged as the standard for Internet telephony (VoIP). SIP messages can be transmitted over TCP or UDP. SIP messages are of two types: request messages and response messages.

The traffic in a SIP based communication system is routed through dedicated devices and applications (entities). In a multimedia communication session, these entities exchange messages. The following figure shows a basic SIP based communication system:

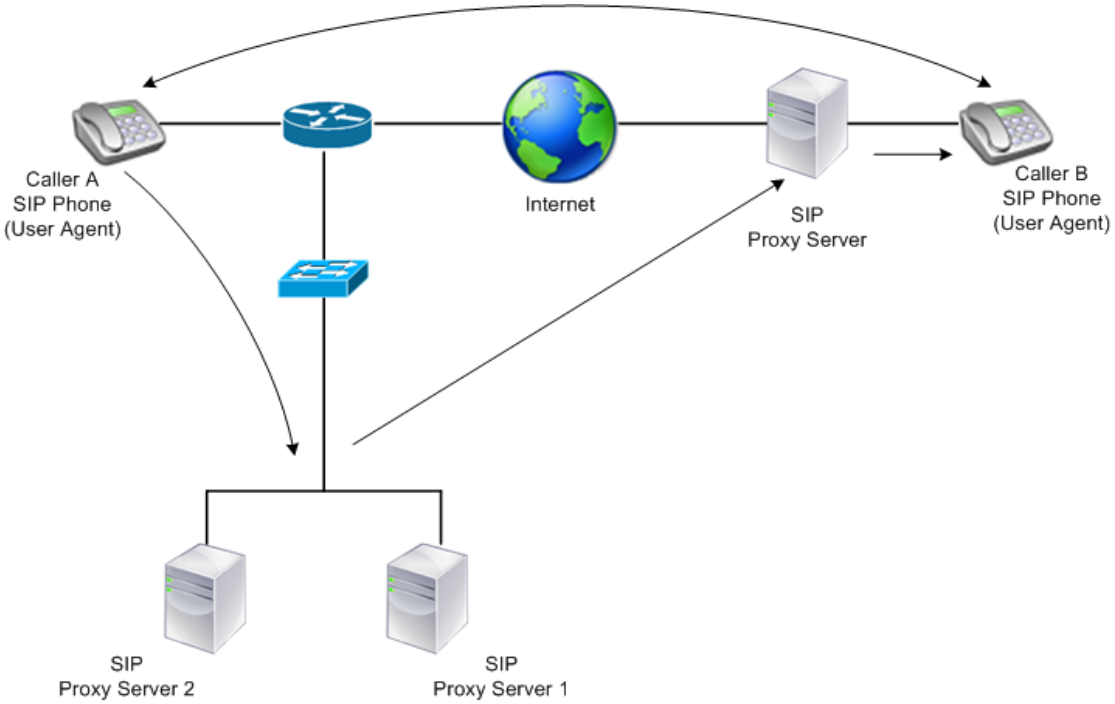


Figure 1. SIP Based Communication System

A NetScaler ADC enables you to load balance SIP messages over UDP or over TCP (including TLS). You can configure the NetScaler ADC to load balance SIP requests to a group of SIP proxy servers. To do so, you create a load balancing virtual server with the load balancing method and the type of persistence set to one of the following combinations:

- Call-ID hash load balancing method with no persistence setting
- Call-ID based persistence with least connection or round robin load balancing method
- Rule based persistence with least connection or round robin load balancing method

Also, by default, the NetScaler ADC appends RPORT to the via header of the SIP request, so that the server sends the response back to the source IP address and port from which the request originated.

Note: For load balancing to work, you must configure the SIP proxies so that they do not add private IP addresses or private domains to the SIP header/payload. SIP proxies must add to the SIP header a domain name that resolves to the IP address of the SIP virtual server. Also, the SIP proxies must communicate with a common database to share registration information.

Server Initiated Traffic

For SIP-server initiated outbound traffic, configure RNAT on the NetScaler ADC so that the private IP addresses used by the clients are translated into public IP addresses.

If you have configured SIP parameters that include the RNAT source or destination port, the appliance compares the values of the source and destination ports of the request packets with the RNAT source port and RNAT destination port. If one of the values matches, the appliance updates the VIA header with RPORT. The SIP response from the client then traverses the same path as the request.

For server-initiated SSL traffic, the NetScaler ADC uses a built-in certificate-key pair. If you want to use a custom certificate-key pair, bind the custom certificate-key pair to the NetScaler internal service named **nsrnatsip-127.0.0.1-5061**.

Support for Policies and Expressions

The NetScaler default expressions language contains a number of expressions that operate on Session Initiation Protocol (SIP) connections. These expressions can be bound only to SIP based (`sip_udp`, `sip_tcp` or `sip_ssl`) virtual servers, and to global bind points. You can use these expressions in content switching, rate limiting, responder, and rewrite policies.

For more information, see SIP Expressions.

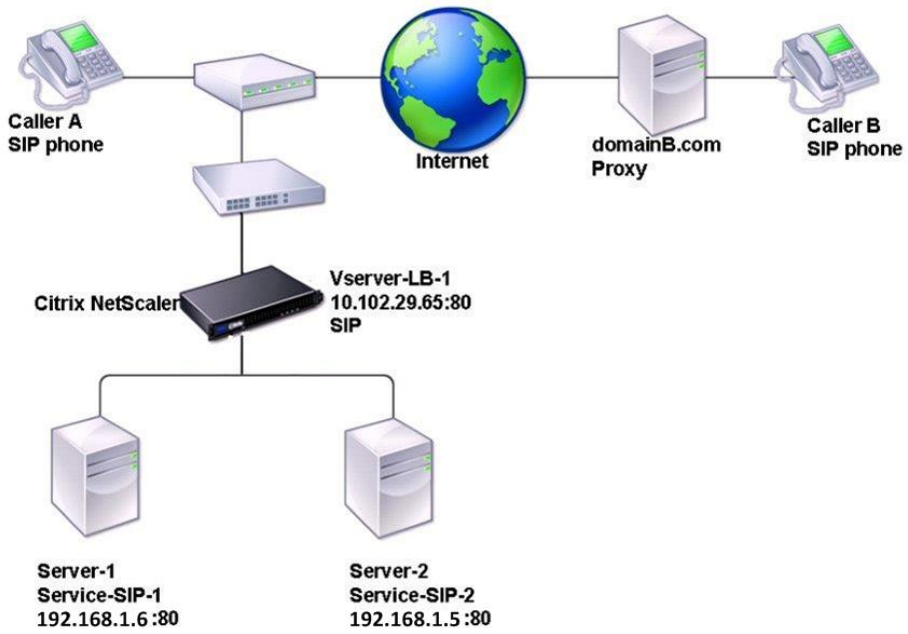


Figure 2. SIP Load Balancing Topology

In the example, the services Service-SIP-1 and Service-SIP-2 are bound to the virtual server Vserver-LB-1. The following table lists the names and values of the entities that you need to configure on the appliance in inline mode (also called two-arm mode).

Entity type	Name	IP address	Port	Protocol
Virtual Server	Vserver-LB-1	10.102.29.65	80	SIP-UDP
Services	Service-SIP-1	192.168.1.6	80	SIP-UDP
	Service-SIP-2	192.168.1.5	80	SIP-UDP
Monitors	Default	None	80	SIP-UDP

The following diagram shows the load balancing entities and the values of the parameters to be configured on the appliance.

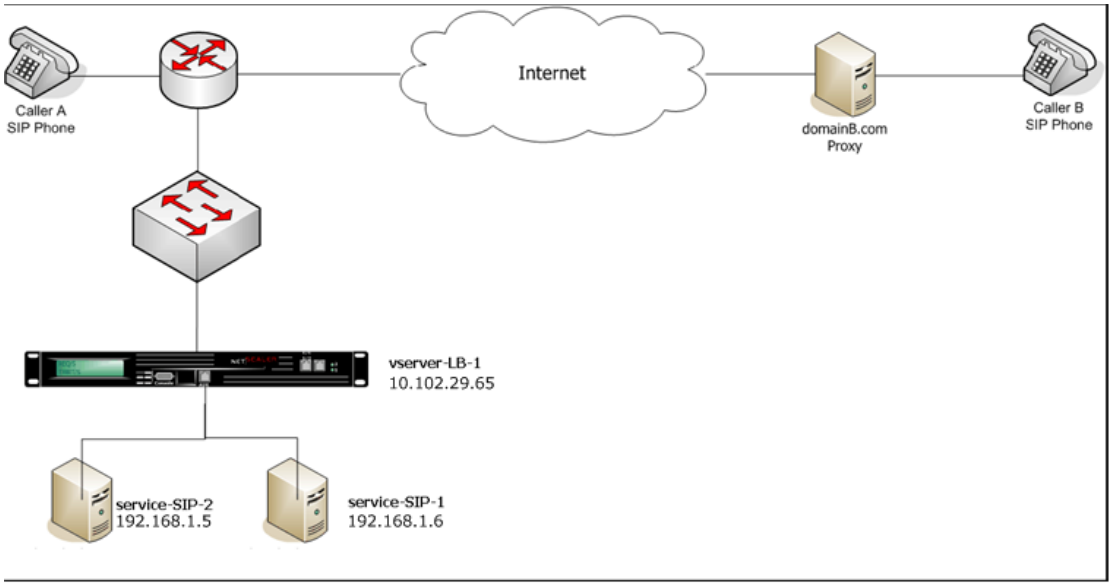


Figure 3. Load Balancing SIP Servers Entity Model

To configure a basic load balancing setup for SIP, see Setting Up Basic Load Balancing. You create services and virtual servers of type SIP-UDP, naming the entities and setting the parameters as described in the previous table. You must then configure RNAT.

Configuring Load Balancing for SIP Signaling Traffic over TCP or UDP

The NetScaler ADC can load balance SIP servers that send requests over UDP or TCP, including TCP traffic secured by TLS. The ADC provides the following service types to load balance the SIP servers:

- SIP_UDP – Used when SIP servers send SIP messages over UDP.
- SIP_TCP – Used when SIP servers send SIP messages over TCP.

- SIP_SSL – Used to secure SIP signaling traffic over TCP by using SSL or TLS. The NetScaler ADC supports the following modes:
  - End-to-end TLS connection between the client, the ADC, and the SIP server.
  - TLS connection between the client and the ADC, and TCP connection between the ADC and the SIP server.
  - TCP connection between the client and the ADC, and TLS connection between the ADC and the SIP server.

The following figure shows the topology of a setup configured to load balance a group of SIP servers sending SIP messages over TCP or UDP.

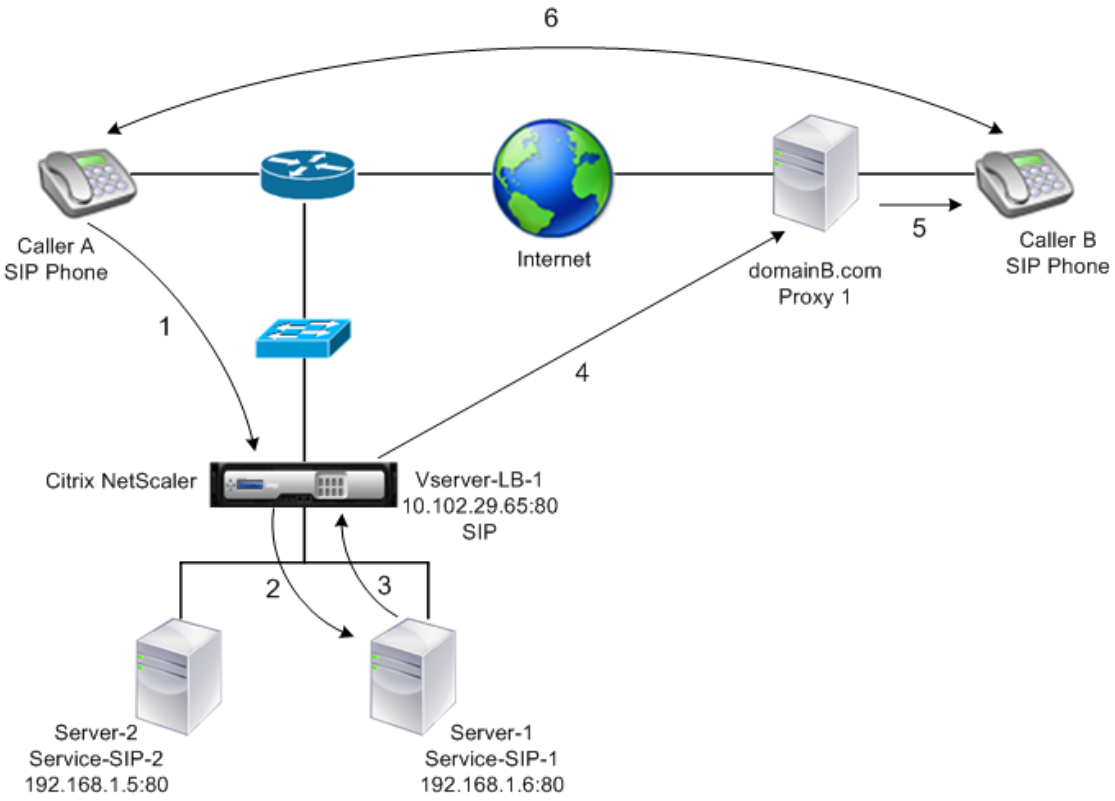


Figure 4. SIP Load Balancing Topology

Entity type	Name	IP address	Port	Service type / Protocol
Virtual Server	Vserver-LB-1	10.102.29.65	80	SIP_UDP / SIP_TCP / SIP_SSL
Services	Service-SIP-1	192.168.1.6	80	SIP_UDP / SIP_TCP / SIP_SSL
	Service-SIP-2	192.168.1.5	80	SIP_UDP / SIP_TCP / SIP_SSL

Monitors	Default	None	80	SIP_UDP / SIP_TCP / SIP_SSL

Following is an overview of configuring basic load balancing for SIP traffic:

1. Configure services, and configure a virtual server for each type of SIP traffic that you want to load balance:

   - **SIP_UDP** – If you are load balancing the SIP traffic over UDP.

   - **SIP_TCP** – If you are load balancing the SIP traffic over TCP.

   - **SIP_SSL** – If you are load balancing and securing the SIP traffic over TCP.

   Note: If you use SIP_SSL, be sure to create an SSL certificate-key pair. For more information, see Adding a Certificate Key Pair.

2. Bind the services to the virtual servers.

3. If you want to monitor the states of the services with a monitor other than the default (**tcp-default**), create a custom monitor and bind it to the services. The NetScaler ADC provides two custom monitor types, **SIP-UDP** and **SIP-TCP**, for monitoring SIP services.

4. If using a SIP_SSL virtual server, bind an SSL certificate-key pair to the virtual server.

5. If you are using the NetSCaler ADC as the gateway for the SIP servers in your deployment, configure RNAT.

6. If you want to append RPORT to the SIP messages that are initiated from the SIP server, configure the SIP parameters.

To configure a basic load balancing setup for SIP traffic by using the command line interface

1. Create one or more services. At the command prompt, type:

   add service <name> <serverName> (SIP_UDP | SIP_TCP | SIP_SSL) <port>

   Example

   ```
   add service Service-SIP-UDP-1 192.0.2.5 SIP_UDP 80
   ```

2. Create as many virtual servers as necessary to handle the services that you created. The virtual server type must match the type of services that you will bind to it. At the command prompt, type:

   add lb vserver <name> <serverName> (SIP_UDP | SIP_TCP | SIP_SSL) <port>

   Example

   ```
   add lb vserver Vserver-LB-1 SIP_UDP 10.102.29.60 80
   ```

3. Bind each service to a virtual server. At the command prompt, type:

   bind lb vserver <name> <serverName>

   Example

   ```
   bind lb vserver Vserver-LB-1 Service-SIP-UDP-1
   ```

4. (Optional) Create a custom monitor of type SIP-UDP or SIP-TCP, and bind the monitor to the service. At the command prompt, type:

   add lb monitor <monitorName> <monitorType> [<interval>]

   bind lb monitor <monitorName> <ServiceName>

   Example

   ```
   add lb monitor mon1 sip-UDP -sipMethod REGISTER -sipuRI
   sip:mon@test.com -sipregURI sip:mon@test.com -respcode 200

   bind monitor mon1 Service-SIP-UDP-1
   ```

5. If you created a SIP_SSL virtual server, bind an SSL certificate key pair to the virtual server. At the command prompt, type: At the command prompt, type:

   bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName> -CA -skipCAName

   Example

   ```
   bind ssl vserver Vserver-LB-1 -certkeyName CertKey-SSL-1
   ```

6. Configure RNAT as required by your network topology. At the command prompt, type one of the following commands to create, respectively, an RNAT entry that uses a network address as the condition and a MIP or SNIP as the NAT IP address, an RNAT entry that uses a network address as the condition and a unique IP address as the NAT IP address, an RNAT entry that uses an ACL as the condition and a MIP or SNIP as the NAT IP address, or an RNAT entry that uses an ACL as a condition and a unique IP address as the NAT IP address:

   set rnat <IPAddress> <netmask>

   set rnat <IPAddress> <netmask> -natip <NATIPAddress>

   set rnat <aclname> [-redirectPort <port>]

   set rnat <aclname> [-redirectPort <port>] -natIP <NATIPAddress>

   Example

   ```
   set rnat 192.168.1.0 255.255.255.0 -natip 10.102.29.50
   ```

   If you want to use a custom certificate-key pair, bind the custom certificate-key pair to the NetScaler internal service named **nsrnatsip-127.0.0.1-5061**.

   add ssl certKey <certkeyName> -cert <string> [-key <string>]

   bind ssl service <serviceName> -certkeyName <string>

   Example

   ```
   add ssl certKey c1 -cert cert.epm -key key.ky

   bind ssl service nsrnatsip-127.0.0.1-5061 -certkeyName c1
   ```

7. If you want to append RPORT to the SIP messages that the SIP server initiates, type the following command at the command prompt:

   set lb sipParameters -rnatSrcPort <rnatSrcPort> -rnatDstPort<rnatDstPort> -retryDur <integer> -addRportVip <addRportVip> - sip503RateThreshold <sip503_rate_threshold_value>

Sample Configuration for load balancing the SIP traffic over UDP

```
> add service service-UDP-1 10.102.29.5 SIP_UDP 80

Done

> add lb vserver vserver-LB-1 SIP_UDP 10.102.29.60 80

Done

> bind lb vserver vserver-LB-1 service-UDP-1
```

```
Done

> add lb mon mon1 sip-udp -sipMethod REGISTER -sipuRI
sip:mon@test.com -sipregURI sip:mon@test.com -respcode 200

Done

> bind mon mon1 service-UDP-1

Done

> set rnat 192.168.1.0 255.255.255.0

Done

> set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur
1000 -addRportVip ENABLED -sip503RateThreshold 1000

Done
```

Sample Configuration for load balancing the SIP traffic over TCP

```
> add service service-TCP-1 10.102.29.5 SIP_TCP 80

Done

> add lb vserver vserver-LB-1 SIP_TCP 10.102.29.60 80

Done

> bind lb vserver vserver-LB-1 service-TCP-1

Done

> add lb mon mon1 sip-tcp -sipMethod REGISTER -sipuRI
sip:mon@test.com -sipregURI sip:mon@test.com -respcode 200

Done

> bind mon mon1 service-TCP-1

Done

> set rnat 192.168.1.0 255.255.255.0

Done

> set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur
1000 -addRportVip ENABLED -sip503RateThreshold 1000

Done
```

Sample Configuration for load balancing and securing SIP traffic over TCP

```
> add service service-SIP-SSL-1 10.102.29.5 SIP_SSL 80

Done

> add lb vserver vserver-LB-1 SIP_SSL 10.102.29.60 80

Done

> bind lb vserver vserver-LB-1 service-SIP-SSL

Done

> add lb mon mon1 sip-tCP -sipMethod REGISTER -sipuRI
sip:mon@test.com -sipregURI sip:mon@test.com -respcode 200

Done

> bind mon mon1 service-SIP-SSL

Done

> bind ssl vserver Vserver-LB-1 -certkeyName CertKey-SSL-1

Done

> set rnat 192.168.1.0 255.255.255.0

Done

> set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur
1000 -addRportVip ENABLED -sip503RateThreshold 1000

Done
```

To configure a basic load balancing setup for SIP traffic by using the configuration utility

1. Navigate to Traffic Management > Load Balancing > Virtual Servers, and add a virtual server of type SIP_UDP, SIP_TCP, or SIP_SSL.
2. Click the Service section, and add a service of type SIP_UDP, SIP_TCP, or SIP_SSL.
3. (Optional) Click the Monitor section, and add a monitor of type: SIP-UDP or SIP-TCP.
4. Bind the monitor to the service, and bind the service to the virtual server.
5. If you created a SIP_SSL virtual server, bind an SSL certificate key pair to the virtual server. Click the Certificates section, and bind a certificate key pair to the virtual server.
6. Configure RNAT as required by your network topology. To configure RNAT:
   a. Navigate to System > Network > Routes.
   b. On the Routes page, click the RNAT tab.
   c. In the details pane, click Configure RNAT.
   d. In the Configure RNAT dialog box, do one of the following:
      - If you want to use the network address as a condition for creating an RNAT entry, click Network and set the following parameters:
        - Network
        - Netmask
      - If you want to use an extended ACL as a condition for creating an RNAT entry, click ACL and set the following parameters:
        - ACL Name
        - Redirect Port
   e. To set a MIP or SNIP address as a NAT IP address, skip to step 7.
   f. To set a unique IP address as a NAT IP, in the Available NAT IP (s) list, select the IP address that you want to set as the NAT IP, and then click Add. The NAT IP you selected appears in the Configured NAT IP(s) list.
   g. Click Create, and then click Close.

If you want to use a custom certificate-key pair, bind the custom certificate-key pair to the NetScaler internal service named **nsrnatsip-127.0.0.1-5061**. To bind the pair:

a. Navigate to Traffic Management > Load Balancing > Services and click the Internal Services tab.
b. Select nsrnatsip-127.0.0.1-5061 and click **Edit**.
c. Click the **Certificates** section and bind a certificate key pair to the internal service.

7. If you want to append RPORT to the SIP messages that the SIP server initiates, configure the SIP parameters. Navigate to Traffic Management > Load Balancing and click Change SIP settings, set the various SIP parameters.

SIP Expression and Policy Example: Compression Enabled in Client Requests

A NetScaler ADC cannot process compressed client SIP requests, so the client SIP request fails.

You can configure a responder policy that intercepts the SIP NEGOTIATE message from the client and looks for the compression header. If the message includes a compression header, the policy responds with "400 Bad Request," so that the client resends the request without compressing it.

At the command prompt, type the following commands to create the responder policy:

```
> add responder action sipaction1 respondwith q{"SIP/2.0 400 Bad
Request\r\n\r\n"}

Done.

> add responder policy sippol1

> add responder policy sippol1 "SIP.REQ.METHOD.EQ(\"NEGOTIATE\")&&SIP
.REQ.HEADER(\"Compression\").EXISTS" sipaction1
```

To configure RNAT by using the command line interface

At the command prompt, type:

set rnat<network> <netmask>

Example

set rnat 192.168.1.0 255.255.255.0

Parameters for configuring RNAT

network

IPv6 address of the network on whose traffic you want the NetScaler appliance to do RNAT processing.

netmask

Subnet mask associated with the network address.

To configure RNAT by using the configuration utility

1. In the navigation pane expand Network, expand Routing, and then click Routes.
2. On the Routes page, click the RNAT tab.
3. In the details pane, click Configure RNAT.
4. In the Configure RNAT dialog box, do one of the following:
   - If you want to use the network address as a condition for creating an RNAT entry, click Network and set the following parameters:
     - Network
     - Netmask
   - If you want to use an extended ACL as a condition for creating an RNAT entry, click ACL and set the following parameters:
     - ACL Name
     - Redirect Port
5. To set a MIP or SNIP address as a NAT IP address, skip to step 7.
6. To set a unique IP address as a NAT IP, in the Available NAT IP (s) list, select the IP address that you want to set as the NAT IP, and then click Add. The NAT IP you selected appears in the Configured NAT IP(s) list.
7. Click Create, and then click Close.

After you configure RNAT, the appliance sends SIP responses to the IP address and port that the client uses to send the request. The appliance also adds the RPORT tag in the VIA header of the message. The appliance compares the values of the source and destination ports of the request packets with the RNAT source port and RNAT destination port. If one of the values matches, the appliance updates the VIA header with the RPORT setting.

You must enable this setting when RPORT is not configured on either client.

To configure SIP parameters by using the command line interface

At the command prompt, type:

set lb sipParameters -rnatSrcPort <rnatSrcPort> -rnatDstPort<rnatDstPort> -retryDur <integer> -addRportVip <addRportVip> - sip503RateThreshold <sip503_rate_threshold_value>

Example

```
set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000 -addRportVip ENABLED -sip503RateT
```

Parameters for configuring the SIP parameters

rnatSrcPort

Port number with which to match the source port in server-initiated SIP traffic. The rport parameter is added, without a value, to SIP packets that have a matching source port number, and CALL-ID based persistence is implemented for the responses received by the virtual server.

rnatDstPort

Port number with which to match the destination port in server- initiated SIP traffic. The rport parameter is added, without a value, to SIP packets that have a matching source port number, and CALL-ID based persistence is implemented for the responses received by the virtual server.

retryDur

Time, in seconds, for which a client must wait before initiating a connection after receiving a 503 Service Unavailable response from the SIP server. The time value is sent in the "Retry-After" header in the 503 response. Minimum value: 1. Maximum Value: 32767. Default: 120.

addRportVip

Add the rport parameter to the VIA headers of SIP requests that virtual servers receive from clients or servers. Possible values: ENABLED, DISABLED. Default: ENABLED.

sip503RateThreshold

Maximum number of 503 Service Unavailable responses to generate, once every 10 milliseconds, when a SIP virtual server becomes unavailable. Maximum Value: 65535. Default: 100.

To configure SIP parameters by using the configuration utility

1. Navigate to Traffic Management > DNS > Name Servers.
2. Create a DNS name server of type DNS Virtual Server, and select a server from the DNS Virtual Server list.

1. In the navigation pane, click Load Balancing.
2. On the Load Balancing landing page, under Settings, click Change SIP settings.
3. In the Set SIP Parameters dialog box, set values for the following parameters:

- RNAT Source Port
- RNAT Destination Port
- Retry Duration (secs)
- SIP503 Rate Threshold

4. Select Enable Add Rport VIP.
5. Click OK.

Load Balancing RTSP Servers

The NetScaler appliance can balance load on RTSP servers to improve the performance of audio and video streams over networks. The following diagram describes the topology of an load balancing setup configured to load balance a group of RTSP servers.

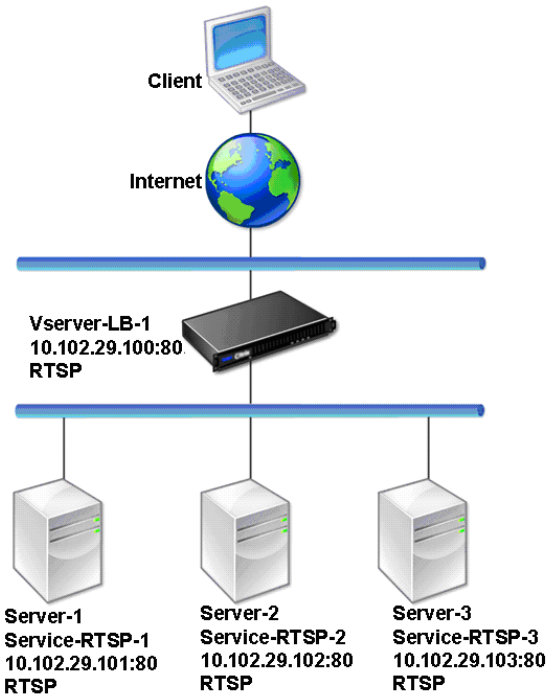


Figure 1. Load Balancing Topology for RTSP

In the example, the services Service-RTSP-1, Service-RTSP-2, and Service-RTSP-3 are bound to the virtual server Vserver-LB-1. The following table lists the names and values of the example entities.

Entity type	Name	IP address	Port	Protocol
Virtual Server	Vserver-LB-1	10.102.29.100	554	RTSP
Services	Service-RTSP-1	10.102.29.101	554	RTSP
	Service-RTSP-2	10.102.29.102	554	RTSP
	Service-RTSP-3	10.102.29.103	554	RTSP
Monitors	Monitor-RTSP-1	None	554	RTSP

The following diagram shows the load balancing entities used in RTSP configuration.

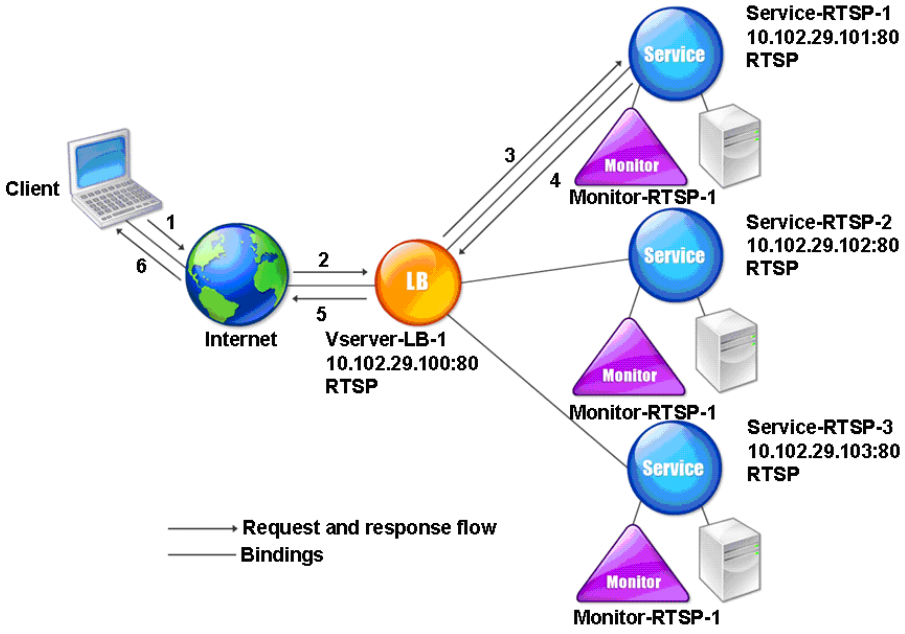


Figure 2. Load Balancing RTSP Servers Entity Model

To configure a basic load balancing setup for RTSP servers, see Setting Up Basic Load Balancing. Create services and virtual servers of type RTSP. When you configure a basic load balancing setup, the default TCP-default monitor is bound to the services. To bind an RTSP monitor to these services, see Binding Monitors to Services. The following procedure describes how create a monitor that checks RTSP servers.

To configure RTSP monitors by using the command line interface

At the command prompt, type:

add lb monitor <monitorName> <type>

Example

add lb monitor Monitor-RTSP-1 RTSP

To configure RTSP monitors by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. In the details pane, click Add.
3. In the Create Monitor dialog box, in the Name and Interval text boxes, type the name and probing interval of a monitor.
4. In the Type list, select the type of the monitor.
5. Click Create, and then click Close.

Load Balancing of Remote Desktop Protocol (RDP) Servers

Remote Desktop Protocol (RDP) is a multichannel-capable protocol that allows for separate virtual channels for carrying presentation data, serial device communication, licensing information, highly encrypted data (keyboard and mouse activity), and so on.

RDP is used for providing a graphical user interface to another computer on the network. RDP is used with Windows terminal servers for providing fast access with almost real-time transmission of mouse movements and key presses even over low-bandwidth connections.

When multiple terminal servers are deployed to provide remote desktop services, the NetScaler appliance provides load balancing of the terminal servers (Windows 2003 and 2008 Server Enterprise Editions). In some cases, a user who is accessing an application remotely may want to leave the application running on the remote machine but shut down the local machine. The user therefore closes the local application without logging out of the remote application. After reconnecting to the remote machine, the user should be able to continue with the remote application. To provide this functionality, the NetScaler RDP implementation honors the routing token (cookie) set by the Terminal Services Session Directory or Broker so that the client can reconnect to the same terminal server to which it was connected previously. The Session Directory, implemented on Windows 2003 Terminal Server, is referred to as Broker on Windows 2008 Terminal Server.

When a TCP connection is established between the client and the load balancing virtual server, the NetScaler applies the specified load balancing method and forwards the request to one of the terminal servers. The terminal server checks the session directory to determine whether the client has a session running on any other terminal server in the domain.

If there is no active session on any other terminal server, the terminal server responds by serving the client request, and the NetScaler forwards the response to the client.

If there is an active session on any other terminal server, the terminal server that receives the request inserts a cookie (referred to as routing token) with the details of the active session and returns the packets to the NetScaler, which returns the packet to the client. The server closes the connection with the client. When the client retries to connect, the NetScaler reads the cookie information and forwards the packet to the terminal server on which the client has an active session.

The user on the client machine experiences a continuation of the service and does not have to take any specific action.

Note: The Windows Session Directory feature requires the Remote Desktop client that was first released with Windows XP. If a session with a Windows 2000 or Windows NT 4.0 Terminal Server client is disconnected and the client reconnects, the server with which the connection is established is selected by the load balancing algorithm.

The following diagram describes RDP load balancing.

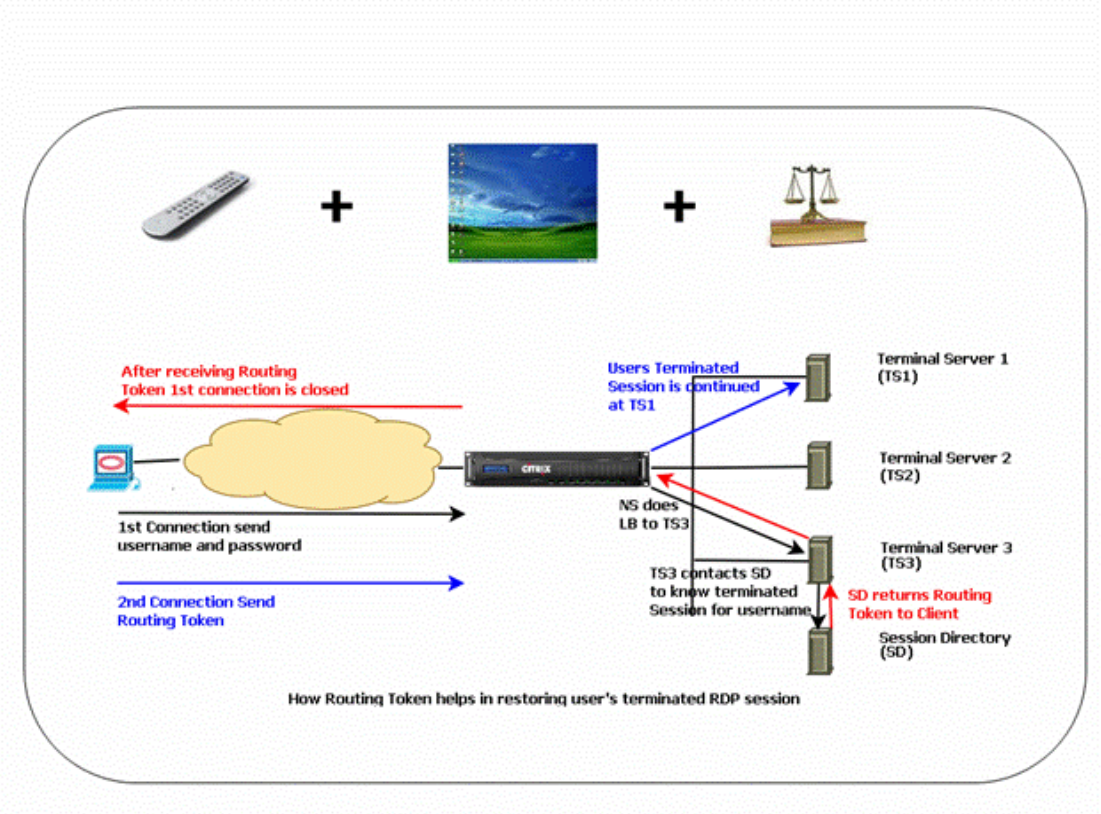


Figure 1. Load Balancing Topology for RDP

Note: When an RDP service is configured, persistence is automatically maintained by using a routing token. You need not enable persistence explicitly.

Ensure that the disconnected RDP sessions are cleared on the terminal servers at the backend to avoid flapping between two terminal servers when an RDP session is disconnected without logging out. For more information, see http://technet.microsoft.com/en-us/library/cc758177(WS.10).aspx#BKMK_2

When you add an RDP service, by default, NetScaler adds a monitor of the type TCP and binds it to the service. The default monitor is a simple TCP monitor that checks whether or not a listening process exists at the 3389 port on the server specified for the RDP service. If there is a listening process at 3389, NetScaler marks this service as UP and if there is no listening process, it marks the service as DOWN.

For more efficient monitoring of an RDP service, in addition to the default monitor, you can configure a script monitor that is meant for the RDP protocol. When you configure the scripting monitor, the NetScaler opens a TCP connection to the specified server and sends an RDP packet. The monitor marks the service as UP only if it receives a confirmation of the connection from the physical server. Therefore, from the scripting monitor, the NetScaler can know whether the RDP service is ready to service a request.

The monitor is a user-type monitor and the script is located on the NetScaler at /nsconfig/monitors/nsrdp.pl. When you configure the user monitor, the NetScaler runs the script automatically. To configure the scripting monitor, add the monitor and bind it to the RDP service.

To configure RDP load balancing, create services of type RDP and bind them to an RDP virtual server.

To configure RDP load balancing services by using the command line interface

At the command prompt, type the following commands to configure an RDP load balancing setup and verify the configuration:

add service <name>@ <serverName> <serviceType> <port>

Note: Repeat the above command to add more services.

Example

```
> add service ser1 10.102.27.182 RDP 3389
Done
> add service ser2 10.102.27.183 RDP 3389
Done
>show service ser1
ser1 (10.102. 27.182:3389) - RDP
       State: UP
…
          Server Name: 10.102.27.182
          Server ID : 0          Monitor Threshold : 0
       Down state flush: ENABLED
…
1)     Monitor Name: tcp-default
             State: UP       Weight: 1
…
             Response Time: 4.152 millisec
 Done
```

Parameters for configuring a service

serviceName

Name of the service. The name must not exceed 127 characters, and the leading character must be a number or a letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serverName

Name or IP address of the server in IPv4 format.

serviceType

The service type must be RDP.

port

The default port, 3389, must be used.

To configure RDP load balancing services by using the configuration utility

1. In the navigation pane, expand Load Balancing and then click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring a service" as shown:
   - Service Name*—serviceName
   - Protocol*—serviceType
   - Server*—serverName
   - Port*—port

   *A required parameter
4. Click Create.
5. Create all the RDP services to be load balanced.
6. From the services pane, open the service you added, and verify the addition.

To configure an RDP load balancing virtual server by using the command line interface

At the command prompt, type the following commands to configure an RDP load balancing virtual server and verify the configuration:

- add lb vserver <name>@ <serviceType> <ipAddress> <port>
- bind lb vserver <name>@ <serviceName>

  Bind all the RDP services to be load balanced to the virtual server.

Example

This example has two RDP services bound to the RDP virtual server.

```
> add lb vs v1 rdP 10.102.27.186 3389
Done
```

```
> bind lb vs v1 ser1
service "ser1" bound
> bind lb vs v1 ser2
service "ser2" bound
Done

>sh lb vs v1
v1 (10.102.27.186:3389) - RDP   Type: ADDRESS
State: UP
…
No. of Bound Services :  2 (Total)       2 (Active)
Configured Method: LEASTCONNECTION
  Current Method: Round Robin, Reason: A new service is bound
Mode: IP
Persistence: NONE
  L2Conn: OFF

1) ser1 (10.102.27.182: 3389) - RDPState: UP   Weight: 1
2) ser2 (10.102.27.183: 3389) - RDPState: UP   Weight: 1
Done
```

Parameters for configuring a virtual server

vServerName

Name of the virtual server that is associated with the service. The name must not exceed 127 characters, and the leading character must be a number or a letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

ipAddress

IP address of the virtual server in the IPv4 format.

serviceType

The service type must be RDP.

port

The default port, 3389, must be used.

To configure an RDP load balancing virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server (Load Balancing) dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a virtual server” as shown:
   - Name*—vServerName
   - IP Address*—ipAddress
   - Protocol*—serviceType
   - Port*—port

   *A required parameter
4. In the Services tab, select the services to be bound to the virtual server by checking the service names.
5. Click Create.
6. In the Load Balancing Virtual Servers pane, select the RDP virtual server you configured, and then click Open to verify the configuration.

To configure a scripting monitor for RDP services by using the command line interface

At the command prompt, type the following commands:

- add lb monitor <monitorName> USER -scriptName nsrdp.pl
- bind lb monitor <monitorName> <rdpServiceName>

Example

```
add service ser1 10.102.27.182 RDP 3389
add lb monitor RDP_MON USER -scriptName nsrdp.pl
bind lb monitor RDP_MON ser1
```

Parameter for configuring RDP scripting monitor

scriptName

Name of the script to be run.

To configure a scripting monitor for RDP services by using the configuration utility

1. In the navigation pane, expand Load Balancing and then click Monitors.
2. In the details pane, click Add.
3. In the Create Monitor dialog box, specify a name for the RDP monitor.
4. In the Type drop-down list, select USER.
5. On the Special Parameters tab, for the Script Name, click Browse and select nsrdp.pl from the default location.
6. Click Create.
7. From the Monitors pane, open the monitor you added, and verify the addition.
8. In the navigation pane, expand Load Balancing, and then click Services.
9. In the details pane, select the RDP service, and then click Open.
10. In the Configure Service dialog box, select the RDP scripting monitor that you added and click Add.
11. Click OK.

Use Cases

Certain deployment scenarios are useful to perform load balancing in a wide variety of circumstances. Several protocols benefit from a configuration that allows the server to respond directly to the client rather than through the NetScaler appliance. This is called *direct server return (DSR) mode*. Many deployments are faster when you connect the appliance to the network through a single interface, rather than placing it directly in the flow of traffic. This is called *one-arm mode*. Other deployments require that the appliance be installed in the flow of traffic, so that it transparently intercepts traffic that is sent to and from the servers that it manages. This is called *inline mode* or (occasionally) *two-arm mode*. These use cases are described in detail below.

Configuring Rule Based Persistence Based on a Name-Value Pair in a TCP Byte Stream

Some protocols transmit name-value pairs in a TCP byte stream. The protocol in the TCP byte stream in this example is the Financial Information eXchange (FIX) protocol. In its traditional, non-XML implementation, the FIX protocol enables two hosts communicating over a network to exchange business or trade-related information as a list of name-value pairs (called "FIX fields"). The field format is `<tag>=<value><delimiter>`. This traditional tag-value format makes the FIX protocol ideal for the use case.

The tag in a FIX field is a numeric identifier that indicates the meaning of the field. For example, the tag `35` indicates the message type. The value after the equal sign holds a specific meaning for the given tag and is associated with a data type. For example, a value of `A` for the tag `35` indicates that the message is a logon message. The delimiter is the nonprinting "Start of Header" (SOH) ASCII character (`0x01`), which is the caret symbol (`^`). Each field is also assigned a name. For example, the field with tag `35` is the `msgType` field. Following is an example of a logon message.

```
8=FIX.4.1 9=61 35=A 49=INVMGR 56=BRKR 34=1 52=20000426-12:05:06 98=0
108=30 10=157
```

Your choice of persistence type for a tag-value list such as the one shown above is determined by the options that are available to you for extracting a particular string from the list. Token-based persistence methods require you to specify the offset and length of the token that you want to extract from the payload. The FIX protocol does not allow you to do that, because the offset of a given field and the length of its value can vary from one message to another (depending on the message type, the preceding fields, and the lengths of the preceding values) and from one implementation to another (depending on whether custom fields have been defined). Such variations make it impossible to predict the exact offset of a given field or to specify the length of the value that is to be extracted as the token. In this case, therefore, rule based persistence is the preferred persistence type.

Assume that a virtual server `fixlb1` is load balancing TCP connections to a farm of servers hosting instances of a FIX-enabled application, and that you want to configure persistence for connections on the basis of the value of the `SenderCompID` field, which identifies the firm sending the message. The tag for this FIX field is `49` (shown in the earlier logon message example).

To configure rule based persistence for the load balancing virtual server, set the persistence type for the load balancing virtual server to `RULE` and configure the rule parameter with an expression. The expression must be one that extracts the portion of the TCP payload in which you expect to find the `SenderCompID` field, typecasts the resulting string to a name-value list based on the delimiters, and then extracts the value of the `SenderCompID` field (tag `49`), as follows:

```
set lb vserver fixlb1 -persistenceType RULE -rule
"CLIENT.TCP.PAYLOAD(300).TYPECAST_NVLIST_T('=','^').VALUE(\"49\")"
```

Note: Backslash characters have been used in the expression because this is a CLI command. If you are using the configuration utility, do not enter the backslash characters.

If the client sends a FIX message that contains the name-value list in the earlier logon message example, the expression extracts the value `INVMGR`, and the NetScaler appliance creates a persistence session based on this value.

The argument to the `PAYLOAD()` function can be as large as you deem is necessary to include the `SenderCompID` field in the string extracted by the function. Optionally, you can use the `SET_TEXT_MODE(IGNORECASE)` function if you want the appliance to ignore case when extracting the value of the field, and the `HASH` function to create a persistence session based on a hash of the extracted value. The following expression uses the `SET_TEXT_MODE(IGNORECASE)` and `HASH` functions:

```
CLIENT.TCP.PAYLOAD(500).TYPECAST_NVLIST_T('=','^').SET_TEXT_MODE(IGNO
RECASE).VALUE("49").HASH
```

Following are more examples of rules that you can use to configure persistence for FIX connections (replace `<tag>` with the tag of the field whose value you want to extract):

- To extract the value of any FIX field in the first 300 bytes of the TCP payload, you can use the expression `CLIENT.TCP.PAYLOAD(300).BEFORE_STR("^").AFTER_STR("<tag>=").`
- To extract a string that is 20 bytes long at offset 80, cast the string to a name-value list, and then extract the value of the field that you want, use the expression `CLIENT.TCP.PAYLOAD(100).SUBSTR(80,20).TYPECAST_NVLIST_T('=','^').VALUE("<tag>").`
- To extract the first 100 bytes of the TCP payload, cast the string to a name-value list, and extract the value of the third occurrence of the field that you want, use the expression `CLIENT.TCP.PAYLOAD(100).TYPECAST_NVLIST_T('=','^').VALUE("<tag>",2).`

  Note: If the second argument that is passed to the `VALUE()` function is `n`, the appliance extracts the value of the $(n+1)^{th}$ instance of the field because the count starts from zero (`0`).

Following are more examples of rules that you can use to configure persistence. Only the payload-based expressions can evaluate data being transmitted through the FIX protocol. The other expressions are more general expressions for configuring persistence based on lower networking protocols.

- `CLIENT.TCP.PAYLOAD(100)`
- `CLIENT.TCP.PAYLOAD(100).HASH`
- `CLIENT.TCP.PAYLOAD(100).SUBSTR(5,10)`
- `CLIENT.TCP.SRCPORT`
- `CLIENT.TCP.DSTPORT`
- `CLIENT.IP.SRC`

- CLIENT.IP.DST
- CLIENT.IP.SRC.GET4
- CLIENT.IP.DST.GET4
- CLIENT.ETHER.SRCMAC.GET6
- CLIENT.ETHER.DSTMAC.GET5
- CLIENT.VLAN.ID

Configuring Load Balancing in Direct Server Return Mode

Load balancing in direct server return (DSR) mode allows the server to respond to clients directly by using a return path that does not flow through the NetScaler appliance. In DSR mode, however, the appliance can continue to perform health checks on services. In a high-data volume environment, sending server traffic directly to the client in DSR mode increases the overall packet handling capacity of the appliance because the packets do not flow through the appliance.

DSR mode has the following features and limitations:

- It supports one-arm mode and inline mode.
- The appliance ages out sessions based on idle timeout.
- Because the appliance does not proxy TCP connections (that is it does not send SYN-ACK to the client), it does not completely shut out SYN attacks. By using the SYN packet rate filter, you can control the rate of SYNs to the server. To control the rate of SYNs, set a threshold for the rate of SYNs. To get protection from SYN attacks, you must configure the appliance to proxy TCP connections. However, that requires the reverse traffic to flow through the appliance.
- In a DSR configuration, the NetScaler appliance does not replace the load balancing virtual server's IP address with the destination server's IP address. Instead, it forwards packets to a service by using the server's MAC address, which it obtains from the monitor bound to the service. However, custom user monitors (monitors of type USER), which use scripts stored on the NetScaler appliance, do not learn a server's MAC address. If you use only custom monitors in a DSR configuration, for each request the virtual server receives, the appliance attempts to resolve the destination IP address to a MAC address (by sending ARP requests). Because the destination IP address is a virtual IP address owned by the NetScaler appliance, the ARP requests always resolve to the MAC address of the NetScaler interface. Consequently, all traffic received by the virtual server is looped back to the appliance. If you use user monitors in a DSR configuration, you must also configure another monitor of a different type (for example, a PING monitor) for the services, ideally with a longer interval between probes, so that the MAC address of the servers can be learned.

In the example scenario, the services Service-ANY-1, Service-ANY-2, and Service-ANY-3 are created and bound to the virtual server Vserver-LB-1. The virtual server load balances the client request to a service, and the service responds to clients directly, bypassing the NetScaler. The following table lists the names and values of the entities configured on the NetScaler in DSR mode.

Entity type	Name	IP address	Protocol
Virtual server	Vserver-LB-1	10.102.29.94	ANY
Services	Service-ANY-1	10.102.29.91	ANY
	Service-ANY-2	10.102.29.92	ANY

	Service-ANY-3	10.102.29.93	ANY
Monitors	TCP	None	None

The following diagram shows the load balancing entities and values of the parameters to be configured on the appliance.

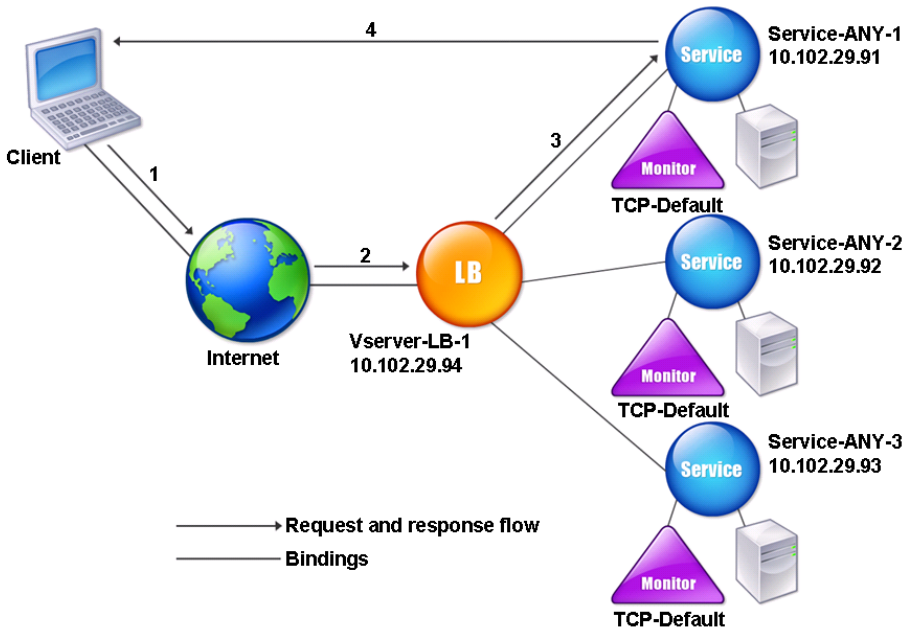


Figure 1. Entity Model for Load Balancing in DSR Model

For the appliance to function correctly in DSR mode, the destination IP in the client request must be unchanged. Instead, the appliance changes the destination MAC to that of the selected server. This setting enables the server to determine the client MAC address for forwarding requests to the client while bypassing the server. To enable the appliance to do this, you must enable MAC-based forwarding.

To enable MAC-based forwarding by using the command line interface

At the command prompt, type:

enable ns mode `MACbasedforwarding`

To enable MAC-based forwarding by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. On the Settings pane, under Modes and Features, click Configure modes.
3. In the Configure Modes dialog box, select the MAC Based Forwarding check box, and then click OK.
4. In the Enable/Disable Mode(s)? dialog box, click Yes.

Next, you configure a basic load balancing setup as described in Setting Up Basic Load Balancing, naming the entities and setting the parameters using the values described in the previous table.

After you configure the basic load balancing setup, you must customize it for DSR mode. To do this, you configure a supported load balancing method, such as the Source IP Hash method with a sessionless virtual server. You also need to set the redirection mode to allow the server to determine the client MAC address for forwarding responses and bypass the appliance.

After you configure the load balancing method and redirection mode, you need to enable the USIP mode on each service. The service then uses the source IP address when forwarding responses.

To configure the load balancing method and redirection mode for a sessionless virtual server by using the command line interface

At the command prompt, type:

set lb vserver <vServerName> -lbMethod <LBMethodOption> -m <RedirectionMode> -sessionless <Value>

Example

set lb vserver Vserver-LB-1 -lbMethod SourceIPHash -m MAC -sessionless enabled

To configure the load balancing method and redirection mode for a sessionless virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server (for example, Vserver-LB-1), and then click Open.
3. On the Method and Persistence tab, under LB Method, select SOURCE IP Hash.
4. On the Advanced tab, under Redirection Mode, select MAC Based.
5. Select the Sessionless check box and click OK.

To configure a service to use source IP address by using the command line interface

At the command prompt, type:

set service <ServiceName> -usip <Value>

Example

set service Service-ANY-1 -usip yes

To configure a service to use source IP address by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.

2. On the Services pane, click Service-ANY-1, and then click Open.

3. On the Advanced tab, under Settings, select the Use Source IP check box, and then click OK.

4. Repeat steps 1-5 for the services Service-ANY-2 and Service-ANY-3.

Some additional steps are required in certain situations, which are described in the succeeding sections.

Configuring LINUX Servers in DSR Mode

The LINUX operating system requires that you set up a loopback interface with the NetScaler appliance virtual IP address (VIP) on each load balanced server in the DSR cluster.

To configure LINUX server in DSR mode

To create a loop back interface with the NetScaler appliance's VIP on each load balanced server, at the Linux OS prompt type the following commands:

```
ifconfig dummy0 up

ifconfig dummy0:0 inet <netscaler vip> netmask 255.255.255.255 up

echo 1 > /proc/sys/net/ipv4/conf/dummy0/arp_ignore

echo 2 > /proc/sys/net/ipv4/conf/dummy0/arp_announce
```

Then, run the software that re-maps the TOS id to VIP.

Note: Add the correct mappings to the software before running it. In the preceding commands, the LINUX server uses dummy0 to connect to the network. When you use this command, type the name of the interface that your LINUX server uses to connect to the network.

Configuring DSR Mode When Using TOS

Differentiated services (DS), also known as TOS (Type of Service), is a field that is part of the TCP packet header. TOS is used by upper layer protocols for optimizing the path for a packet. The TOS information encodes the NetScaler appliance virtual IP address (VIP), and the load balanced servers extract the VIP from it.

In the following scenario, the appliance adds the VIP to the TOS field in the packet and then forwards the packet to the load balanced server. The load balanced server then responds directly to the client, bypassing the appliance, as illustrated in the following diagram.

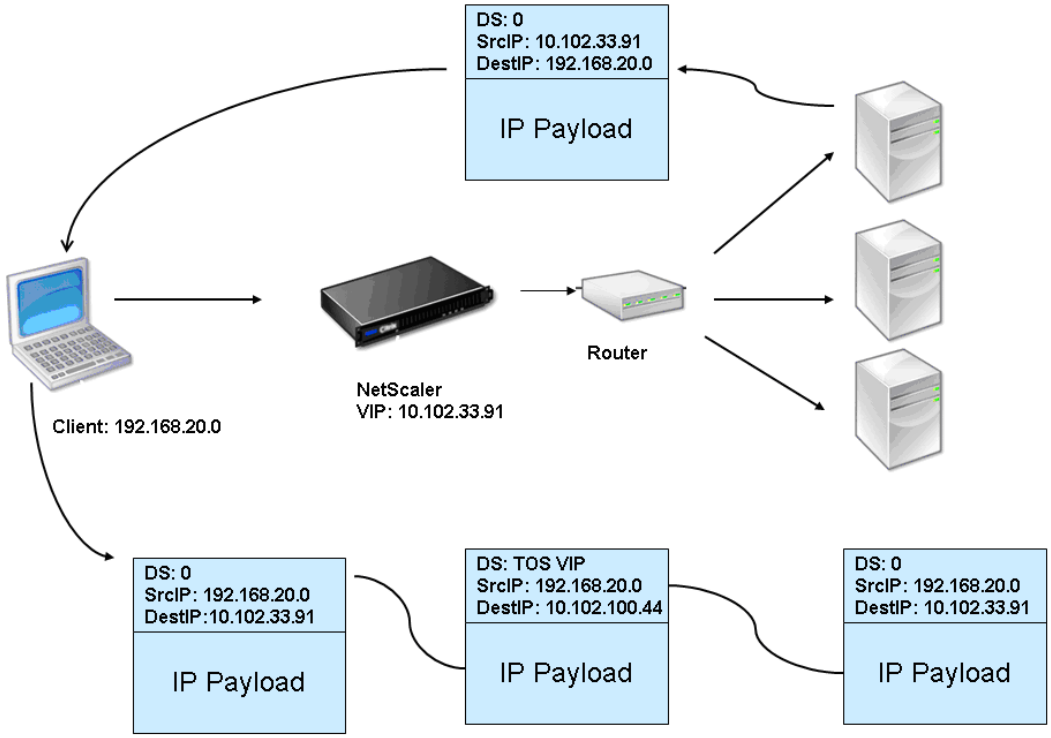


Figure 1. The NetScaler Appliance in DSR mode with TOS

The TOS feature is specifically customized for a controlled environment, as described below:

- The environment must not have any stateful devices, such as stateful firewall and TCP gateways, in the path between the appliance and the load balanced servers.
- Routers at all the entry points to the network must remove the TOS field from all incoming packets to make sure that the load balanced server does not confuse another TOS field with that added by the appliance.
- Each server can have only 63 VIPs.

- The intermediate router must not send out ICMP error messages regarding fragmentation. The client will not understand the message, as the source IP address will be the IP address of the load balanced server and not the NetScaler VIP.
- TOS is valid only for IP-based services. You cannot use domain name based services with TOS.

In the example, Service-ANY-1 is created and bound to the virtual server Vserver-LB-1. The virtual server load balances the client request to the service, and the service responds to clients directly, bypassing the appliance. The following table lists the names and values of the entities configured on the appliance in DSR mode.

Entity Type	Name	IP Address	Protocol
Virtual server	Vserver-LB-1	10.102.33.91	ANY
Services	Service-ANY-1	10.102.100.44	ANY
Monitors	PING	None	None

DSR with TOS requires that load balancing be set up on layer 3. To configure a basic load balancing setup for Layer 3, see Setting Up Basic Load Balancing. Name the entities and set the parameters using the values described in the previous table.

After you configure the load balancing setup, you must customize the load balancing setup for DSR mode by configuring the redirection mode to allow the server to decapsulate the data packet and then respond directly to the client and bypass the appliance.

After specifying the redirection mode, you can optionally enable the appliance to transparently monitor the server. This enables the appliance to transparently monitor the load balanced servers.

To configure the redirection mode for the virtual server by using the command line interface

At the command prompt, type:

set lb vserver <vServerName> -m <Value> -tosId <Value>

Example

set lb vserver Vserver-LB-1 -m TOS -tosId 3

To configure the redirection mode for the virtual server by using the configuration utility

1. In the left navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the Load Balancing Virtual Servers pane, select the virtual server and click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, on the Advanced tab, in Redirection Mode, click TOS Based.
4. In the TOS Id box, enter a value for the TOS ID.
5. Click OK.

To configure the transparent monitor for TOS by using the command line interface

At the command prompt, type:

add monitor <MonitorName> <Type> -destip <DestinationIP> -tos <Value> -tosId <Value>

Example

add monitor mon1 PING -destip 10.102.33.91 -tos Yes -tosId 3

To create the transparent monitor for TOS by using the configuration utility

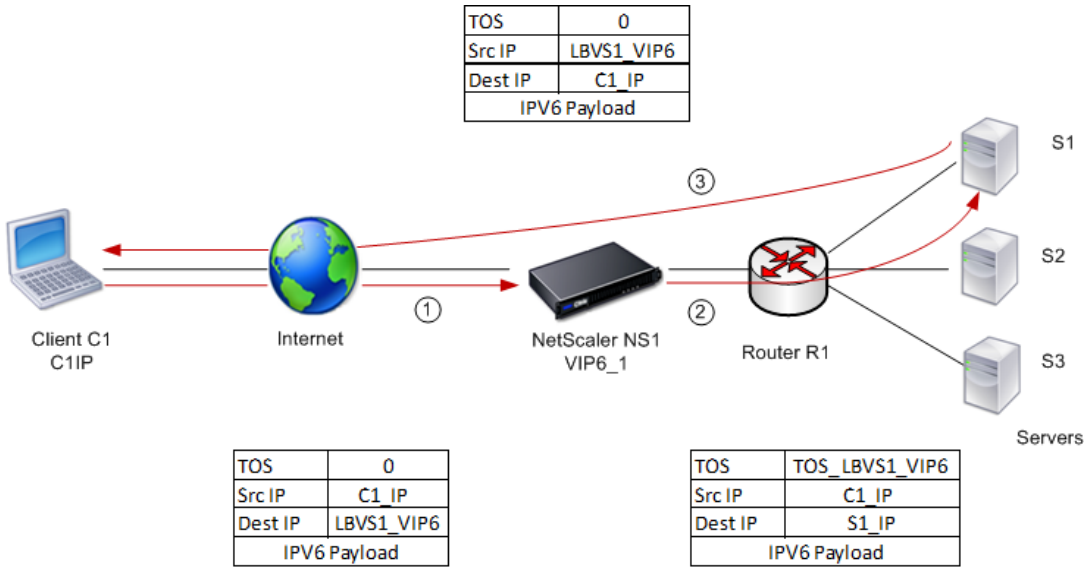
1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. On the Monitors pane, select the monitor (for example, tcp), and click Add.
3. In the Create Monitor dialog box, in the Name and Destination IP boxes, enter the monitor name and the destination IP address (for example, PING and 10.102.33.91).
4. In the Type list, select the type of monitor (for example, PING).
5. To configure the monitor for TOS, select the TOS check box.
6. In the TOS Id box, enter the same TOS ID that you had entered for the virtual server (for example, 3.)
7. Click OK.

Configuring Load Balancing in DSR Mode for IPv6 Networks by Using the TOS Field

You can configure load balancing in Direct Server Return (DSR) mode for IPv6 networks by using the Type of Service (TOS) field when the NetScaler appliance and the servers are in different networks.

Note: The TOS field is also called the Traffic Class field.

In DSR mode, when a client sends a request to a VIP6 address on a NetScaler appliance, the appliance forwards this request to the server by changing the destination IPv6 address of the packet to the IPv6 address of the server and sets an encoded value of the VIP6 address in the TOS (also called traffic class) field of the IPv6 header. You can configure the server to use the information in the TOS field to derive the VIP6 address from the encoded value, which is then used as source IP address in response packets. Response traffic directly goes to the client, bypassing the NetScaler.



Consider an example where a load balancing virtual server LBVS1, configured on a NetScaler appliance NS1, is used to load balance traffic across servers S1, S2, and S3. The NetScaler appliance NS1 and the servers S1, S2, and S3 are in different networks so router R1 is deployed between NS1 and the servers.

The following table lists the settings used in this example.

Entities	Name
IPv6 address of client C1	C1_IP (for reference purposes only)
Load balancing virtual server on NS1	LBVS1
IPv6 address of LBVS1	LBVS1_VIP6 (for references purpose only)

TOS value	TOS_ LBVS1_VIP6 (for references purpose only)
Service for server S1 on NS1	SVC_S1
IPv6 address for server S1	S1_IP (for references purpose only)
Service for server S2 on NS1	SVC_S2
IPv6 address for server S1	S2_IP (for references purpose only)
Service for server S3 on NS1	SVC_S3
IPv6 address for server S1	S3_IP (for references purpose only)

Following is the traffic flow in the example scenario:

1. Client C1 sends a request to virtual server LBVS1.
2. LBVS1's load balancing algorithm selects server S1 and the appliance opens a connection to S1. NS1 sends the request to S1 with:
   - TOS field set to TOS_ LBVS1_VIP6.
   - Source IP address as C1_IP.
3. The server S1, on receiving the request, uses the information in the TOS field to derive the LBVS1_VIP6 address, which is the IP address of the virtual server LBVS1 on NS1. The server directly sends the response to C1, bypassing the NetScaler, with:
   - Source IP address set to the derivedLBVS1_VIP6 address so that the client communicates to the virtual server LBVS1 on NS1 and not to server S1.

To configure load balancing in DSR Mode using TOS, perform the following steps on the appliance:

1. Enable USIP mode globally.
2. Add the servers as services.
3. Configure a load balancing virtual server with a TOS value.
4. Bind the services to the virtual server.

To configure load balancing in DSR Mode using TOS by using the command line interface

At the command prompt, type:

- enable ns mode USIP
- add service <*serviceName*> <*IP*> <*serviceType*> <*port*>

  Repeat the above command as many times as necessary to add each server as a service on the NetScaler appliance.

- add lb vserver <*name*> <*serviceType*> <*ip*> <*port*> -m <*redirectionMode*> -tosId <*positive_integer*>
- bind lb vserver <*vserverName*> <*serviceName*>

Parameters for configuring a service

serviceName (Service Name)

Name of the service. This alphanumeric string is required. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

IP (Server)

Pv6 address of the server that is associated with the service.

serviceType (Protocol)

Protocol used by the service. Specify a service type of ANY.

port (Port)

Port on which the server listens for connections. The port number must be from 1 through 65534.

Parameters for configuring a load balancing virtual server

name (Name)

Name of the virtual server. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

IPAddress (IP Address)

IPv6 address of the virtual server.

serviceType (Protocol)

Protocol used by the virtual server. Specify a type of ANY.

Port (Port)

Port on which the virtual server listens for client connections. The port number must be from 1 through 65534.

m (Redirection Mode)

The load balancing redirection mode. Specify TOS for this parameter.

tosId (TOS Id)

Specify a value that the appliance sets to the TOS field of the request packets before forwarding to the server. Applicable only when the redirection mode is set as TOS for this virtual server. Minimum value: 1. Maximum value: 63.

To enable USIP mode by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the Modes and Features group, click Configure Modes.
3. In the Configure Modes dialog box, select the Use Source IP check box.

To create services by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, set the following parameters.
   - Service Name*
   - Server*
   - Protocol* (Select ANY from the drop-down list.)
   - Port*
4. Click **Create**.
5. Repeat steps 3-4 to create another service.
6. Click Close.
7. In the Services pane, select the services that you just configured and verify that the settings displayed at the bottom of the screen are correct.

To create a load balancing virtual server and bind services by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the Load Balancing Virtual Servers pane, click Add.
3. In the Create Virtual Servers (Load Balancing) dialog box, select IP Address Based and then select IPv6.
4. Set the following parameters.
   - Name*
   - IP Address*
   - Protocol* (Select ANY from the drop-down list.)
   - Port*

   * A required parameter
5. On the Advanced tab, under Redirection Mode, click TOS Based. In the TOS Id box, enter a value.
6. Under the Services tab, in the Active column, select the check box for the service that you want to bind to the virtual server.
7. Click Create, and then click Close. In the Load Balancing Virtual Servers tab, select the virtual server that you just created, and verify that the settings displayed in the Details pane are correct.

Configuring Load Balancing in DSR Mode by Using IP Over IP

You can configure your NetScaler appliance to use direct server return (DSR) mode across Layer 3 networks by using IP tunneling, also called *IP over IP* configuration. As with standard load balancing configurations for DSR mode, this allows servers to respond to clients directly instead of using a return path through the NetScaler appliance, improving response times and throughput. As with standard DSR mode, the NetScaler appliance monitors the servers and performs health checks on the application ports.

With IP over IP configuration, the NetScaler appliance and the servers do not need to be on the same Layer 2 subnet. Instead, the NetScaler appliance encapsulates the packets before sending them to the destination server. After the destination server receives the packets, it decapsulates the packets, and then sends its responses directly to the client.

To configure IP over IP DSR mode on your NetScaler appliance, you must do the following:

- **Create a load balancing virtual server.** Set the protocol to ANY and set the mode to IPTUNNEL.
- **Create services.** Create a service for each of your back-end applications. Bind the services that you created to the virtual server.

Configuring a Load Balancing Virtual Server

Configure a virtual server to handle requests to your applications. Assign a service type of ANY and set the forwarding method to IPTUNNEL. Optionally, configure the virtual server to operate in sessionless mode. You can configure any load balancing method that you want to use.

To create and configure a load balancing virtual server for IP over IP DSR by using the command line interface

At the command prompt type the following command to configure a load balancing virtual server for IP over IP DSR and verify the configuration:

- add lb vserver <name> serviceType <serviceType> IPAddress <ip> Port <port> -lbMethod <method> -m <ipTunnelTag> -sessionless <sessionless>
- show lb vserver <name>

Example

In the following example, we have selected the load balancing method as sourceIPhash and configured sessionless load balancing.

```
add lb vserver Vserver-LB-1 ANY 10.102.29.60 * -lbMethod SourceIPHash -m IPTUNNEL -sessionless enabled
```

Parameters for configuring virtual servers

name

A name for your new virtual server. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols.

serviceType

The protocol that your virtual server processes. For an IP over IP DSR virtual server, set the protocol to ANY.

IP

The IP address assigned to your virtual server. This is normally an Internet-routable IP address.

Note: If the virtual server uses IPv6, select the IPv6 check box and enter the address in IPv6 format. (An IPv6 format address appears as follows: 1000:0000:0000:0000:0005:0600:700a:888b.)

Port

The port that your virtual server listens on for traffic. For an IP over IP DSR virtual server, set the port to *.

Method

The load balancing method to use for this load balancing configuration. For information about the various load balancing methods, see "Load Balancing Algorithms."

Mode

Redirection mode for load balancing. For an IP over IP DSR virtual server, set to IPTUNNEL to perform IP-in-IP encapsulation for client IP packets.

sessionless

Perform load balancing on a per-packet basis, without establishing sessions. Recommended for load balancing in scenarios involving direct server return (DSR), where session information is unnecessary.

To create and configure a load balancing virtual server for IP over IP DSR by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Create Virtual Server dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring virtual servers" as shown:
   - Name*—name
   - Protocol*—protocol
   - IP address*—IPAddress
   - Port*—port

   * A required parameter
4. On the Advanced tab, under Redirection Mode, select IP Tunnel Based.
5. Click Create, and then click Close. The virtual server that you created now appears in the Virtual Servers pane.

Configuring Services for IP over IP DSR

After creating your load-balanced server, You must configure one service for each of your applications. The service handles traffic from the NetScaler appliance to those applications, and allows the NetScaler appliance to monitor the health of each application.

You assign a service type of ANY and configure it for USIP mode. Optionally, you can also bind a monitor of type IPTUNNEL to the service for tunnel-based monitoring.

To create and configure a service for IP over IP DSR by using the command line interface

At the command prompt, type the following commands to create a service and optionally, create a monitor and bind it to the service:

- add service <serviceName> <serverName> <serviceType> <port> -usip <usip>
- add monitor <monitorName> <monitorType> -destip <ip> -iptunnel <iptunnel>
- bind service <serviceName> -monitorName <monitorName>

Example

In the following example, we are creating a monitor of type IPTUNNEL:

```
add monitor mon-1 PING -destip 10.102.29.60 -iptunnel yes
add service Service-DSR-1 10.102.30.5 ANY * -usip yes
bind service Service-DSR-1 -monitorName mon-1
```

Service Configuration Parameters

serviceName

Name for the service. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the service has been created. Maximum Length: 127

serverName

Name of the server that hosts the service. Maximum Length: 127

serviceType

Protocol in which data is exchanged with the service.

port

Port number of the service.

usip

Use the client's IP address as the source IP address when initiating a connection to the server. Possible values: YES, NO. Set to YES for IP over IP DSR, to configure the service to use source IP mode.

monitorName

The name of the monitor that you are binding to the service.

monitorType

The type of monitor that you are binding to the service.

destip

IP address of the virtual server to which to send probes. If the parameter is set to 0, the IP address of the server to which the monitor is bound is considered the destination IP address.

iptunnel

Send the monitoring probe to the service through an IP tunnel. A destination IP address must be specified. Possible values: YES, NO. Default value: NO. Set to YES for IP over IP DSR.

To configure a monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Monitors.
2. In the details pane, click Add.
3. In the Create Monitor dialog box, specify values for the following parameters, which correspond to parameters described in "Service Configuration Parameters" as shown:
   - Monitor Name*—name
   - Type*—type
   - Destination IP—destip. Specify the IP address of the virtual server that you created earlier.

   * A required parameter
4. Select IP Tunnel.
5. Click Create, and then click Close.

To create and configure a service for IP over IP DSR by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. In the details pane, click Add.
3. In the Create Service dialog box, specify values for the following parameters, which correspond to parameters described in "Service Configuration Parameters" as shown:
   - Service Name*—name
   - Protocol*—type
   - Server*—IP
   - Port*—port

   * A required parameter
4. On the Monitors tab, from the Available list, select the monitor that you created earlier and add it to the Configured list.
5. On the Advanced tab, select Use Source IP.
6. Click Create, and then click Close.

To bind a service to a load balancing virtual server by using the command line interface

At the command prompt type the following command:

bind lb vserver <name> <serviceName>

Example

bind lb vserver Vserver-LB-1 Service-DSR-1

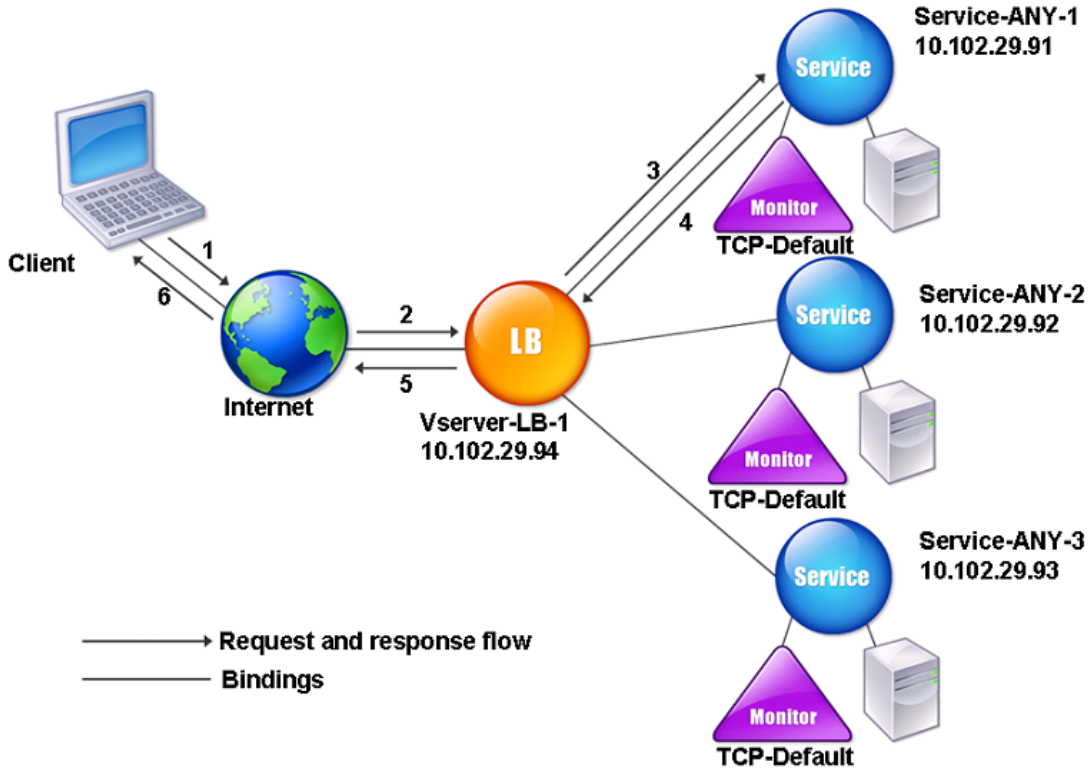
To bind a service to a load balancing virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the load balancing virtual server that you created earlier, and then select Open.
3. In the Services tab, select the check box beside the name of the service(s) that you created earlier.
4. Click OK.

Configuring Load Balancing in One-arm Mode

In a one-arm setup, you connect the NetScaler appliance to the network through a single interface. This is one of the simplest deployment scenarios, where the router, the servers and the appliance are all connected to the same switch. The client can access the server directly, bypassing the appliance, if the client knows the IP address of the server. Client requests at the switch are forwarded to the appliance, and the appliance uses the configured load balancing method to select the service, as is shown in the following diagram.

Figure 1. Entity Model for Load Balancing in One-Arm Mode



In the example scenario, the services Service-ANY-1, Service-ANY-2, and Service-ANY-3 are created and bound to the virtual server Vserver-LB-1. The virtual server load balances the client request to a service. The following table lists the names and values of the entities configured on the appliance in one-arm mode.

Entity type	Name	IP address	Protocol
Virtual server	Vserver-LB-1	10.102.29.94	ANY
Services	Service-ANY-1	10.102.29.91	ANY
	Service-ANY-2	10.102.29.92	ANY

	Service-ANY-3	10.102.29.93	ANY
Monitors	TCP	None	None

To configure a load balancing setup in one-arm mode, see "Setting Up Basic Load Balancing."

Configuring Load Balancing in the Inline Mode

In an inline mode (also called two-arm mode) setup, you deploy the NetScaler appliance to the network through more than one interface. In the two-arm setup, the appliance is connected between the servers and the client. Traffic from clients passes through the appliance to access the load balanced server. Client requests at the switch are forwarded to the appliance, and the appliance uses the configured load balancing method to select the service. This is shown in the following diagram.

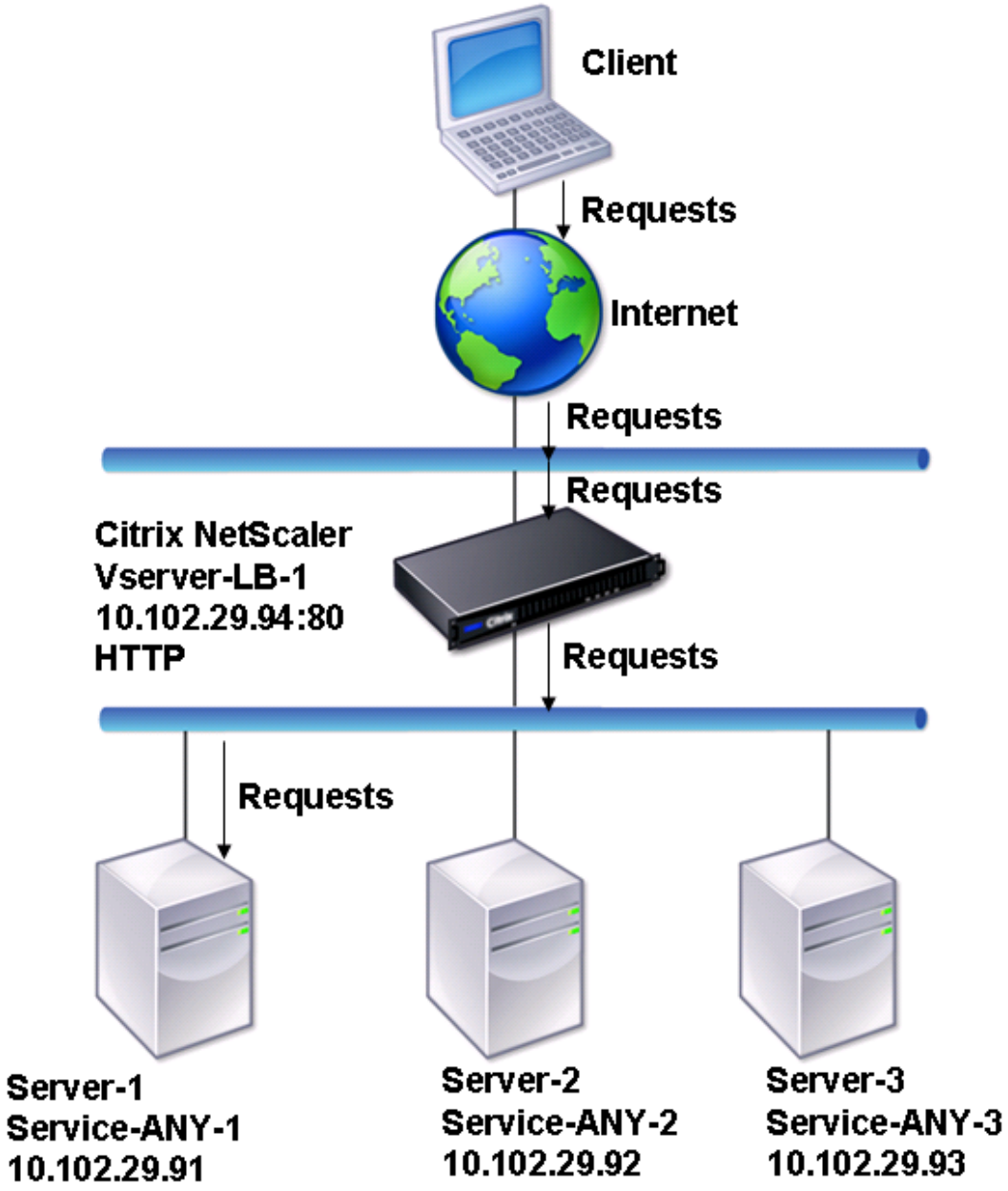


Figure 1. Load Balancing in Inline Mode

The configuration and the entity diagram for inline mode are the same as described in "Configuring Load Balancing in One-arm Mode."

Load Balancing of Intrusion Detection System Servers

To enable the NetScaler appliance to support load balancing of intrusion detection system (IDS) servers, the IDS servers and clients must be connected through a switch that has port mirroring enabled. The client sends a request to the server. Because port mirroring is enabled on the switch, the request packets are copied or sent to the NetScaler appliance virtual server port. The appliance then uses the configured load balancing method to select an IDS server, as shown in the following diagram.

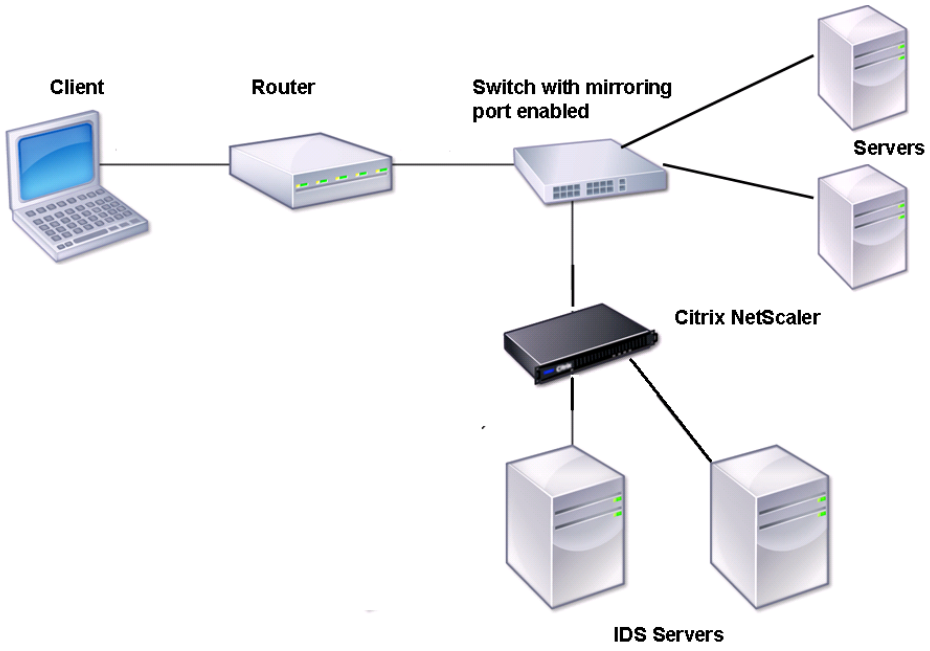


Figure 1. Topology of Load Balanced IDS Servers

Note: Currently, the appliance supports load balancing of passive IDS devices only.

As illustrated in the preceding diagram, the IDS load balancing setup functions as follows:

1. The client request is sent to the IDS server, and a switch with a mirroring port enabled forwards these packets to the IDS server. The source IP address is the IP address of the client, and the destination IP address is the IP address of the server. The source MAC address is the MAC address of the router, and the destination MAC address is the MAC address of the server.

2. The traffic that flows through the switch is mirrored to the appliance. The appliance uses the layer 3 information (source IP address and destination IP address) to forward the packet to the selected IDS server without changing the source IP address or

destination IP address. It modifies the source MAC address and the destination MAC address to the MAC address of the selected IDS server.

Note: When load balancing IDS servers, you can configure the SRCIPHASH, DESTIPHASH, or SRCIPDESTIPHASH load balancing methods. The SRCIPDESTIPHASH method is recommended because packets flowing from the client to a service on the appliance must be sent to a single IDS server.

Suppose Service-ANY-1, Service-ANY-2, and Service-ANY-3 are created and bound to Vserver-LB-1. The virtual server balances the load on the services. The following table lists the names and values of the entities configured on the appliance.

Entity type	Name	IP address	Port	Protocol
Virtual server	Vserver-LB-1	*	*	ANY
Services	Service-ANY-1	10.102.29.101	*	ANY
	Service-ANY-2	10.102.29.102	*	ANY
	Service-ANY-3	10.102.29.103	*	ANY
Monitors	Ping	None	None	None

Note: You can use inline mode or one-arm mode for an IDS load balancing setup.

The following diagram shows the load balancing entities and values of the parameters to be configured on the appliance.

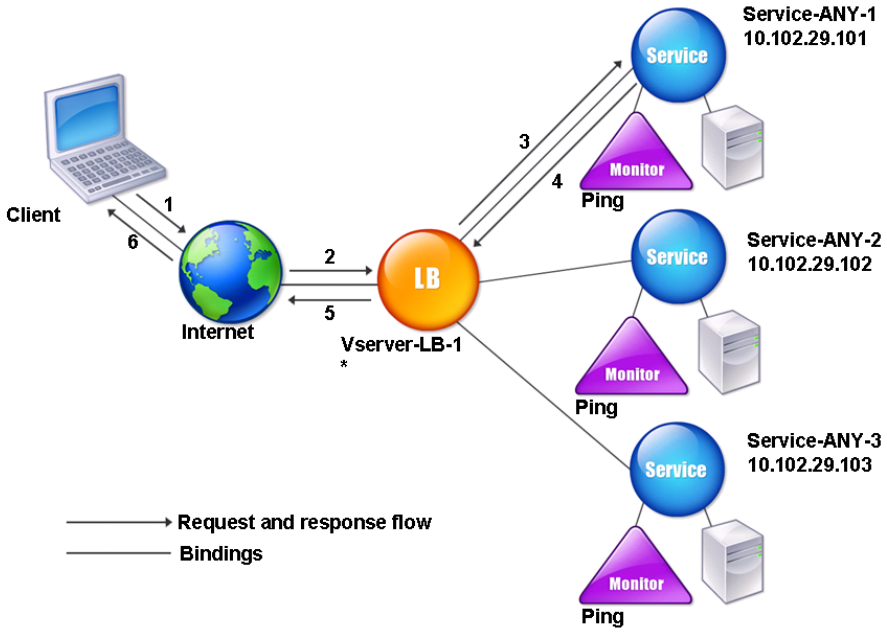


Figure 2. Entity Model for Load Balancing IDS Servers

To configure an IDS load balancing setup, you must first enable MAC-based forwarding. You must also disable layer 2 and layer 3 modes on the appliance.

To enable MAC-based forwarding by using the command line interface

At the command prompt, type:

enable ns mode <ConfigureMode>

Example

enable ns mode MAC

To enable MAC-based forwarding by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. On the Settings landing page, under Modes and Features, click modes.
3. In the Configure Modes dialog box, select the MAC Based Forwarding check box, and then click OK.
4. In the Enable/Disable Feature(s)? dialog box, and then click Yes.

Next, see "Setting Up Basic Load Balancing", to configure a basic load balancing setup.

After you configure the basic load balancing setup, you must customize it for IDS by configuring a supported load balancing method (such as the SRCIPDESTIP Hash method on a sessionless virtual server) and enabling MAC mode. The appliance does not maintain the state of the connection and only forwards the packets to the IDS servers without processing them. The destination IP address and port remains unchanged because the virtual server is in the MAC mode.

To configure LB method and redirection mode for a sessionless virtual server by using the command line interface

At the command prompt, type:

set lb vserver <vServerName> -lbMethod <LBMethodOption> -m <RedirectionMode> -sessionless <Value>

Example

set lb vserver Vserver-LB-1 -lbMethod SourceIPDestIPHash -m MAC -sessionless enabled

To configure LB method and redirection mode for a sessionless virtual server by using the configuration utility

1. In the left navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the Load Balancing Virtual Servers pane, click the virtual server Vserver-LB-1, and then click Open.
3. On the Method and Persistence tab, under LB Method, select Source IP Destination IP Hash.
4. On the Advanced tab, under Redirection Mode, click MAC Based.

5. Select the Sessionless check box, and then click OK.

To set a service to use source IP address by using the command line interface

At the command prompt, type:

set service <ServiceName> -usip <Value>

Example

set service Service-ANY-1 -usip yes

To set a service to use source IP address by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Services.
2. On the Services pane, select the service, Service-ANY-1, and then click Open.
3. On the Advanced tab, under Settings, select the Use Source IP check box.
4. Click OK.
5. Repeat steps 1-5 for the services Service-ANY-2 and Service-ANY-3.

For USIP to function correctly, you must set it globally. For more information about configuring USIP globally, see "IP Addressing."

Isolating the Network Paths by Using Traffic Domains

A very common security requirement in a data center is to maintain network path isolation between the traffic of various applications or tenants. One application or tenant's traffic must be isolated from the traffic of other applications or tenants. For example, a financial services company would want to keep the traffic of its insurance department's applications separate from that of its financial services applications. In the past, this was easily achieved through physical separation of network service devices such as firewalls, load balancers, and IDP, and network monitoring and logical separation in the switching fabric.

As data center architectures evolve toward multi-tenant virtualized data centers, networking services in the aggregation layer of a data center are getting consolidated. This development has made network path isolation a critical component for network service devices and is driving the requirement for ADCs to be able to isolate traffic at the L4 to L7 levels. Furthermore, all the traffic of a particular tenant must go through a firewall before reaching the service layer.

To address the requirement of isolating the network paths, a NetScaler appliance identifies network domains and controls the traffic across the domains. The NetScaler solution has two main components: listen policies and shadow virtual servers.

Each network path to be isolated is assigned a virtual server on which a listen policy is defined so that the virtual server listens to traffic only from a specified traffic domain.

To isolate the traffic, listen policies can be based on a number of client parameters or their combinations, and the policies can be assigned priorities. The following table lists the parameters that can be used in listen policies for identifying the traffic.

Table 1. Client Parameters Used to Define Listen Policies

Category	Parameters
Ethernet protocol	Source MAC address, destination MAC address
Network interface	Network ID, receiving throughput, sending throughput, transmission throughput
IP protocol	Source IP address, destination IP address
IPv6 protocol	Source IPv6 address, destination IPv6 address
TCP protocol	Source port, destination port, maximum segment size, payload, and other options
UDP protocol	Source port, destination port
VLAN	ID

On the NetScaler appliance, a virtual server is configured for each domain, with a listen policy specifying that the virtual server is to listen only to traffic for that domain. Also configured for each domain is a shadow load balancing virtual server, which listens to

traffic destined for any domain. Each of the shadow load balancing virtual servers has a wildcard (*) IP address and port, and its service type is set to ANY.

In each domain, a firewall for the domain is bound as a service to the shadow load balancing virtual server, which forwards all traffic through the firewall. Local traffic is forwarded to its destination, and traffic destined for another domain is forwarded to the firewall for that domain. The shadow load balancing virtual servers are configured for MAC mode redirection.

How Network Paths Are Isolated by Using NetScaler Traffic Domains

The following figure shows a typical traffic flow across domains. Consider the traffic flow within Network Domain 1, and between Network Domain 1 and Network Domain 2.

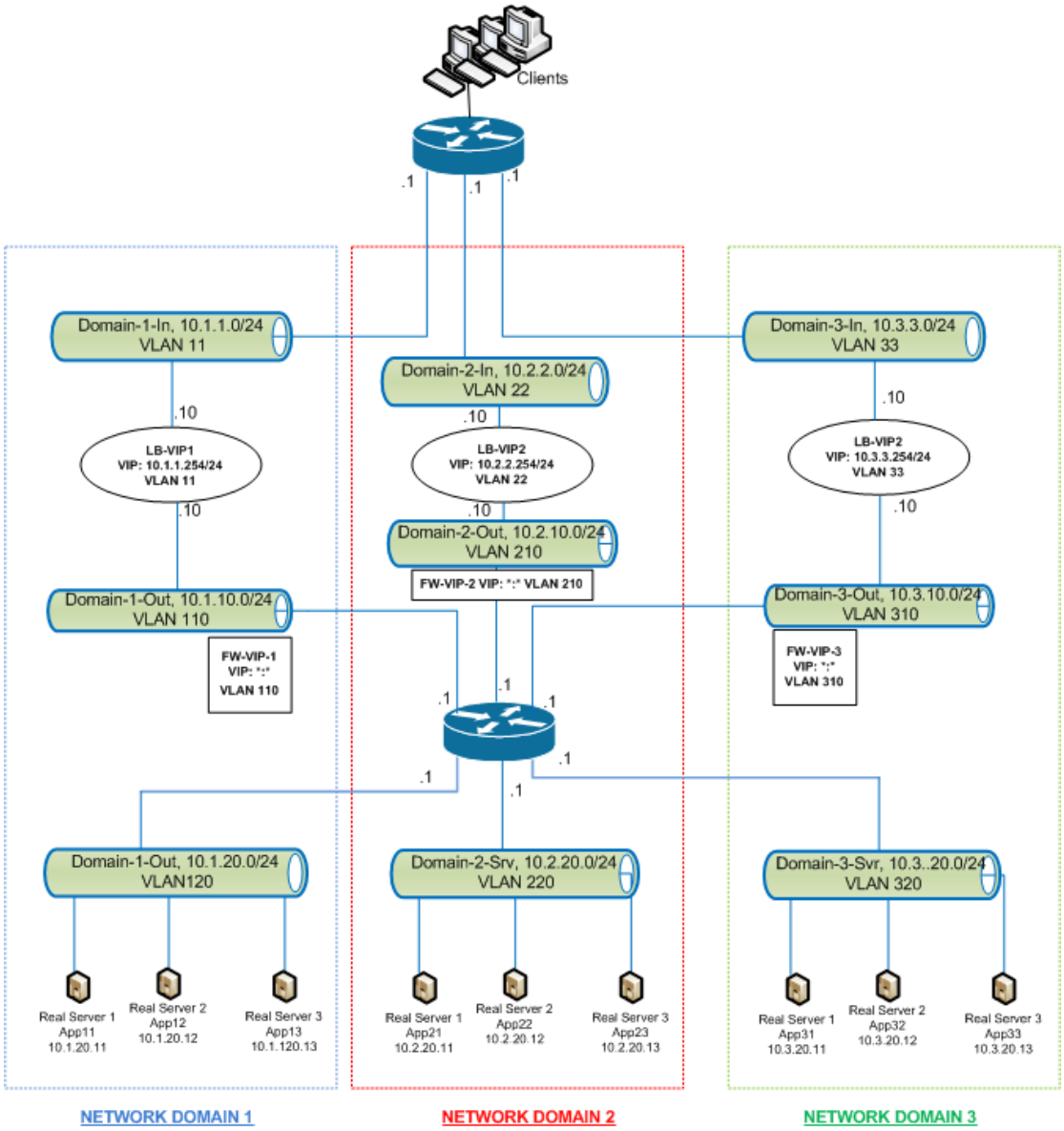


Figure 1. Network Path Isolation Using Traffic Domains

Traffic within Network Domain 1

Network Domain 1 has three VLANs: VLAN 11, VLAN110, and VLAN120. The following steps describe the traffic flow.

- A client from VLAN 11 sends a request for a service available from the service pool in VLAN 120.
- The load balancing virtual server LB-VIP1, which is configured to listen to traffic from VLAN 11, receives the request and forwards the request to VLAN 110. The virtual server in VLAN 110 forwards the request to shadow load balancing virtual server FW-VIP-1.
- FW-VIP-1, which is configured to listen to traffic from VLAN 110, receives the request and forwards it to VLAN 120.
- The load balancing virtual server in VLAN 120 load balances the request to one of the physical servers, App11, App12, or App13.
- The response sent by the physical server returns by the same path to the client in VLAN 11.

This configuration ensures that traffic is always segregated inside the NetScaler for all the traffic that originates from a client.

Traffic between Network Domain 1 and Network Domain 2

Network Domain 1 has three VLANs: VLAN 11, VLAN 110, and VLAN 120. Network Domain 2 also has three VLANS: VLAN 22, VLAN 210, and VLAN 220. The following steps describe the traffic flow from VALN 11 to VLAN 22.

- A client from VLAN 11, which belongs to Network Domain 1, sends a request for a service available from the service pool in VLAN 220, which belongs to the Network Domain 2.
- In Network Domain 1, the load balancing virtual server LB-VIP1, which is configured to listen to traffic from VLAN 11, receives the request and forwards the request to VLAN 110.
- Shadow load balancing virtual server FW-VIP-1, which is configured to listen to VLAN 110 traffic destined to any other domain, receives the request and forwards it to firewall virtual server FW-VIP-2 because the request is destined to a physical server in Network Domain 2.
- In Network Domain 2, FW-VIP-2 forwards the request to VLAN 220.
- The load balancing virtual server in VLAN 220 load balances the request to one of the physical servers, App21, App22, or App23.
- The response sent by the physical server returns by the same path through the firewall in Network Domain 2 and then to Network Domain 1 to reach the client in VLAN 11.

Configuring Traffic Domains

To configure network path isolation by using listen policies, do the following:

- Add listen policy expressions. Each expression specifies a domain to which traffic is destined. You can use the VLAN ID or other parameters to identify the traffic. For more details, see "Client Parameters Used to Define Listen Policies."
- For each network domain, configure two virtual servers as follows:
  - Create a load balancing virtual server for which you specify a listen policy that identifies the traffic destined for this domain. You can specify the name of an expression created earlier, or you can create a new expression while creating the virtual server.
  - Create another load balancing virtual server, referred to as shadow virtual server, for which you specify a listen policy expression that applies to traffic destined for any domain. On this virtual server, set the service type to ANY and the IP address and port to an asterisk (*). Enable MAC-based forwarding on this virtual server.
  - Enable the L2 Connection option on both the virtual servers.

    Generally, to identify a connection, the NetScaler uses the 4-tuple of client IP address, client port, destination IP address, and destination port. When you enable the L2 Connection option, the Layer 2 parameters of the connection (channel number, MAC address, and VLAN ID) are used in addition to the normal 4-tuple.
- Add services representing the server pools in the domain, and bind them to the virtual server.
- Configure the firewall for each domain as a service, and bind all of the firewall services to the shadow virtual server.

To configure traffic domains by using the command line interface

At the command prompt, type the following commands:

- add policy expression <expressionName> <listenPolicyExpression>
- add lb vserver <name> <serviceType> <ip> <port> -l2conn ON -listenPolicy <expressionName>

  Add a load balancing virtual server for each domain. This virtual server is for traffic of the same domain.
- add lb vserver <name> ANY * * -l2conn ON -m MAC -listenPolicy <expressionName>

  Add a shadow load balancing virtual server for each domain. This virtual server is for traffic of other domains.

Example

```
add policy expression e110 client.vlan.id==110
add policy expression e210 client.vlan.id==210
add policy expression e310 client.vlan.id==310
add policy expression e11 client.vlan.id==11
add policy expression e22 client.vlan.id==22
add policy expression e33 client.vlan.id==33

add lb vserver LB-VIP1 HTTP 10.1.1.254 80 -persistenceType NONE -listenPolicy e11
-cltTimeout 180 -l2Conn ON

add lb vserver LB-VIP2 HTTP 10.2.2.254 80 -persistenceType NONE - listenPolicy e22
-cltTimeout 180 -l2Conn ON

add lb vserver LB-VIP3 HTTP 10.3.3.254 80 -persistenceType NONE - listenPolicy e33
-cltTimeout 180 -l2Conn ON


add lb vserver FW-VIP-1 ANY * * -persistenceType NONE -lbMethod ROUNDROBIN - listenPolicy e110 -Listenpri

add lb vserver FW-VIP-2 ANY * * -persistenceType NONE -lbMethod ROUNDROBIN - listenPolicy e210 -Listenpri

add lb vserver FW-VIP-3 ANY * * -persistenceType NONE -lbMethod ROUNDROBIN - listenPolicy e310 -Listenpri


add service RD-1 10.1.1.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO -CMP NO

add service RD-2 10.2.2.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO -CMP NO

add service RD-3 10.3.3.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO -CMP NO


bind lb vserver FW-VIP-1 RD-1

bind lb vserver FW-VIP-2 RD-2

bind lb vserver FW-VIP-3 RD-3
```

Parameters for configuring a service

name

Name of the service. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serverName

Either the name of a previously created server object, or the IP address of the load-balanced server that hosts this service, in either IPv4 or IPv6 format. When you

provide the IP address of the service, a server object is created with this IP address as its name. You can also create a server object manually, and then select the server name instead of an IP address from the drop-down menu that is associated with this field.

If the server is not reachable from the NetScaler or is not active, the service is designated as DOWN.

serviceType

The type of connections that the service will handle. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, DNS_TCP, ADNS_TCP, RADIUS, MYSQL, MSSQL, and RDPHTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, and SSL_DIAMETER. Default: HTTP.

port

Port on which the service listens. The port number must be a positive number not greater than 65534.

Parameters for configuring a virtual server

name

Name of the virtual server. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( )

IPAddress

IP address of the virtual server. This IP address can be an IPv4 or IPv6 address, and is usually a public IP address. Clients send connection requests to this IP address.

serviceType

The type of services to which the virtual server distributes requests. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, and MSSQLHTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, and SSL_DIAMETER. Default: HTTP

port

Port on which the virtual server listens for client connections. The port number must be between 0-65535.

l2conn

The tuple used to identify a connection includes the layer 2 parameters

To configure traffic domains by using the configuration utility

1. Add services representing the servers, as described in "Creating a Service."
2. Add each firewall as a service:
    a. In the navigation pane, expand Load Balancing, and then click Services.
    b. In the details pane, click Add.
    c. In the Create Service dialog box, specify values for the following parameters:
        · Service Name*—The name that you assign to the service.
        · Protocol*—Select ANY from the drop-down list.
        · Server*—The firewall's IP address.
        · Port*—Specify a value of 80.
    *A required parameter
    d. Click Create.
    e. From the Services pane, open the services you created and verify the settings.
3. Configure a load balancing virtual server.
    a. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
    b. In the details pane, click Add.
    c. In the Create Virtual Server (Load Balancing) dialog box, specify values for the following parameters, which are described in "Creating a Virtual Server."
        · Name*
        · Protocol*
        · IP Address*
        · Port*
    *A required parameter
    d. On the Services tab, select the corresponding services.
    e. On the Advanced tab, select the L2 Connection check box and, for Redirection Mode, select MAC Based. Then, click the Listen Policy link and create the listen policy for the virtual server.
    f. Click Create.
4. Configure the shadow load balancing virtual server.
    a. For the shadow virtual server, specify

- Protocol—ANY
- IP Address*—*
- Port*—*

*A required parameter

b. Bind the firewall services to the shadow virtual server.

5. For each network domain, repeat steps 3 and 4.
6. From the Load Balancing Virtual Servers pane, open the virtual servers that you created and verify the settings.

Configuring XenDesktop for Load Balancing

For an improved performance in the delivery of virtual desktop applications, you can integrate the NetScaler appliance with Citrix XenDesktop and use the NetScaler load balancing feature to distribute the load across the Web Interface servers and the Desktop Delivery Controller (DDC) servers.

Generally, you use XenDesktop in situations where applications are not compatible with running on a terminal server or XenApp, or if each virtual desktop has unique requirements. In such cases, you need one desktop host for each user that connects. However, the hosts can be pooled so that you need only one host for each currently connected user.

The core application service deployed for XenDesktop is the Desktop Delivery Controller (DDC). The DDC is installed on a server, and its main function is to register desktop hosts and broker client connections to them.

The DDC also authenticates users and manages the assembly of the users' virtual desktop environments by controlling the state of the desktops, and starting and stopping the desktops.

Generally, multiple DDCs are installed to enhance availability.

The Web Interface servers provide secure access to virtual desktops. The Web Interface is the initial connection portal to the Desktop Delivery Controller (DDC). The Web browser on the user's device sends information to the Web server, which communicates with the server farm to provide the user with access to the virtual desktop.

The following figure shows the topology of a NetScaler appliance working with XenDesktop.

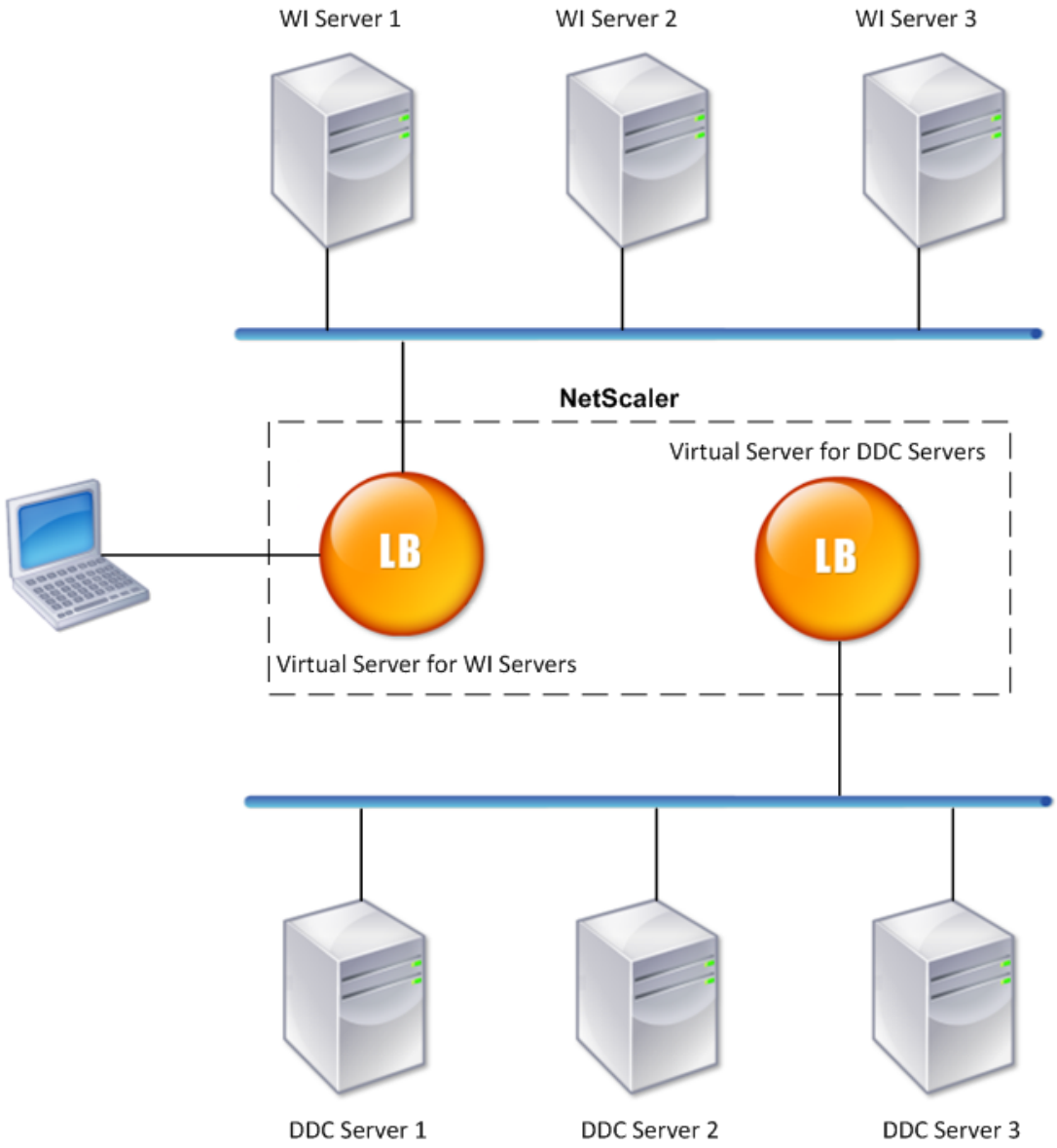


Figure 1. **Load Balancing of XenDesktop**

Note: Although you can use the HTTP protocol, Citrix recommends that you use SSL for communication between the client and the NetScaler. You can use the HTTP protocol for communication between the NetScaler and the DDC servers even though you use the SSL protocol for communication with the client.

A wizard is available for configuring basic load balancing in a XenDesktop deployment. You can use the wizard to configure Web interface servers and a virtual server for them, and DDC servers and a virtual server for them. The virtual servers that you configure are bound to services specified as Web Interface services and DDC services. Each virtual server is configured with the default load balancing method, and the default features are enabled. A monitor is created and bound to each virtual server.

The wizard creates a basic setup, with default values for options such as the load balancing method, policies, persistence, and advanced settings. You can change any of the values if necessary.

To configure load balancing for XenDesktop by using the configuration utility

1. In the navigation pane, click Load Balancing.
2. In the Getting Started group, click Load balancing wizard for Citrix XenDesktop.
3. Follow the instructions presented by the wizard.

Configuring XenApp for Load Balancing

For efficient delivery of applications, you can integrate the NetScaler appliance with Citrix XenApp and use the NetScaler load balancing feature to distribute the load across the XenApp server farms. The following figure is a topology diagram of such a setup.

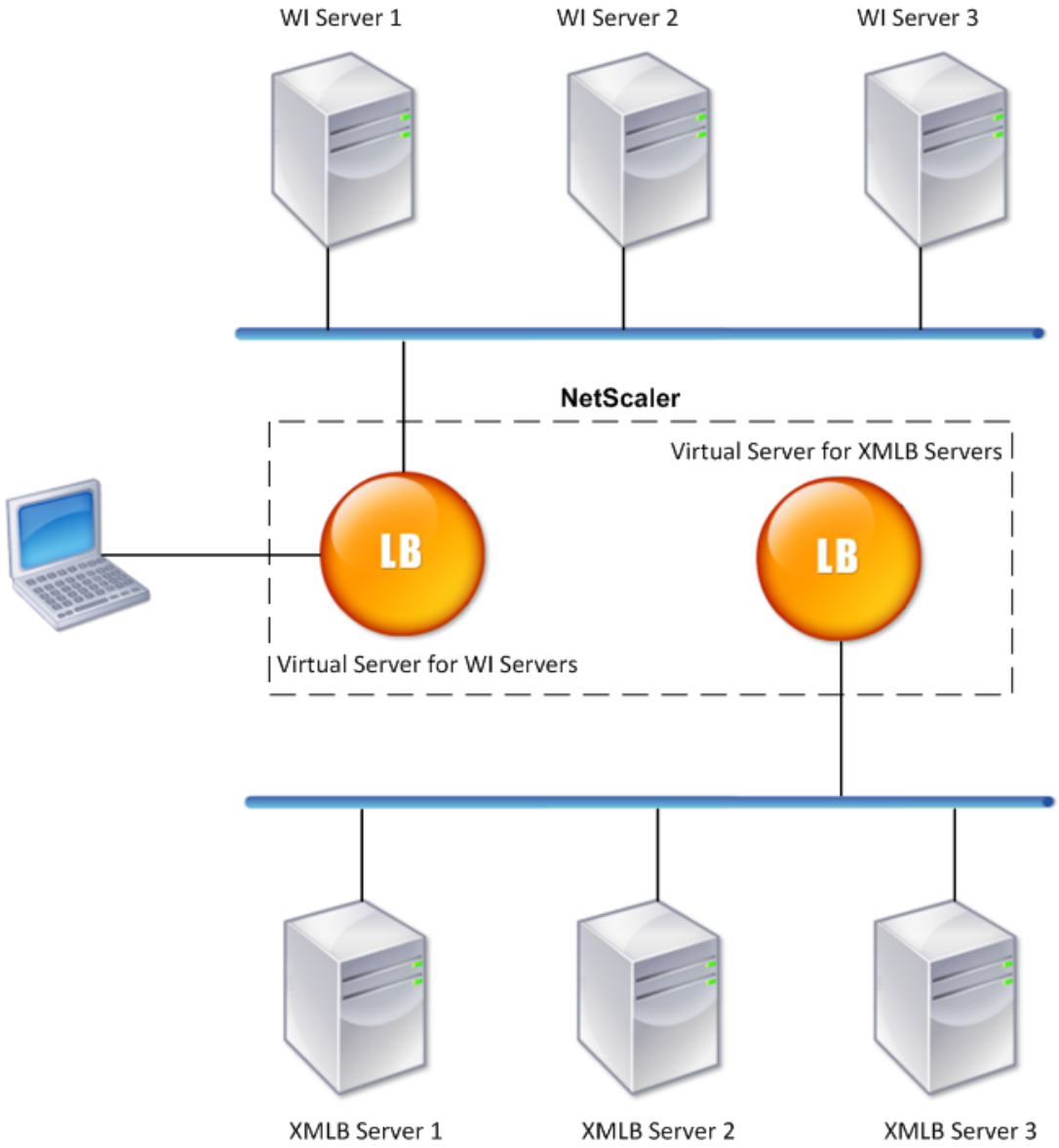


Figure 1. Load Balancing of XenApp

The Web Interface servers provide secure access to XenApp application resources through the user's Web browser. The Web Interface client presents to the users all the resources, such as applications, content, and desktops that are made available in the XenApp server farms. Users can access the published resources through a standard Web browser or through the Citrix online plug-in.

The Web browser on the user's device sends information to the Web server, which communicates with the servers on the server farm to provide the user with access to the resources.

The Web Interface and the XML Broker are complementary services. The Web Interface provides users with access to applications, and the XML Broker evaluates the user's permissions to determine which applications appear in the Web Interface.

The XML service is installed on all the servers in the server farm. The XML service specified in the Web Interface functions as an XML broker. On the basis of the user credentials passed by the Web Interface server, the XML Broker server sends a list of applications accessible to the user.

In large enterprises where multiple Web Interface servers and XML Broker servers are deployed, Citrix recommends load balancing these servers by using NetScaler. Configure one virtual server to load balance all of the Web Interface servers and another for all of the XML Broker servers. The load balancing method and other features can be configured on the virtual server as required.

Note: Although you can use the HTTP protocol, Citrix recommends that you use SSL for communication between the client and the NetScaler. You can use the HTTP protocol for communication between the NetScaler and the WI servers even though you use the SSL protocol for communication with the client.

The configuration utility provides a wizard for setting up basic load balancing for XenApp.

Through this wizard, you can configure Web Interface servers and a virtual server for them, and XML Broker servers and a virtual server for them. You can also specify the site through which the status of Web Interface servers can be monitored and the software application used to monitor the status of the XML Broker servers.

When you complete the wizard, a basic load balancing setup is configured on the NetScaler. The specified virtual servers are created and bound to the services specified as Web Interface services and XML Broker services. Each virtual server is configured with the default load balancing method, and the default features are enabled. A monitor is created and bound to each virtual server.

The wizard creates a basic setup with default values for options such as the load balancing method, policies, persistence, and advanced settings. You can change any of the values if necessary.

To configure load balancing for XenApp by using the configuration utility

1. In the navigation pane, click Load Balancing.
2. In the Getting Started group, click Load balancing wizard for Citrix XenApp.
3. Follow the instructions presented by the wizard.

Troubleshooting Common Problems

Below are a few tips for troubleshooting common problems when configuring load balancing on the NetScaler appliance.

- When a metric bound to a monitor is present in the local and custom metric tables, add the local prefix to the metric name if the metric is chosen from the local metric table. If the metric is chosen from the custom table, no prefix needs to be added.
- If the metric table is modified (for example, if the OID for the metric is changed), the change is reflected in the monitoring table. SNMP queries originating from the monitor then use the new OID.
- Load monitors cannot decide the state of the service. Therefore, setting a weight on the load monitors is inappropriate.
- If multiple load monitors are bound to a service, then the load on the service is the sum of all the values on the load monitors bound to it. For load balancing to work properly, you must bind the same set of monitors to all the services.
- When you bind a service to a virtual server where the LB method is CUSTOMLOAD, and if the service is up, then the virtual server is put to initial round robin. It continues to be in round robin if the service has no custom load monitors, or if at least one of the custom load monitors is not up.
- If you disable a load monitor bound to the service, and if the service is bound to a virtual server, then the virtual server goes to round robin.
- If you disable a metric-based binding, and if this is the last active metric, then the specific virtual server goes to round robin. A metric is disabled by setting the metric threshold to zero.
- When a metric bound to a monitor crosses the threshold value, then that particular service is not considered for load balancing.
- If all the services have reached the threshold, then the virtual server goes into round robin and an error message “5xx - server busy error” is received.

    - All the services that are bound to a virtual server where the load balancing method is CUSTOMLOAD must have load monitors bound to them.
    - The OIDs must be scalar variables.
    - For successful load balancing, the interval must be as low as possible. If the interval is high, the time period for retrieving the load value increases. As a result, load balancing takes place using improper values.
    - The CUSTOMLOAD load balancing method also follows startup round robin.
    - A user cannot modify the local table.

- A maximum of 10 metrics from a custom table can be bound to the monitor.

SSL Offload and Acceleration

A Citrix® NetScaler® appliance configured for SSL acceleration transparently accelerates SSL transactions by offloading SSL processing from the server. To configure SSL offloading, you configure a virtual server to intercept and process SSL transactions, and send the decrypted traffic to the server (unless you configure end-to-end encryption, in which case the traffic is re-encrypted). Upon receiving the response from the server, the appliance completes the secure transaction with the client. From the client's perspective, the transaction seems to be directly with the server. A NetScaler configured for SSL acceleration also performs other configured functions, such as load balancing.

Configuring SSL offloading requires an SSL certificate and key pair, which you must obtain if you do not already have an SSL certificate. Other SSL-related tasks that you might need to perform include managing certificates, managing certificate revocation lists, configuring client authentication, and managing SSL actions and policies.

A non-FIPS NetScaler appliance stores the server's private key on the hard disk. On a FIPS appliance, the key is stored in a cryptographic module known as a hardware security module (HSM). Only the MPX 9700/10500/12500/15500 appliances support a FIPS card, so other NetScaler models cannot be equipped with an HSM.

Beginning with release 10.5, build 52.1115.e, all NetScaler appliances that do not support a FIPS card (including virtual appliances) support the Thales nShield® Connect external HSM. (MPX 9700/10500/12500/15500 appliances do not support an external HSM.)

Note: FIPS-related options for some of the SSL configuration procedures described in this document are specific to a FIPS-enabled NetScaler.

Configuring SSL Offloading

To configure SSL offloading, you must enable SSL processing on the NetScaler appliance and configure an SSL based virtual server that will intercept SSL traffic, decrypt the traffic, and forward it to a service that is bound to the virtual server. To enable SSL offloading, you must import a valid certificate and key and bind the pair to the virtual server.

Enabling SSL Processing

To process SSL traffic, you must enable SSL processing. You can configure SSL based entities, such as virtual servers and services, without enabling SSL processing, but they will not work until SSL processing is enabled.

To enable SSL processing by using the command line interface

At the command prompt, type:

- enable ns feature `ssl`
- show ns feature

Example

```
> enable ns feature SSL
 Done
> show ns feature

      Feature                Acronym          Status
      -------                -------          ------
1)    Web Logging              WL               OFF
2)    Surge Protection         SP               ON
3)    Load Balancing           LB               ON
.
.
.
9)    SSL Offloading           SSL              ON
.
.
.
24)   NetScaler Push           push             OFF
Done
```

To enable SSL processing by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. Under Modes and Features, click Configure basic features.
3. Select the SSL Offloading check box, and then click OK.
4. In the Enable/Disable Feature(s)? message box, click Yes. A message appears in the status bar, stating that the feature has been enabled.

Configuring Services

On the NetScaler appliance, a service represents a physical server or an application on a physical server. Once configured, services are in the disabled state until the appliance can reach the physical server on the network and monitor its status.

To add a service by using the command line interface

At the command prompt, type the following commands to add a service and verify the configuration:

- add service <name> (<IP> | <serverName>) <serviceType> <port>
- show service <serviceName>

Example

```
> add service ssl1 10.102.29.252 HTTP 80
 Done
> show service ssl1
        ssl1 (10.102.29.252:80) - HTTP
        State: UP
        Last state change was at Thu Nov 12 05:26:31 2009
        Time since last state change: 0 days, 00:00:06.750
        Server Name: 10.102.29.252
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): YES
        Idle timeout: Client: 180 sec   Server: 360 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: ON
        Down state flush: ENABLED

1)      Monitor Name: tcp-default
                State: UP       Weight: 1
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.
                Response Time: N/A
 Done
```

To modify or remove a service by using the command line interface

To modify a service, use the set service command, which is just like using the add service command, except that you enter the name of an existing service. To remove a service, use the rm service command, which accepts only the <name> argument.

Parameters for adding a service

name (Service Name)

The name of the service you are configuring. The name can begin with a letter, a number, or the underscore symbol, and can consist of from one to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should choose a name that helps identify the type of service being added. (Cannot be changed after the action has been created.)

IP (Server)

The physical IP address of the server that the service you are configuring represents. Make sure that the server is reachable by the NetScaler.

serverName

The name of the server that the service you are configuring represents.

serviceType (Protocol)

The type of data handled by the server or application that the service you are configuring represents. For example, for web traffic, add a service of type HTTP.

port (Port)

The port number on which the service sends and receives data to and from the server.

To configure a service by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Services.
2. In the Details pane, do one of the following:
   - To create a new service, click Add.
   - To modify an existing service, select the service, and then click Open.
3. In the Create Service or Configure Service dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for adding a service” as shown:
   - Service Name*
   - Server*
   - Protocol*
   - Port*

   * A required parameter
4. Click Create or OK, and then click Close. In the Services pane, select the service that you just configured and verify that the settings displayed at the bottom of the screen are correct.

Configuring an SSL-Based Virtual Server

Secure sessions require establishing a connection between the client and an SSL-based virtual server on the NetScaler appliance. The SSL virtual server intercepts SSL traffic, decrypts it and processes it before sending it to services that are bound to the virtual server.

Note: The SSL virtual server is marked as down on the NetScaler appliance until a valid certificate / key pair and at least one service are bound to it. An SSL based virtual server is a load balancing virtual server of protocol type SSL or SSL_TCP. The load balancing feature must be enabled on the NetScaler.

To add an SSL-based virtual server by using the command line interface

At the command prompt, type the following commands to create an SSL-based virtual server and verify the configuration:

- add lb vserver <name> (serviceType) <IPAddress> <port>
- show lb vserver <name>

Example

```
> add lb vserver vssl  SSL 10.102.29.133 443
 Done
> show ssl vserver vssl

        Advanced SSL configuration for VServer vssl:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 0
        Session Reuse: ENABLED          Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)      Cipher Name: DEFAULT
        Description: Predefined Cipher Alias
 Done
```

To modify or remove an SSL-based virtual server by using the command line interface

To modify the load balancing properties of an SSL virtual server, use the set lb vserver command, which is just like using the add lb vserver command, except that you enter the name of an existing vserver. To modify the SSL properties of an SSL-based virtual server, use the set ssl vserver command. For more information, see Customizing the SSL Configuration.

To remove an SSL virtual server, use the rm lb vserver command, which accepts only the <name> argument.

Parameters for adding an SSL-based virtual server

name (Name)

The name of the SSL based virtual server you are configuring. The name can begin with a letter, a number, or the underscore symbol, and can consist of from one to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should choose a name that helps identify the server being added.

IPAddress (IP Address)

The IP address of the virtual server that you are adding.

serviceType (Protocol)

The service that you are adding can either be of type SSL to handle secure HTTP traffic or SSL_TCP to handle secure TCP traffic.

port (Port)

The port number on which the virtual server receives SSL traffic. This is usually set to 443 for all secure transactions.

To configure an SSL-based virtual server by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. In the Details pane, do one of the following:
   - To create a new virtual server, click Add.
   - To modify an existing virtual server, select the virtual server, and then click Open.
3. In the Create Virtual Server (SSL Offload) or Configure Virtual Server (SSL Offload) dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for adding an SSL-based virtual server” as shown:
   - Name*
   - IP Address*
   - Protocol*
   - Port*

   * A required parameter
4. Click Create or OK, and then click Close. In the SSL Offload Virtual Servers pane, select the virtual server that you just configured and verify that the settings displayed at the bottom of the screen are correct.

Binding Services to the SSL-Based Virtual Server

For the NetScaler appliance to forward decrypted SSL data to servers in the network, services representing these physical servers must be bound to the virtual server that receives the SSL data.

Because the link between the NetScaler and the physical server is typically secure, data transfer between the appliance and the physical server does not have to be encrypted. However, you can provide end-to end-encryption by encrypting data transfer between the NetScaler and the server. For details, see Configuring SSL Offloading with End-to-End Encryption.

Note: The Load Balancing feature should be enabled on the NetScaler appliance before you bind services to the SSL based virtual server.

To bind a service to a virtual server by using the command line interface

At the command prompt, type the following commands to bind the service to the virtual server and verify the configuration:

- bind lb vserver <name> <serviceName>
- show lb vserver <name>

Example

```
> bind lb vserver vssl ssl1
 Done
> show lb vserver vssl
      vssl (10.102.29.133:443) - SSL  Type: ADDRESS
      State: DOWN[Certkey not bound]
      Last state change was at Thu Nov 12 05:31:17 2009 (+485 ms)
      Time since last state change: 0 days, 00:08:52.130
      Effective State: DOWN
      Client Idle Timeout: 180 sec
      Down state flush: ENABLED
      Disable Primary Vserver On Down : DISABLED
      No. of Bound Services :  1 (Total)      1 (Active)
      Configured Method: LEASTCONNECTION
      Mode: IP
      Persistence: NONE
      Vserver IP and Port insertion: OFF
      Push: DISABLED  Push VServer:
```

```
        Push Multi Clients: NO
        Push Label Rule: none

1) ssl1 (10.102.29.252: 80) - HTTP State: UP    Weight: 1
 Done
```

To unbind a service from a virtual server by using the command line interface

At the command prompt, type the following command:

unbind lb vserver <name> <serviceName>

Example

unbind lb vserver vssl ssl1

Parameters for binding a service to a virtual server

name

The name of the SSL based virtual server to which you are binding the service.

serviceName

The name of the service being bound to the SSL based virtual server. The service must be configured on the NetScaler before it is bound to the virtual server.

To bind a service to a virtual server by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. In the details pane, select the virtual server to which you want to bind the service, and click Open.
3. In the Configure Virtual Server (SSL Offload) dialog box, select the Services tab, and then select the check box in the Active column of the ssl service that you want to bind to the virtual server.
4. Click OK. A message appears in the status bar, stating that the service has been bound successfully

Adding or Updating a Certificate-Key Pair

For any SSL transaction, the server needs a valid certificate and the corresponding private and public key pair. The SSL data is encrypted with the server's public key, which is available through the server's certificate. Decryption requires the corresponding private key.

Because the NetScaler appliance offloads SSL transactions from the server, the server's certificate and private key must be present on the appliance, and the certificate must be paired with its corresponding private key. This certificate-key pair must then be bound to the virtual server that processes the SSL transactions.

Both the certificate and the key must be in local storage on the NetScaler appliance before they can be added to the appliance. If your certificate or key file is not on the appliance, upload it to the appliance before you create the pair.

Important: Certificates and keys are stored in the /nsconfig/ssl directory by default. If your certificates or keys are stored in any other location, you must provide the absolute path to the files on the NetScaler appliance. The NetScaler FIPS appliances do not support external keys (non-FIPS keys). On a FIPS appliance, you cannot load keys from a local storage device such as a hard disk or flash memory. The FIPS keys must be present in the Hardware Security Module (HSM) of the appliance.

On a NetScaler MPX appliance and a NetScaler FIPS appliance, only RSA private keys are supported. On a VPX virtual appliance, both RSA and DSA private keys are supported. On an SDX appliance if SSL chips are assigned to an instance, then only RSA private keys are supported. However, if SSL chips are not assigned to an instance, then both RSA and DSA private keys are supported. In all the cases, you can bind a CA certificate with either RSA or DSA keys.

Set the notification period and enable the expiry monitor to be prompted before the certificate expires.

Note: A certificate must be signed by using one of the following hash algorithms:

- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

An MPX appliance supports certificates from 512-bits up to the following sizes:

- 4096-bit server certificate on the virtual server
- 4096-bit client certificate on the service

- 4096-bit CA certificate (includes intermediate and root certificates)
- 4096-bit certificate on the back end server
- 4096-bit client certificate (if client authentication is enabled on the virtual server)

A virtual appliance supports certificates from 512-bits up to the following sizes:

- 4096-bit server certificate on the virtual server
- 4096-bit client certificate on the service
- 4096-bit CA certificate (includes intermediate and root certificates)
- 2048-bit certificate on the back end server
- 2048-bit client certificate (if client authentication is enabled on the virtual server)

To add a certificate-key pair by using the command line interface

At the command prompt, type the following commands to add a certificate-key pair and verify the configuration:

- add ssl certKey <certkeyName> -cert <string>[(-key <string> [-password]) | -fipsKey <string>] [-inform (DER | PEM)] [<passplain>] [-expiryMonitor (ENABLED | DISABLED) [-notificationPeriod <positive_integer>]]
- show ssl certKey [<certkeyName>]

Example

```
> add ssl certKey sslckey -cert server_cert.pem -key server_key.pem -password ssl -expiryMonitor ENABLED -
 Done
Note: For FIPS appliances, replace -key with -fipskey
> show ssl certKey sslckey
      Name: sslckey          Status: Valid,   Days to expiration:8418
      Version: 3
      Serial Number: 01
      Signature Algorithm: md5WithRSAEncryption
      Issuer:  C=US,ST=SJ,L=SJ,O=NS,OU=NSSSL,CN=www.root.com
      Validity
            Not Before: Jul 15 02:25:01 2005 GMT
            Not After : Nov 30 02:25:01 2032 GMT
      Subject:  C=US,ST=SJ,L=SJ,O=NS,OU=NSSSL,CN=www.server.com
      Public Key Algorithm: rsaEncryption
      Public Key size: 1024
 Done
```

To update or remove a certificate-key pair by using the command line interface

To modify the expiry monitor or notification period in a certificate-key pair, use the set ssl certkey command. To replace the certificate or key in a certificate-key pair, use the update ssl certkey command. The update ssl certkey command has an additional parameter for overriding the domain check. For both commands, enter the name of an existing certificate-key pair. To remove an SSL certificate-key pair, use the rm ssl certkey command, which accepts only the <certkeyName> argument.

Parameters for adding a certificate-key pair

certkeyName (Certificate-Key Pair Name)

The name of the certificate-key pair added to the NetScaler. Maximum length: 31. (Cannot be changed after the certificate has been added.)

cert (Certificate File Name)

The file name of the valid certificate. The certificate file should be present on the NetScaler appliance's hard-disk drive. The default path for the certificate file is /nsconfig/ssl/. If the certificate is stored at any other location, the absolute path to the file must be provided. However, Citrix does not recommend storing the certificate in a location other than the default, because this may result in inconsistency during synchronization in an HA setup. Maximum length: 63 characters.

key (Private Key File Name)

The file name of the private key used to create the certificate. The private-key file must be present on the NetScaler appliance's hard disk drive. The default path for the key file is /nsconfig/ssl/. If the key is stored at any other location, the absolute path to the file must be provided. If you are adding a Certificate-Authority (CA) certificate file, do not add a private key. This parameter is not applicable to an SSL FIPS appliance. Maximum length: 63 characters.

fipskey

The name of the FIPS key used to create the certificate. The FIPS key is created and stored inside the FIPS Hardware Security Module (HSM). This option is applicable only to an SSL FIPS appliance. Maximum length: 63 characters.

password (Password)

The pass phrase that was used to encrypt the private key. This option can be used to load encrypted private-keys. Maximum length: 31 characters.

Note: Password protected private keys are supported only for the PEM format.

inform (Certificate Format)

The input format of the certificate and the private-key files.

The two formats supported by the system are:

PEM: Privacy Enhanced Mail

DER: Distinguished Encoding Rule

Possible values: DER, PEM

Default value: PEM

passplain

The pass phrase that was used to encrypt the private key. This option can be used to load encrypted private keys. Maximum length: 31 characters.

Note: Password protected private key is supported only for the PEM format. Maximum length: 31 characters.

expiryMonitor (Notify When Expires)

Issue an alert when the certificate is about to expire. Possible values: ENABLED, DISABLED

notificationPeriod (Notification Period)

Number of days before certificate expiration, at which to generate an alert that the certificate is about to expire. Minimum value: 10. Maximum value: 100.

noDomainCheck (No Domain Check)

When updating a certificate-key pair, override the check for matching domain names.

To add or update a certificate-key pair by using the configuration utility

1. In the navigation pane, expand SSL, and then click Certificates.
2. In the Details pane, do one of the following:
   - To add a new certificate-key pair, click Add.
   - To update an existing certificate-key pair, click Update.
3. In the Install Certificate or Update Certificate dialog box, set the following parameters:
   - Certificate-Key Pair Name*
   - Certificate File Name*
   - Private Key File Name
   - Password
   - Certificate Format
   - Notify When Expires
   - Notification Period
   - No Domain Check (Available in the Update Certificate dialog box only)

   * A required parameter
4. Click Install or OK, and then click Close. In the SSL Certificates pane, select the certificate that you just configured and verify that the settings displayed at the bottom of the screen are correct.

Binding the Certificate-Key Pair to the SSL-Based Virtual Server

An SSL certificate is an integral element of the SSL encryption and decryption process. The certificate is used during an SSL handshake to establish the identity of the SSL server.

The certificate being used for processing SSL transactions must be bound to the virtual server that receives the SSL data. If you have multiple virtual servers receiving SSL data, a valid certificate-key pair must be bound to each of them.

You can use a valid, existing SSL certificate that you have uploaded to the NetScaler appliance. As an alternative for testing purposes, you can create your own SSL certificate on the appliance. Intermediate certificates created by using a FIPS key on the NetScaler cannot be bound to an SSL virtual server.

For details on how to create your own certificate, see Managing Certificates.

Note: Citrix recommends that you use only valid SSL certificates that have been issued by a trusted certificate authority.

To bind an SSL certificate-key pair to a virtual server by using the command line interface

At the command prompt, type the following commands to bind an SSL certificate-key pair to a virtual server and verify the configuration:

- bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>
- show ssl vserver <vServerName>

Example

```
> bind ssl vserver vssl -certkeyName
sslckey
 Done
> show ssl vserver vssl

        Advanced SSL configuration for VServer vssl:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 0
        Session Reuse: ENABLED          Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
```

```
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)      CertKey Name: sslckey   Server Certificate

1)      Cipher Name: DEFAULT
        Description: Predefined Cipher Alias
 Done
```

To unbind an SSL certificate-key pair from a virtual server by using the command line interface

If you try to unbind a certificate-key pair from a virtual server by using the `unbind ssl certKey <certkeyName>` command, an error message appears because the syntax of the command has changed. At the command prompt, type the following command:

unbind ssl vserver <vServerName> -certkeyName <string>

Example

```
unbind ssl vserver vssl -certkeyName sslckey
```

Parameters for binding the certificate-key pair to the virtual server

vServerName

The name of the SSL based virtual server to which you are binding the certificate-key pair.

certkeyName

The name of the certificate-key pair that you are binding to the virtual server. This certificate-key pair should already be configured on the NetScaler.

To bind an SSL certificate-key pair to a virtual server by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. Select the virtual server to bind the certificate key to, and then click Open.
3. In the Configure Virtual Server (SSL Offload) dialog box, click SSL Settings.
4. In the Available pane, select a certificate.
5. Click Add to add the certificate as a server certificate. To add as an SNI certificate, in the Add drop-down list select As SNI. To add as a CA certificate, in the Add drop-down list select As CA.
6. Click OK. The certificate pair is bound to the virtual server.

Configuring an SSL Virtual Server for Secure Hosting of Multiple Sites

Virtual hosting is used by Web servers to host more than one domain name with the same IP address. The NetScaler supports hosting of multiple secure domains by offloading SSL processing from the Web servers using transparent SSL services or vserver-based SSL offloading. However, when multiple Web sites are hosted on the same virtual server, the SSL handshake is completed before the expected host name is sent to the virtual server. As a result, the NetScaler cannot determine which certificate to present to the client after a connection is established. This problem is resolved by enabling Server Name Indication (SNI) on the virtual server. SNI is a Transport Layer Security (TLS) extension used by the client to provide the host name during handshake initiation. Based on the information provided by the client in the SNI extension, the NetScaler presents the corresponding certificate to the client.

A wildcard SSL Certificate helps enable SSL encryption on multiple subdomains if the domains are controlled by the same organization and share the same second-level domain name. For example, a wildcard certificate issued to a sports network using the common name "*.sports.net" can be used to secure domains, such as "login.sports.net" and "help.sports.net" but not "login.ftp.sports.net."

Note: On a NetScaler appliance, SNI is not supported with a Subject Alternative Name (SAN) extension certificate.

You can bind multiple server certificates to a single SSL virtual server or transparent service using the -SNICert option. These certificates are issued by the virtual server or service if SNI is enabled on the virtual server or service. You can enable SNI at any time.

To bind multiple server certificates to a single SSL virtual server by using the command line interface

At the command prompt, type the following commands to configure SNI and verify the configuration:

- set ssl vserver <vServerName>@ [-SNIEnable (ENABLED | DISABLED)]
- bind ssl vserver <vServerName>@ -certkeyName <string> -SNICert
- show ssl vserver <vServerName>

  To bind multiple server certificates to a transparent service by using the NetScaler command line, replace vserver with service and vservername with servicename in the above commands.

  Note: The SSL service should be created with -clearTextPort 80 option.

Example

```
set ssl vserver v1 -snI ENABLED
bind ssl vserver v1 -certkeyName serverabc -SNICert
sh ssl vserver v1
Advanced SSL configuration for VServer v1:
…
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: ENABLED
SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
1)CertKey Name: servercert Server Certificate
1)CertKey Name: abccert Server Certificate for SNI
2)CertKey Name: xyzcert Server Certificate for SNI
3)CertKey Name: startcert Server Certificate for SNI
1)Cipher Name: DEFAULT
Description: Predefined Cipher Alias
Done
```

Parameters for configuring SNI

vServerName

The name of the SSL virtual server on which SNI is enabled.

serviceName

The name of the SSL transparent service on which SNI is enabled.

SNIEnable

State of the Server Name Indication (SNI) feature on the virtual server and service-based offload. SNI helps to enable SSL encryption on multiple domains on a single virtual server or service if the domains are controlled by the same organization and share the same second-level domain name. For example, *.sports.net can be used to secure domains such as login.sports.net and help.sports.net. Possible values: ENABLED, DISABLED Default: DISABLED

SNICert

Name of the certificate-key pair to bind for use in SNI processing.

To bind multiple server certificates to a single SSL virtual server or transparent SSL service by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers or Services.
2. In the details pane, select the virtual server or service on which SNI is to be enabled, and then click Open.
3. In the Configure Virtual Server (SSL Offload) or Configure Service dialog box, on the SSL Settings tab, click SSL Parameters.
4. In the Configure SSL Params dialog box, under Others, select the SNI Enable check box.
5. Click OK.
6. On the SSL Settings tab, under Available, select a certificate.
7. In the Add drop-down list select As SNI.
8. To add more certificates, repeat step 7.
9. Under Configured, verify that the certificate is added as a server certificate for SNI.
10. Click OK.

Managing Certificates

An SSL certificate, which is an integral part of any SSL transaction, is a digital data form (X509) that identifies a company (domain) or an individual. The certificate has a public key component that is visible to any client that wants to initiate a secure transaction with the server. The corresponding private key, which resides securely on the NetScaler appliance, is used to complete asymmetric key (or public key) encryption and decryption.

You can obtain an SSL certificate and key in either of the following ways:

- From an authorized certificate authority (CA), such as VeriSign
- By generating a new SSL certificate and key on the NetScaler appliance

Alternately, you can use an existing SSL certificate on the appliance.

Caution: Citrix recommends that you use certificates obtained from authorized CAs, such as VeriSign, for all your SSL transactions. Certificates generated on the NetScaler appliance should be used for testing purposes only, not in any live deployment.

Obtaining a Certificate from a Certificate Authority

A certificate authority (CA) is an entity that issues digital certificates for use in public key cryptography. Certificates issued or signed by a CA are automatically trusted by applications, such as web browsers, that conduct SSL transactions. These applications maintain a list of the CAs that they trust. If the certificate being used for the secure transaction is signed by any of the trusted CAs, the application proceeds with the transaction.

To obtain an SSL certificate from an authorized CA, you must create a private key, use that key to create a certificate signing request (CSR), and submit the CSR to the CA. The only special characters allowed in the file names are underscore and dot.

Creating a Private Key

The private key is the most important part of a digital certificate. By definition, this key is not to be shared with anyone and should be kept securely on the NetScaler appliance. Any data encrypted with the public key can be decrypted only by using the private key.

The appliance supports two encryption algorithms, RSA and DSA, for creating private keys. You can submit either type of private key to the CA. The certificate that you receive from the CA is valid only with the private key that was used to create the CSR, and the key is required for adding the certificate to the NetScaler.

Caution: Be sure to limit access to your private key. Anyone who has access to your private key can decrypt your SSL data.

All SSL certificates and keys are stored in the /nsconfig/ssl folder on the appliance. For added security, you can use the Data Encryption Standard (DES) or triple DES (3DES) algorithm to encrypt the private key stored on the appliance.

Note: The length of the SSL key name allowed includes the length of the absolute path name if the path is included in the key name.

To create an RSA private key by using the command line interface

At the command prompt, type the following command:

create ssl rsakey <keyFile> <bits> [-exponent (3 | F4)] [-keyform (DER | PEM)]

Example

> create ssl rsakey Key-RSA-1 1024 -exponent F4 -keyform PEM

To create a DSA private key by using the command line interface

At the command prompt, type the following command:

create ssl dsakey <keyfile> <bits> [-keyform (DER | PEM)]

Example

> create ssl dsakey Key-DSA-1 1024 -keyform PEM

To create an RSA private key by using the configuration utility

1. In the navigation pane, click SSL.
2. In the details pane, under SSL Keys, click Create RSA Key.
3. In the Create RSA Key dialog box, configure the RSA key parameters. For a description of a parameter, hover the mouse cursor over the corresponding field.
4. Click Create, and then click Close.

To create an DSA private key by using the configuration utility

1. In the navigation pane, click SSL.
2. In the details pane, under SSL Keys, click Create DSA Key.
3. In the Create DSA Key dialog box, configure the DSA key parameters. For a description of a parameter, hover the mouse cursor over the corresponding field.
4. Click Create, and then click Close.

Creating a Certificate Signing Request

The certificate signing request (CSR) is a collection of information, including the domain name, other important company details, and the private key to be used to create the certificate. To avoid generating an invalid certificate, make sure that the details you provide are accurate.

To create a certificate signing request by using the command line interface

At the command prompt, type the following command:

create ssl certreq <reqFile> -keyFile <input_filename> | -fipsKeyName <string>) [-keyForm (DER | PEM) {-PEMPassPhrase }] -countryName <string> -stateName <string> -organizationName <string> [-organizationUnitName <string>] [-localityName <string>] [-commonName <string>] [-emailAddress <string>] {-challengePassword } [-companyName <string>]

Example

> create ssl certreq csreq1 -keyfile ramp -keyform PEM -countryName IN -stateName Karnataka -localityNam

To create a certificate signing request by using the configuration utility

1. In the navigation pane, click SSL.
2. In the details pane, under SSL Certificates, click Create CSR (Certificate Signing Request).
3. In the Create CSR (Certificate Signing Request) dialog box, configure the CSR parameters. For a description of a parameter, hover the mouse cursor over the corresponding field.
4. Click Create, and then click Close. The certificate signing request you created is saved on the appliance in the specified location.

Submitting the CSR to the CA

Most CAs accept certificate submissions by email. The CA will return a valid certificate to the email address from which you submit the CSR.

Importing Existing Certificates and Keys

If you want to use certificates and keys that you already have on other secure servers or applications in your network, you can export them, and then import them to the NetScaler appliance. You might have to convert exported certificates and keys before you can import them to the NetScaler appliance.

For the details of how to export certificates from secure servers or applications in your network, see the documentation of the server or application from which you want to export.

Note: For installation on the NetScaler appliance, key and certificate names cannot contain spaces or special characters other than those supported by the UNIX file system. Follow the appropriate naming convention when you save the exported key and certificate.

A certificate and private key pair is commonly sent in the PKCS#12 format. The NetScaler supports PEM and DER formats for certificates and keys. To convert PKCS#12 to PEM or DER, or PEM or DER to PKCS#12, see Converting the Format of SSL Certificates for Import or Export.

The NetScaler appliance does not support PEM keys in PKCS#8 format. However, you can convert these keys to a supported format by using the OpenSSL interface, which you can access from the NetScaler command line or the configuration utility. Before you convert the key, you need to verify that the private key is in PKCS#8 format. Keys in PKCS#8 format typically start with the following text:

-----BEGIN ENCRYPTED PRIVATE KEY-----

leuSSZQZKgrgUQ==

-----END ENCRYPTED PRIVATE KEY-----

To open the OpenSSL interface from the command line interface

1. Open an SSH connection to the appliance by using an SSH client, such as PuTTY.
2. Log on to the appliance by using the administrator credentials.
3. At the command prompt, type shell.
4. At the shell prompt type `openssl`.

To open the ssl interface from the configuration utility

1. In the navigation pane, click SSL.
2. In the details pane, under Tools, click OpenSSL interface.

To convert a non-supported PKCS#8 key format to an encrypted supported key format by using the OpenSSL interface

At the OpenSSL prompt, type one of the following commands, depending on whether the non-supported key format is of type rsa or dsa:

- `rsa-` in <PKCS#8 Key Filename> -des3 -out <encrypted Key Filename>
- `dsa` -in <PKCS#8 Key Filename> -des3 -out <encrypted Key Filename>

To convert a non-supported PKCS#8 key format to an unencrypted key format by using the OpenSSL interface

At the OpenSSL prompt, type the following commands, depending on whether the non-supported key format is of type rsa or dsa:

- `rsa` -in <PKCS#8 Key Filename> -out <unencrypted Key Filename>
- `dsa` -in <PKCS#8 Key Filename> -out <unencrypted Key Filename>

Parameters for converting an unsupported key format to a supported key format

<PKCS#8 Key Filename>

The input file name of the incompatible PKCS#8 private key.

<encrypted Key Filename>

The output file name of the compatible encrypted private key in PEM format.

<unencrypted Key Filename>

The output file name of the compatible unencrypted private key in PEM format.

Generating a Self-Signed Certificate

The NetScaler appliance has a built in CA tools suite that you can use to create self-signed certificates for testing purposes.

Caution: Because these certificates are signed by the NetScaler itself, not by an actual CA, you should not use them in a production environment. If you attempt to use a self-signed certificate in a production environment, users will receive a "certificate invalid" warning each time the virtual server is accessed.

The NetScaler supports creation of the following types of certificates

- Root-CA certificates
- Intermediate-CA certificates
- End-user certificates
  - server certificates
  - client certificates

Before generating a certificate, create a private key and use that to create a certificate signing request (CSR) on the appliance. Then, instead of sending the CSR out to a CA, use the NetScaler CA Tools to generate a certificate.

For details on how to create a private key and a CSR, see Obtaining a Certificate from a Certificate Authority.

To create a certificate by using a wizard

1. In the navigation pane, click SSL.
2. In the details pane, under Getting Started, select the wizard for the type of certificate that you want to create.
3. Follow the instructions on the screen.

To create a Root-CA certificate by using the command line interface

At the command prompt, type the following command:

create ssl cert <certFile> <reqFile> <certType> [-keyFile <input_filename>] [-keyform (**DER** | **PEM**)] [-days <positive_integer>]

Example

```
> create ssl cert certi1 csreq1 ROOT_CERT -keyFile
rsa1 -keyForm PEM -days 365
  Done
```

To create an Intermediate-CA certificate or end-user certificate by using the command line interface

At the command prompt, type the following command:

create ssl cert <certFile> <reqFile> <certType> [-keyFile <input_filename>] [-keyform (**DER** | **PEM**)] [-days <positive_integer>] [-certForm (**DER** | **PEM**)] [-CAcert <input_filename>] [-CAcertForm (**DER** | **PEM**)] [-CAkey <input_filename>] [-CAkeyForm (**DER** | **PEM**)] [-CAserial <output_filename>]

Example

```
> create ssl cert certsy csr1 INTM_CERT -CAcert cert1
-CAkey rsakey1 -CAserial 23
Done
```

Parameters for creating a self-signed certificate

certFile (Certificate File Name)

The name of the generated certificate file. The newly created certificate file is stored by default in the /nsconfig/ssl/ directory.

reqFile (Certificate Request File Name)

The certificate signing request (CSR) file that is used to generate the certificate.

certType (Certificate Type)

The type of the certificate being created. You can create a Root Certificate, an Intermediate Certificate, a Client Certificate or a Server Certificate. Select one of the following options

- **ROOT_CERT:** Specifies a self-signed Root-CA certificate. If you choose this setting, you must also set the -keyFile parameter. The generated Root-CA certificate can be used for signing end-user certificates (Client/Server) or to create Intermediate-CA certificates.
- **INTM_CERT:** Specifies an Intermediate-CA certificate.

- **CLNT_CERT:** Specifies an end-user client certificate that is used for client authentication.
- **SRVR_CERT:** Specifies an SSL server certificate to be used on physical SSL servers for an SSL backend-encryption setup.

The parameters CAcert, CAkey, and CAserial, are mandatory when creating an intermediate, client, or server certificate.

keyFile (Key File Name)

The private key used to create the certificate. You can either use an existing RSA or DSA key that you own or create a new private key on the NetScaler. This file is required only when creating a self-signed Root-CA certificate. The key file is stored in the /nsconfig/ssl directory by default.

Note: If the input key specified is an encrypted key, the user will be prompted to enter the PEM pass-phrase that was used for encrypting the key.

keyform (Key Format)

The file format in which the private key is stored. Possible values: PEM, DER. Default: PEM.

days (Validity Period)

The number of days for which the created certificate will be valid. The certificate is valid from the time and day (system time) of its creation to the number of days specified in this field. Minimum value: 1. Maximum value: 3650. Default: 365 days.

certForm (Certificate Format)

The format in which to save the certificate. Possible values: PEM, DER. Default: PEM.

CAcert (CA Certificate File Name)

The CA certificate file that will issue and sign the Intermediate-CA certificate or the end-user certificates (Client/Server). The default input path for the CA certificate file is /nsconfig/ssl/.

CAcertForm (CA Certificate File Format)

The format in which to store the CA certificate. Possible values: PEM, DER. Default: PEM.

CAkey (CA Key File Name)

The private key associated with the CA certificate that is used to sign the Intermediate-CA certificate or the end-user certificates (Client/Server). If the CA key file is password protected, the user will be prompted to enter the pass-phrase used when encrypting the key.

CAkeyForm (CA Key File Format)

The file format in which the private key of the CA certificate is stored. Possible values: PEM, DER. Default: PEM.

CAserial (CA Serial Number File)

The serial number file maintained for the CA certificate. The file will contain the serial number of the next certificate to be issued/signed by the CA (-CAcert). If the specified file does not exist, a new file will be created. The NetScaler stores the newly generated file in the /nsconfig/ssl/ directory by default.

Note: Specify the proper path of the existing serial file. Otherwise, a new serial file will be created, and that can change the certificate serial numbers assigned by the CA certificate to each of the certificate it signs.

To create a Root-CA certificate by using the configuration utility

1. In the navigation pane, click SSL.
2. Under SSL Certificates, click Create Certificate.
3. In the Create Certificate dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating a self-signed certificate” as shown:
   - Certificate File Name*
   - Certificate Format
   - Certificate Type
   - Certificate Request File Name*
   - Key File Name*
   - Key Format
   - PEM Passphrase (For Encrypted Key)—If the key is encrypted, you are prompted to enter the password at run-time on the CLI.
   - Validity Period (Number of Days)

   * A required parameter

   Note: Instead of typing the file name, you can use the browse button to launch the NetScaler file browser and select the file.
4. Click Create, and then click Close. The Root-CA certificate you created is saved on the NetScaler.

To create an Intermediate-CA certificate or end-user certificate by using the configuration utility

1. In the navigation pane, click SSL.
2. Under SSL Certificates, click Create Certificate.
3. In the Create Certificate dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating a self-signed certificate” as shown:
   - Certificate File Name*
   - Certificate Format
   - Certificate Type
   - Certificate Request File Name*
   - PEM Passphrase (For Encrypted Key)—If the key is encrypted, you are prompted to enter the password at run-time on the CLI.
   - Validity Period (Number of Days)
   - CA Certificate File Name*
   - CA Certificate File Format
   - CA Key File Name*—CAkey
   - CA Key File Format
   - PEM Passphrase (For Encrypted CA Key)
   - CA Serial Number File*

   * A required parameter

   Note: Instead of typing the file name, you can use the browse button to launch the NetScaler file browser and select the file.
4. Click Create, and then click Close. The Intermediate-CA certificate you created is saved on the NetScaler.

Generating a Diffie-Hellman (DH) Key

The Diffie-Hellman (DH) key exchange is a way for two parties involved in an SSL transaction that have no prior knowledge of each other to agree upon a shared secret over an insecure channel. This secret can then be converted into cryptographic keying material for mainly symmetric key cipher algorithms that require such a key exchange.

This feature is disabled by default and should be specifically configured to support ciphers that use DH as the key exchange algorithm.

Note: Generating a 2048-bit DH key may take a long time (up to 30 minutes).

To generate a DH key by using the command line interface

At the command prompt, type the following command:

create ssl dhparam <dhFile> [<bits>] [-gen (2 | 5)]

Example

create ssl dhparam Key-DH-1 512 -gen 2

Parameters for creating a DH Key

dhFile (DH File Name)

The name of the DH key that is created. The DH key is stored in the /nsconfig/ssl directory on the appliance by default.

bits (DH Parameter Size)

The size in bits of the DH key being generated.

gen (DH Generator)

The random number required for generating the DH key. This is required as part of the DH key generation algorithm. Possible Values: 2, 5. Default Value: 2

To generate a DH key by using the configuration utility

1. In the navigation pane, click SSL.
2. Under Tools, click Create Diffe-Hellman (DH) Key.
3. In the Create DH Param dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for creating a DH Key” as shown:
   - DH File Name (with path)*
   - DH Parameter Size (Bits)*
   - DH Generator

   * A required parameter
4. Click OK.

Adding a Group of SSL Certificates

If the server certificate is issued by an intermediate CA that is not recognized by standard web browsers as a trusted CA, the CA certificate(s) must be sent to the client with the server's own certificate. Otherwise, the browser terminates the SSL session because it fails to authenticate the server certificate.

There are two ways to add the server and intermediate certificates:

- Create a certificate set that contains the chain of certificates.
- Create a chain of certificates manually by adding and linking the certificates individually.

Adding and Linking a Certificate Set

Note: This feature is not supported on the NetScaler FIPS platform.

Instead of adding and linking individual certificates, you can now group a server certificate and up to nine intermediate certificates in a single file, and then specify the file's name when adding a certificate-key pair. Before you do so, make sure that the following prerequisites are met.

- The certificates in the file are in the following order:
  - Server certificate (should be the first certificate in the file)
  - Optionally, a server key
  - Intermediate certificate 1 (ic1)
  - Intermediate certificate 2 (ic2)
  - Intermediate certificate 3 (ic3), and so on

    Note: Intermediate certificate files are created for each intermediate certificate with the name "<certificatebundlename>.pem_ic<*n*>" where n is between 1 and 9. For example, bundle.pem_ic1, where bundle is the name of the certificate set and ic1 is the first intermediate certificate in the set.
- Bundle option is selected.
- No more than nine intermediate certificates are present in the file.

The file is parsed and the server certificate, intermediate certificates, and server key (if present) are identified. First, the server certificate and key are added. Then, the intermediate certificates are added, in the order in which they were added to the file, and linked accordingly.

An error is reported if any of the following conditions exist:

- A certificate file for one of the intermediate certificates already exists on the appliance.
- The key is placed before the server certificate in the file.
- An intermediate certificate is placed before the server certificate.
- Intermediate certificates are not in placed in the file in the same order as they are created.
- No certificates are present in the file.
- A certificate is not in the proper PEM format.
- The number of intermediate certificates in the file exceeds nine.

To add a certificate set by using the command line interface

At the command prompt, type the following commands to create a certificate set and verify the configuration:

1. add ssl certKey <certkeyName> -cert <string> -key <string> -bundle (YES | NO)
2. show ssl certKey
3. show ssl certlink

Example

In the following example, the certificate set (bundle.pem) contains the following files:

- server certificate (bundle) linked to bundle_ic1
- First intermediate certificate (bundle_ic1) linked to bundle_ic2
- Second intermediate certificate (bundle_ic2) linked to bundle_ic3
- Third intermediate certificate (bundle_ic3)

```
> add ssl certKey bundle -cert bundle.pem -key bundle.pem -bundle yes

> show ssl certkey

1) Name: bundle
Cert Path: /nsconfig/ssl/bundle.pem
Format: PEM
Status: Valid, Days to expiration:10415
Certificate Expiry Monitor: DISABLED

2) Name: bundle_ic1
Cert Path: /nsconfig/ssl/bundle.pem_ic1
Format: PEM
Status: Valid, Days to expiration:10415
Certificate Expiry Monitor: DISABLED

3) Name: bundle_ic2
Cert Path: /nsconfig/ssl/bundle.pem_ic2
Format: PEM
Status: Valid, Days to expiration:10415
Certificate Expiry Monitor: DISABLED

4) Name: bundle_ic3
Cert Path: /nsconfig/ssl/bundle.pem_ic3
Format: PEM
Status: Valid, Days to expiration:10415
Certificate Expiry Monitor: DISABLED
Done
```

```
> show ssl certlink

1) Cert Name: bundle CA Cert Name: bundle_ic1
2) Cert Name: bundle_ic1 CA Cert Name: bundle_ic2
3) Cert Name: bundle_ic2 CA Cert Name: bundle_ic3
Done
```

Parameters for adding a certificate

certKeyName

Name of the certificate-key pair that is linked to its issuer's certificate-key pair in the chain.

cert

File name and path for the X509 certificate file. The certificate file should be present on the NetScaler appliance's hard disk drive or solid-state drive. The default input path for the certificate file is /nsconfig/ssl/.

key

File name and path for the private-key file. The private-key file should be present on the hard disk drive or solid-state drive. The default input path for the key file is /nsconfig/ssl/.

bundle

Parse the certificate chain as a single file after linking the server certificate to its issuer's certificate within the file.

To add a certificate set by using the configuration utility

1. In the navigation pane, expand SSL, and then click Certificates.
2. In the SSL Certificates pane, click Install.
3. In the Install Certificate dialog box, type the details, such as the certificate and key file name, and then select Certificate Bundle.
4. Click Install, and then click Close.

Creating a Chain of Certificates

Instead of using a set of certificates (a single file), you can create a chain of certificates. The chain links the server certificate to its issuer (the intermediate CA). For this approach to work, the intermediate CA certificate file must already be installed on the NetScaler appliance, and one of the certificates in the chain must be trusted by the client application. For example, link Cert-Intermediate-A to Cert-Intermediate-B, where Cert-Intermediate-B is linked to Cert-Intermediate-C, which is a certificate trusted by the client application.

Note: The NetScaler supports sending a maximum of 10 certificates in the chain of certificates sent to the client (one server certificate and nine CA certificates).

To create a certificate chain by using the command line interface

At the command prompt, type the following commands to create a certificate chain and verify the configuration. (Repeat the first command for each new link in the chain.)

- link ssl certkey <certKeyName> <linkCertKeyName>
- show ssl certlink

Example

```
> link ssl certkey siteAcertkey CAcertkey
 Done

> show ssl certlink

linked certificate:
      1) Cert Name: siteAcertkey CA Cert Name: CAcertkey
 Done
```

Parameters for creating a certificate chain

certKeyName

The name of the certificate-key pair that is linked to its issuer's certificate-key pair in the chain.

linkCertKeyName

The name of the issuer of the certificate that is being linked to.

The two certificate-key pairs are linked only if the certificate specified in the certKeyName parameter is issued by the Certificate-Authority specified in the linkCertKeyName parameter.

To create a certificate chain by using the configuration utility

1. In the navigation pane, expand SSL, and then click Certificates.
2. Select the server certificate you want to link, and then click Link.
3. In Link Server Certificate(s), select CA Certificate Name to be linked to.
4. Click OK. The server certificate is now linked to the intermediate certificate.

Generating a Server Test Certificate

The NetScaler appliance allows you to create a test certificate for server authentication by using a GUI wizard in the configuration utility. A server certificate is used to authenticate and identify a server in an SSL handshake. A server certificate is generally issued by a trusted CA and is sent out by the server to a client who uses it to authenticate the server.

For issuing a server test certificate, the appliance operates as a CA. This certificate can be bound to an SSL virtual server for authentication in an SSL handshake with a client. This certificate is for testing purposes only. It should not be used in a production environment.

You can install the server test certificate on any virtual server that uses the SSL or the SSL_TCP protocol.

To generate a server test certificate by using the configuration utility

1. In the navigation pane, click SSL.
2. Under SSL Certificates, click Create and install a Server Test Certificate.
3. In the Create and install a Server Test Certificate dialog box, specify values for the following parameters:
   - Certificate File Name—name of the server test certificate
   - Fully Qualified Domain Name—the domain for which you want to secure the connection
   - Country—the name of the country or region
4. Click OK.

Modifying and Monitoring Certificates and Keys

To avoid downtime when replacing a certificate-key pair, you can update an existing certificate. If you want to replace a certificate with a certificate that was issued to a different domain, you must disable domain checks before updating the certificate.

To receive notifications about certificates due to expire, you can enable the expiry monitor.

Updating an Existing Server Certificate

When you remove or unbind a certificate from a configured SSL virtual server, or an SSL service, the virtual server or service becomes inactive until a new valid certificate is bound to it. To avoid downtime, you can use the update feature to replace a certificate-key pair that is bound to an SSL virtual server or an SSL service, without first unbinding the existing certificate.

To update an existing certificate-key pair by using the command line interface

At the command prompt, type the following commands to update an existing certificate-key pair and verify the configuration:

- update ssl certkey <certkeyName> -cert <string> -key <string>
- show ssl certKey <certkeyName>

Example

```
> update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem
      -key /nsconfig/ssl/pkey.pem
  Done

> show ssl certkey siteAcertkey
Name: siteAcertkey       Status: Valid
      Version: 3
      Serial Number: 02
      Signature Algorithm: md5WithRSAEncryption
      Issuer: /C=US/ST=CA/L=Santa Clara/O=siteA/OU=Tech
      Validity
          Not Before: Nov 11 14:58:18 2001 GMT
          Not After: Aug 7 14:58:18 2004 GMT
      Subject: /C=US/ST-CA/L=San Jose/O=CA/OU=Security
```

```
    Public Key Algorithm: rsaEncryption
    Public Key size: 1024
Done
```

Parameters for updating an existing certificate-key pair

certkeyName

The name of the certificate key pair that you want to update with a new certificate or a new key, or both.

cert

The name of the new certificate with which you want to update the certificate key pair.

key

The name of the private with which key you want to update an existing certificate key pair.

Note: The new certificate and key should be in local storage on the NetScaler. If the files are not stored in the default /nsconfig/ssl folder, provide the absolute path to the files.

To update an existing certificate-key pair by using the configuration utility

1. In the navigation pane, expand SSL, and then click Certificates.
2. Select the certificate you want to update, and then click Update.
3. Use the Browse button next to the Certificate File name and the Key File name and select the new certificate and key files respectively.
4. If the key in encrypted, in the Password text box, type the password used to encrypt the key.
5. Click OK. In SSL Certificates pane, select the certificate that you just updated and verify that the settings displayed at the bottom of the screen are correct.

Disabling Domain Checks

When an SSL certificate is replaced on the NetScaler, the domain name mentioned on the new certificate should match the domain name of the certificate being replaced. For example, if you have a certificate issued to abc.com, and you are updating it with a certificate issued to def.com, the certificate update fails.

However, if you want the server that has been hosting a particular domain to now host a new domain, you can disable the domain check before updating its certificate.

To disable the domain check for a certificate by using the command line interface

At the command prompt, type the following commands to disable the domain check and verify the configuration:

- update ssl certKey <certkeyName> -noDomainCheck
- show ssl certKey <certkeyName>

Example

```
> update ssl certKey sv -noDomainCheck
 Done
> show ssl certkey sv
   Name: sv
   Cert Path: /nsconfig/ssl/complete/server/server_rsa_512.pem
   Key Path: /nsconfig/ssl/complete/server/server_rsa_512.ky
   Format: PEM
   Status: Valid,   Days to expiration:9349
   Certificate Expiry Monitor: DISABLED
 Done
```

To disable the domain check for a certificate by using the configuration utility

1. In the navigation pane, expand SSL, and then click Certificates.
2. Select the certificate you want to update, and then click Update.
3. Select No Domain Check, and then click OK. The domain check for the certificate is now disabled.

Enabling the Expiry Monitor

An SSL certificate is valid for a specific period of time. A typical deployment includes multiple virtual servers that process SSL transactions, and the certificates bound to them can expire at different times. An expiry monitor configured on the NetScaler appliance creates entries in the appliance's syslog and nsaudit logs when a certificate configured on the appliance is due to expire.

If you want to create SNMP alerts for certificate expiration, you must configure them separately.

For information about monitoring on the NetScaler appliance, see Monitors.

To enable an expiry monitor for a certificate by using the command line interface

At the command prompt, type the following commands to enable an expiry monitor for a certificate and verify the configuration:

- set ssl certKey <certkeyName> [-expiryMonitor (ENABLED | DISABLED) [-notificationPeriod <positive_integer>]]
- show ssl certKey <certkeyName>

Example

```
> set ssl certKey sv -expiryMonitor ENABLED –notificationPeriod 60
  Done

> show ssl certkey sv
Name: sv
   Cert Path: /nsconfig/ssl/complete/server/server_rsa_512.pem
   Key Path: /nsconfig/ssl/complete/server/server_rsa_512.ky
   Format: PEM
   Status: Valid,   Days to expiration:9349
   Certificate Expiry Monitor: ENABLED
   Expiry Notification period: 60 days
  Done
```

Parameters for enabling an expiry monitor

certKeyName

The name of the certificate-key pair whose expiry monitor is configured.

expiryMonitor

Enable or disable the expiry monitor for the certificate-key pair

notificationPeriod

The number of days in advance that the NetScaler should warn about a certificate that is about to expire.

To enable an expiry monitor for a certificate by using the configuration utility

1. In the navigation pane, expand SSL, and then click Certificates.
2. Select the certificate you want to update, and then click Update.
3. Select the Enable option.
4. In the Notification Period text box, type the required notification period value.

   Note: The notification period parameter can be set to any value between 10 and 100 days and the default notification period is 30 days.
5. Click OK. In the SSL Certificates pane, select the certificate that you just configured and verify that the settings displayed at the bottom of the screen are correct.

Using Global Site Certificates

A global site certificate is a special-purpose server certificate whose key length is greater than 128 bits. A global site certificate consists of a server certificate and an accompanying intermediate-CA certificate. You must import the global site certificate and its key from the server to the NetScaler appliance.

How Global Site Certificates Work

Export versions of browsers use 40-bit encryption to initiate connections to SSL Web-servers. The server responds to connection requests by sending its certificate. The client and server then decide on an encryption strength based on the server certificate type:

- If the server certificate is a normal certificate and not a global site certificate, the export client and server complete the SSL handshake and uses 40-bit encryption for data transfer.
- If the server certificate is a global site certificate (and if the export client feature is supported by the browser), the export client automatically upgrades to 128-bit encryption for data transfer.

If the server certificate is a global site certificate, the server sends its certificate, along with the accompanying intermediate-CA certificate. The browser first validates the intermediate-CA certificate by using one of the Root-CA certificates that are normally included in web browsers. Upon successful validation of the intermediate-CA certificate, the browser uses the intermediate-CA certificate to validate the server certificate. Once the server is successfully validated, the browser renegotiates (upgrades) the SSL connection to 128-bit encryption.

With Microsoft's Server Gated Cryptography (SGC), if the Microsoft IIS server is configured with an SGC certificate, export clients that receive the certificate renegotiate to use128-bit encryption.

Importing a Global Site Certificate

To import a global site certificate, first export the certificate and server key from the Web server. Global site certificates are generally exported in some binary format, therefore, before importing the global site certificate, convert the certificate and key to the PEM format.

To import a global site certificate

1. Using a text editor, copy the server certificate and the accompanying intermediate-CA certificate into two separate files.

   The individual PEM encoded certificate will begin with the header ----- BEGIN CERTIFICATE----- and end with the trailer -----END CERTIFICATE-----.

2. Use an SFTP client to transfer the server certificate, intermediate-CA certificate, and server-key to the NetScaler.

3. Use the following OpenSSL command to identify the server certificate and intermediate-CA certificate from the two separate files.

   Note: You can launch the OpenSSL interface from the configuration utility. In the navigation pane, click SSL. In the details pane, under Tools, click Open SSL interface.

   > openssl x509 -in >path of the CA cert file< ▫text

   X509v3 Basic Constraints:
   CA:TRUE
   X509v3 Key Usage:
   Certificate Sign, CRL Sign
   Netscape Cert Type:
   SSL CA, S/MIME CA

   > openssl x509 -in >path of the server certificate file< -text

   X509v3 Basic Constraints:
   CA:FALSE
   Netscape Cert Type:
   SSL Server

4. At the FreeBSD shell prompt, enter the following command:

   ```
   openssl x509 -in cert.pem -text | more
   ```

   Where **cert.pem** is one of the two certificate files.

   Read the **Subject** field in the command output. For example,

   Subject: C=US, ST=Oregon, L=Portland,
   O=mycompany, Inc., OU=IT, CN=www.mycompany.com

   If the CN field in the Subject matches the domain-name of your Web site, then this is the server certificate and the other certificate is the accompanying intermediate-CA certificate.

5. Use the server certificate and its private key) to create a certificate key pair on the NetScaler. For details on creating a certificate-key pair on the NetScaler, see Adding a Certificate Key Pair.

6. Add the intermediate-CA certificate on the NetScaler. Use the server certificate you created in step 4 to sign this intermediate certificate. For details on creating an Intermediate-CA certificate on the NetScaler, see Generating a Self-Signed Certificate.

Converting the Format of SSL Certificates for Import or Export

A NetScaler appliance supports the PEM and DER formats for SSL certificates. Other applications, such as client browsers and some external secure servers, require various public key cryptography standard (PKCS) formats. The NetScaler can convert the PKCS#12 format (the personal information exchange syntax standard) to PEM or DER format for importing a certificate to the appliance, and can convert PEM or DER to PKCS#12 for exporting a certificate. For additional security, conversion of a file for import can include encryption of the private key with the DES or DES3 algorithm.

Note: If you use the configuration utility to import a PKCS#12 certificate, and the password contains a dollar sign ($), backquote (`), or escape (\) character, the import may fail. If it does, the `ERROR: Invalid password` message appears. If you must use a special character in the password, be sure to prefix it with an escape character (\) unless all imports are performed by using the NetScaler command line.

To convert the format of a certificate by using the command line interface

At the command prompt, type the following command:

Convert ssl pkcs12 <outfile> [-import [-pkcs12File <inputFilename>] [-des | -des3] [-export [-certFile <inputFilename>] [-keyFile <inputFilename>]] During the operation, you are prompted to enter an import password or an export password. For an encrypted file, you are also prompted to enter a passphrase.

Example

convert ssl pkcs12 Cert-Import-1.pem -import -pkcs12File Cert-Import-1.pfx -des

convert ssl pkcs12 Cert-Client-1.pfx -export -certFile Cert-Client-1 -keyFile Key-Client-1

Parameters for Converting the Format of a Certificate

outfile (Output File Name)

The name of, and optionally the path to, the output file that contains the certificate and the private key after converting from PKCS#12 to PEM format. The default output path for the file is /nsconfig/ssl/. This is a required parameter. Maximum value: 63 characters.

pkcsFile (PKCS12 File Name)

The name of, and optionally the path to, the PKCS#12 file. If the **-import** option is specified, this is the input file name that contains the certificate and the private key in PKCS#12 format. If the **-export** option is specified, this is the output file name that contains the certificate and the private key after converting from PEM to PKCS#12 format. The default input path is /nsconfig/ssl/. Maximum value: 63 characters.

import

Convert the certificate and private key from PKCS#12 format to PEM format.

des (Encoding Format)

Encrypt the private key with DES in CBC mode during the import operation.

des3 (Encoding Format)

Encrypt the private key with DES in EDE CBC mode (168 bit key) during the import operation.

export

Convert the certificate and private key from PEM format to PKCS#12 format.

certFile (Certificate File Name)

The certificate file to be converted from PEM to PKCS#12 format.

keyFile (Key File Name)

The private key file to be converted from PEM to PKCS#12 format.

Password (Import Password/Export Password)

In the CLI, you are prompted to enter the password during the import or export operation. In the configuration utility, you have to enter the password before the operation begins. The import password is the password that was entered while creating the PKCS#12 file. For the export password, you enter a new password that will be required when installing the certificate into the client browser.

PEMPassPhrase (PEM Passphrase)

In the CLI, you are prompted to enter the passphrase during the import operation if you select des or des3 for encrypting your private key or during the export operation if you select des or des3 for encrypting your PKCS#12 file. In the configuration utility, you have to enter the passphrase before the import operation if you select an encoding format, or before the export operation if you want to encrypt your PKCS#12 file.

To convert the format of a certificate by using the configuration utility

1. In the navigation pane, click SSL.
2. Under Tools, do one of the following
   - To convert a PKCS#12 certificate and key to PEM format, click Import PKCS#12.
   - To convert a certificate and key from PEM to PKCS#12 format, click Export PKCS#12.
3. In the Import PKCS12 or Export PKCS12 dialog box, set the following parameters:
   - Output File Name*
   - PKCS12 File Name*
   - Certificate File Name*
   - Key File Name*
   - Import Password*
   - Export Password*
   - Encoding Format
   - PEM Passphrase

   * A required parameter
4. Click OK.

Managing Certificate Revocation Lists

A certificate issued by a CA typically remains valid until its expiration date. However, in some circumstances, the CA may revoke the issued certificate before the expiration date (for example, when an owner's private key is compromised, a company's or individual's name changes, or the association between the subject and the CA changes).

A Certificate Revocation List (CRL) identifies invalid certificates by serial number and issuer.

Certificate authorities issue CRLs on a regular basis. You can configure the NetScaler appliance to use a CRL to block client requests that present invalid certificates.

If you already have a CRL file from a CA, add that to the NetScaler. You can configure refresh options. You can also configure the NetScaler to sync the CRL file automatically at a specified interval, from either a web location or an LDAP location. The NetScaler supports CRLs in either the PEM or the DER file format. Be sure to specify the file format of the CRL file being added to the NetScaler.

If you have used the NetScaler as a CA to create certificates that are used in SSL deployments, you can also create a CRL to revoke a particular certificate. This feature can be used, for example, to ensure that self-signed certificates that are created on the NetScaler are not used either in a production environment or beyond a particular date.

Note:

By default, CRLs are stored in the /var/netscaler/ssl directory on the NetScaler appliance.

Creating a CRL on the NetScaler

Since you can use the NetScaler appliance to act as a certificate authority and create self-signed certificates, you can also revoke certificates that you have created and certificates whose CA certificate you own.

The appliance must revoke invalid certificates before creating a CRL for those certificates. The appliance stores the serial numbers of revoked certificates in an index file and updates the file each time it revokes a certificate. The index file is automatically created the first time a certificate is revoked.

To revoke a certificate or create a CRL by using the command line interface

At the command prompt, type the following command:

create ssl crl <CAcertFile> <CAkeyFile> <indexFile> (-revoke <input_filename> | -genCRL <output_filename>)

Example

create ssl crl Cert-CA-1 Key-CA-1 File-Index-1 -revoke Invalid-1

create ssl crl Cert-CA-1 Key-CA-1 File-Index-1 -genCRL CRL-1

Parameters for revoking a certificate or creating a CRL on the NetScaler

CAcertFile (CA Certificate File Name)

Name of and, optionally, path to the CA certificate file. /nsconfig/ssl/ is the default path. Maximum value: 63.

CAkeyFile (CA Key File Name)

Name of and, optionally, path to the CA key file. /nsconfig/ssl/ is the default path. Maximum value: 63.

indexFile (Index File Name)

Name of and, optionally, path to the file containing the serial numbers of all the certificates that are revoked. Revoked certificates are appended to the file. /nsconfig/ssl/ is the default path. Maximum value: 63.

revoke (Revoke Certificate)

Name of and, optionally, path to the certificate to be revoked. /nsconfig/ssl/ is the default path. You can revoke a certificate only if the certificate and key of the CA that issued the certificate is available on the NetScaler. Maximum value: 63.

genCRL (Generate CRL)

Name of and, optionally, path to the CRL file to be generated. The list of certificates that have been revoked is obtained from the index file. /nsconfig/ssl/ is the default path. Maximum value: 63.

To revoke a certificate or create a CRL by using the configuration utility

1. In the navigation pane, click SSL.
2. Under Getting Started, click CRL Management.
3. In the CRL Management dialog box, set the following parameters:
   - CA Certificate File Name*
   - CA Key File Name*
   - CA Key File Password—the password used to encrypt the key file. On the CLI, you are prompted to enter this password at run time.
   - Index File Name*
   - Choose Operation-
     - Revoke Certificate
     - Generate CRL

   * A required parameter
4. Click Create, and then click Close.

Adding an Existing CRL to the NetScaler

Before you configure the CRL on the NetScaler appliance, make sure that the CRL file is stored locally on the NetScaler. In the case of an HA setup, the CRL file must be present on both NetScaler appliances, and the directory path to the file must be the same on both appliances.

To add a CRL on the NetScaler by using the command line

At the command prompt, type the following commands to add a CRL on the NetScaler and verify the configuration:

- add ssl crl <crlName> <crlPath> [-inform (DER | PEM)]
- show ssl crl [<crlName>]

Example

```
> add ssl crl crl-one /var/netscaler/ssl/CRL-one -inform PEM
 Done
> show ssl crl crl-one
        Name: crl-one   Status: Valid,  Days to expiration: 29
        CRL Path: /var/netscaler/ssl/CRL-one
        Format: PEM     CAcert: samplecertkey
        Refresh: DISABLED
        Version: 1
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:  C=US,ST=California,L=Santa Clara,O=NetScaler Inc.,OU=SSL Acceleration,CN=www.ns.com/ema
        Last_update:Jun 15 10:53:53 2010 GMT
        Next_update:Jul 15 10:53:53 2010 GMT

1)      Serial Number: 00
        Revocation Date:Jun 15 10:51:16 2010 GMT
 Done
```

Parameters for adding an existing CRL

crlName (CRL Name)

The name of the CRL being added on the NetScaler.

crlPath (CRL File)

The name of the CRL file being added on the NetScaler. The NetScaler looks for the CRL file in the /var/netscaler/ssl directory by default.

inform (Format)

The format in which the CRL file is stored on the NetScaler appliance. Possible Values: PEM, DER. Default: PEM.

CAcert (CA Certificate)

The corresponding CA certificate that has issued the CRL. This is the System object identifying the CA certificate that is loaded in System. Maximum Length: 31

Note: The CA certificate should be installed before loading the CRL.

To add a CRL on the NetScaler by using the configuration utility

1. In the navigation pane, expand SSL, and then click CRL.
2. In the details pane, click Add.
3. In the Add CRL dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for adding an existing CRL” as shown:
   - CRL Name*
   - CRL File*
   - Format
   - CA Certificate

   * A required parameter
4. Click Create, and then click Close. In the CRL pane, select the CRL that you just configured and verify that the settings displayed at the bottom of the screen are correct.

Configuring CRL Refresh Parameters

A CRL is generated and published by a Certificate Authority periodically or, in some cases, immediately after a particular certificate is revoked. Citrix recommends that you update CRLs on the NetScaler appliance regularly, for protection against clients trying to connect with certificates that are not valid.

The NetScaler can refresh CRLs from a web location or an LDAP directory. When you specify refresh parameters and a web location or an LDAP server, the CRL does not have to be present on the local hard disk drive at the time you execute the command. The first refresh stores a copy on the local hard disk drive, in the path specified by the CRL File parameter. The default path for storing the CRL is /var/netscaler/ssl.

Note: In release 10.0 and later, the method for refreshing a CRL is not included by default. You must explicitly specify an HTTP or LDAP method. If you are upgrading from an earlier release to release 10.0 or later, you must add a method and run the command again.

To configure CRL autorefresh by using the command line

At the command prompt, type the following commands to configure CRL auto refresh and verify the configuration the following commands to configure CRL auto refresh and verify the configuration:

- set ssl crl <crlName> [-refresh (ENABLED | DISABLED)] [-CAcert <string>] [-url <URL | -server <ip_addr|ipv6_addr>] [-method HTTP | (LDAP [-baseDN <string>] [-bindDN <string>] [-scope (Base | One)] [-password <string>] [-binary (YES | NO)])] [-port <port>] [-interval <interval>]
- show ssl crl [<crlName>]

Example

Set CRL crl1 -refresh enabled -method ldap -inform DER -CAcert ca1 -server 10.102.192.192 -port 389 -scope

set ssl crl crl1 -refresh enabled -method http -cacert ca1 -port 80 -time 00:10 -url http://10.102.192.192/cr

> sh crl

1) Name: crl1 Status: Valid, Days to expiration: 355
CRL Path: /var/netscaler/ssl/crl1
Format: PEM CAcert: ca1
Refresh: ENABLED Method: HTTP
URL: http://10.102.192.192/crl/ca1.crl Port:80
Refresh Time: 00:10
Last Update: Successful, Date:Tue Jul 6 14:38:13 2010

Done

CRL Refresh Parameters

crlName

The name of the CRL being refreshed on the NetScaler.

refresh

Enable or disable CRL auto refresh.

CAcert

The certificate of the CA that has issued the CRL. This CA certificate must be installed on the appliance. The NetScaler can update CRLs only from CAs whose certificates are installed on it.

url (URL)

The URL for the web location from which the CRL should be fetched.

server (Server IP)

The IP address of the LDAP server from which the CRL should be fetched.

method (Method)

Protocol in which to obtain the CRL refresh from a web server (HTTP) or an LDAP server. Possible Values: HTTP, LDAP. Default: LDAP.

baseDN (Base DN)

The baseDN attribute used by LDAP search to query for the **certificateRevocationList** attribute.

Note: Citrix recommends using the baseDN attribute instead of the Issuer-Name from the CA certificate to search for the CRL in the LDAP server. The Issuer-Name field may not exactly match the LDAP directory structure's DN.

bindDN (Bind DN)

The bindDN attribute to be used to access the CRL object in the LDAP repository. This is required if the access to the LDAP repository is restricted, that is, anonymous access is not allowed.

scope (Scope)

The extent of the search operation on the LDAP server. If the scope specified is Base, the search is at exactly the same level as the baseDN. If the scope specified is One, the search extends to one level below the baseDN.

password (Password)

The password used to access the CRL object in the LDAP repository. This is required if the access to the LDAP repository is restricted, that is, anonymous access is not allowed.

binary (Binary)

Set the LDAP based CRL retrieval mode to binary. Possible values: YES, NO. Default: NO.

port (Port)

The port number on which the LDAP or the HTTP server should be contacted.

interval (Interval)

The interval at which the CRL refresh should be carried out. For an instantaneous CRL refresh, specify the interval as NOW. Possible values: MONTHLY, DAILY, WEEKLY, NOW, NONE.

day (Day)

The day on which CRL refresh should be carried out. The option is not available if interval is set to DAILY.

time (Time)

The exact time in 24-hour format when the CRL refresh should be carried out.

To configure CRL autorefresh using LDAP or HTTP by using the configuration utility

1. In the navigation pane, expand SSL, and then click CRL.
2. Select the configured CRL for which you want to update refresh parameters, and then click Open.
3. Select the Enable CRL Auto Refresh option.
4. In the CRL Auto Refresh Parameters group, specify values for the following parameters, which correspond to parameters described in “CRL Refresh Parameters” as shown:
   - Method
   - Binary
   - Scope
   - Server IP
   - Port*
   - URL
   - Base DN*
   - Bind DN
   - Password
   - Interval
   - Day(s)
   - Time

   * A required parameter

   Note: If the new CRL has been refreshed in the external repository before its actual update time as specified by the LastUpdate field of the CRL, you should immediately refresh the CRL on the NetScaler.
5. Click Create. In the CRL pane, select the CRL that you just configured and verify that the settings displayed at the bottom of the screen are correct.

Synchronizing CRLs

The NetScaler appliance uses the most recently distributed CRL to prevent clients with revoked certificates from accessing secure resources.

If CRLs are updated often, the NetScaler needs an automated mechanism to fetch the latest CRLs from the repository. You can configure the NetScaler to update CRLs automatically at a specified refresh interval.

The NetScaler maintains an internal list of CRLs that need to be updated at regular intervals. At these specified intervals, the appliance scans the list for CRLs that need to be updated, connects to the remote LDAP server or HTTP server, retrieves the latest CRLs, and then updates the local CRL list with the new CRLs.

Note: If CRL check is set to mandatory when the CA certificate is bound to the virtual server, and the initial CRL refresh fails, all client-authentication connections with the same issuer as the CRL are rejected as REVOKED until the CRL is successfully refreshed.

You can specify the interval at which the CRL refresh should be carried out. You can also specify the exact time.

To synchronize CRL autorefresh by using the command line interface

At the command prompt, type the following command:

set ssl crl <crlName> [-interval <interval>] [-day <integer>] [-time <HH:MM>]

Example

```
set ssl crl CRL-1 -refresh ENABLE -interval
MONTHLY -days 10 -time 12:00
```

Parameters for synchronizing CRL refresh

interval (Interval)

The CRL refresh interval. Possible values: DAILY, WEEKLY, MONTHLY, NONE, NOW. Specify NONE to reset a previously set interval. Specify NOW for instantaneous refresh. See also day.

day (Day)

Behavior depends on the interval setting. If **-interval** is not set, **-day** specifies the CRL refresh interval as a number of days. If **-interval** is set to MONTHLY, **-day** specifies a day

of the month (1-30/31/28) If **-interval** is set to WEEKLY, **-day** specifies a day of the week, 1 to 7, where 1=Sunday and 7=Saturday. If **-interval** is DAILY, **-day** cannot be used.

time (Time)

The time of the day when the CRL should be refreshed. The time is specified in 24-hour HHMM format, where HH stands for Hours and MM stands for minutes.

To synchronize CRL refresh by using the configuration utility

1. In the navigation pane, expand SSL, and then click CRL.
2. Select the configured CRL for which you want to update refresh parameters, and then click Open.
3. Select the Enable CRL Auto Refresh option.
4. In the CRL Auto Refresh Parameters group, specify values for the following parameters, which correspond to parameters described in “Parameters for synchronizing CRL refresh” as shown:
   - Interval
   - Day(s)
   - Time
5. Click Create. In the CRL pane, select the CRL that you just configured and verify that the settings displayed at the bottom of the screen are correct.

Performing Client Authentication by using a Certificate Revocation List

If a certificate revocation list (CRL) is present on a NetScaler appliance, a CRL check is performed regardless of whether performing the CRL check is set to mandatory or optional.

The success or failure of a handshake depends on a combination of the following factors:

- Rule for CRL check
- Rule for client certificate check
- State of the CRL configured for the CA certificate

The following table lists the results of the possible combinations for a handshake involving a revoked certificate.

Table 1. Result of a Handshake with a Client Using a Revoked Certificate

Rule for CRL Check	Rule for Client Certificate Check	State of the CRL Configured for the CA certificate	Result of a Handshake with a Revoked Certificate
Optional	Optional	Missing	Success
Optional	Mandatory	Missing	Success
Optional	Mandatory	Present	Failure
Mandatory	Optional	Missing	Success
Mandatory	Mandatory	Missing	Failure
Mandatory	Optional	Present	Success
Mandatory	Mandatory	Present	Failure
Optional/Mandatory	Optional	Expired	Success
Optional/Mandatory	Mandatory	Expired	Failure

Note:

- The CRL check is optional by default. To change from optional to mandatory or vice-versa, you must first unbind the certificate from the SSL virtual server, and then bind it again after changing the option.
- In the output of the `sh ssl vserver` command, `OCSP check: optional` implies that a CRL check is also optional. The CRL check settings are displayed in the output of the `sh ssl vserver` command only if CRL check is set to mandatory. If CRL check is set to optional, the CRL check details do not appear.

To configure CRL check by using the command line interface

At the command prompt, type the following command:

bind ssl vserver <vServerName> -certkeyName <string> [(-CA -crlCheck (Mandatory | Optional))]

Example

```
bind ssl vs v1 -certkeyName ca -CA -crlCheck mandatory
sh ssl vserver
> sh ssl vs v1

Advanced SSL configuration for VServer v1:

DH: DISABLED
Ephemeral RSA: ENABLED Refresh Count: 0
Session Reuse: ENABLED Timeout: 120 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: ENABLED Client Cert Required: Mandatory
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: DISABLED
SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
Push Encryption Trigger: Always
Send Close-Notify: YES

1) CertKey Name: ca CA Certificate CRLCheck: Mandatory CA_Name Sent

1) Cipher Name: DEFAULT
Description: Predefined Cipher Alias
Done
```

Parameters for configuring a CRL check on the NetScaler

vServerName

Name of the SSL virtual server.

crlCheck

Rule to use for the CRL corresponding to the CA certificate during client authentication. Available settings function as follows:

- MANDATORY—Deny SSL clients if the CRL is missing or expired, or the Next Update date is in the past, or the CRL is incomplete.
- OPTIONAL—Allow SSL clients if the CRL is missing or expired, or the Next Update date is in the past, or the CRL is incomplete, but deny if the client certificate is revoked in the CRL.

To configure CRL check by using the configuration utility

1. In the navigation pane, expand SSL Offload, and theOpenn click Virtual Servers.
2. In the details pane, select a virtual server, and then click Open.
3. In the Configure Virtual Server (SSL Offload) dialog box, click SSL Settings.
4. In the Configured pane, in the **Check** drop-down list, select CRL Mandatory.
5. Click OK.

Monitoring Certificate Status with OCSP

Online Certificate Status Protocol (OCSP) is an Internet protocol that is used to determine the status of a client SSL certificate. NetScaler appliances support OCSP as defined in RFC 2560. OCSP offers significant advantages over certificate revocation lists (CRLs) in terms of timely information. Up-to-date revocation status of a client certificate is especially useful in transactions involving large sums of money and high-value stock trades. It also uses fewer system and network resources. NetScaler implementation of OCSP includes request batching and response caching.

NetScaler Implementation of OCSP

OCSP validation on a NetScaler appliance begins when the appliance receives a client certificate during an SSL handshake. To validate the certificate, the NetScaler creates an OCSP request and forwards it to the OCSP responder. To do so, the NetScaler uses a locally configured URL. The transaction is in a suspended state until the NetScaler evaluates the response from the server and determines whether to allow the transaction or reject it. If the response from the server is delayed beyond the configured time and no other responders are configured, the NetScaler will allow the transaction or display an error, depending on whether the OCSP check was set to optional or mandatory, respectively.

The NetScaler supports batching of OCSP requests and caching of OCSP responses to reduce the load on the OCSP responder and provide faster responses.

OCSP Request Batching

Each time the NetScaler receives a client certificate, it sends a request to the OCSP responder. To help avoid overloading the OCSP responder, the NetScaler can query the status of more than one client certificate in the same request. For this to work efficiently, a timeout needs to be defined so that processing of a single certificate is not inordinately delayed while waiting to form a batch.

OCSP Response Caching

Caching of responses received from the OCSP responder enables faster responses to the clients and reduces the load on the OCSP responder. Upon receiving the revocation status of a client certificate from the OCSP responder, the NetScaler caches the response locally for a predefined length of time. When a client certificate is received during an SSL handshake, the NetScaler first checks its local cache for an entry for this certificate. If an entry is found that is still valid (within the cache timeout limit), it is evaluated and the client certificate is accepted or rejected. If a certificate is not found, the NetScaler sends a request to the OCSP responder and stores the response in its local cache for a configured length of time.

Configuring an OCSP Responder

Configuring OCSP involves adding an OCSP responder, binding the OCSP responder to a certification authority (CA) certificate, and binding the certificate to an SSL virtual server. If you need to bind a different certificate to an OCSP responder that has already been configured, you need to first unbind the responder and then bind the responder to a different certificate.

To add an OCSP responder by using the command line interface

At the command prompt, type the following commands to configure OCSP and verify the configuration:

- add ssl ocspResponder <name> -url <URL> [-cache (ENABLED | DISABLED)[-cacheTimeout <positive_integer>]] [-batchingDepth <positive_integer>][-batchingDelay <positive_integer>] [-resptimeout <positive_integer>] [-responderCert <string> | -trustResponder] [-producedAtTimeSkew <positive_integer>][-signingCert <string>][-useNonce (YES | NO)][-insertClientCert(YES | NO)]
- bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <positive_integer>]
- bind ssl vserver <vServerName>@ (-certkeyName <string> (CA [-ocspCheck (Mandatory | Optional)]))
- show ssl ocspResponder [<name>]

Example

```
add ssl ocspResponder ocsp_responder1 -url "http:// www.myCA.org:80/ocsp/" -cache ENABLED -cacheTime
bind ssl certKey ca_cert -ocspResponder ocsp_responder1 -priority 1
bind ssl vserver vs1 -certkeyName ca_cert -CA -ocspCheck Mandatory

sh ocspResponder ocsp_responder1
1)Name: ocsp_responder1
URL: http://www.myCA.org:80/ocsp/, IP: 192.128.22.22
Caching: Enabled        Timeout: 30 minutes
Batching: 8 Timeout: 100 mS
HTTP Request Timeout: 100mS
Request Signing Certificate: sign_cert
Response Verification: Full, Certificate: responder_cert
ProducedAt Time Skew: 300 s
Nonce Extension: Enabled
 Client Cert Insertion: Enabled
Done
```

```
show certkey ca_cert
Name: ca_cert     Status: Valid,   Days to expiration:8907
Version: 3
…
1)  VServer name: vs1      CA Certificate
1)  OCSP Responder name: ocsp_responder1     Priority: 1
Done

sh ssl vs vs1
Advanced SSL configuration for VServer vs1:
DH: DISABLED
…
1) CertKey Name: ca_cert CA Certificate OCSPCheck: Mandatory
1) Cipher Name: DEFAULT
  Description: Predefined Cipher Alias
Done
```

To modify an OCSP responder by using the command line interface

You cannot modify the responder name. All other parameters can be changed using the set ssl ocspResponder command.

At the command prompt, type the following commands to set the parameters and verify the configuration:

- set ssl ocspResponder <name> [-url <URL>] [-cache (ENABLED | DISABLED)] [-cacheTimeout <positive_integer>] [-batchingDepth <positive_integer>] [-batchingDelay <positive_integer>] [-resptimeout <positive_integer>] [-responderCert <string> | -trustResponder][-producedAtTimeSkew <positive_integer>][-signingCert <string>] [-useNonce (YES | NO)]
- unbind ssl certKey [<certkeyName>] [-ocspResponder <string>]
- bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <positive_integer>]
- show ssl ocspResponder [<name>]

Parameters for configuring an OCSP Responder

name (Name)

The name of the OCSP responder.

url (URL)

The URL of the OCSP responder.

Maximum length: 128.

cache (Cache)

Enable/disable caching of OCSP.

Possible values: ENABLED, DISABLED. Default: DISABLED.

cacheTimeout (Time-out)

OCSP cache timeout, in minutes. If none is specified, the timeout provided in the OCSP response is used.

Range: 1–1440. Default: 60.

batchingDepth (Batching Depth)

Maximum number of client certificates to batch into one OCSP request. Value of 1 signifies that each request is queried independently. Range: 1–8. Default: 1.

batchingDelay (Batching Delay)

Time, in milliseconds, to wait to accumulate OCSP requests.

Range: 0–10000. Default: 1.

resptimeout (Request Time-out)

Time, in milliseconds, to wait for an OCSP response. This is a mandatory parameter. When this time elapses, an error message appears or the transaction is forwarded, depending on the settings on the virtual server. Includes batchingDelay time.

Range: 0–120000. Default: 2000.

responderCert (Certificate)

responderCert specifies the certificate used to validate OCSP responses. trustResponder specifies that responses will not be verified.

producedAtTimeSkew (Produced At Time Skew)

Specifies the time, in seconds, for which the NetScaler waits before considering the response as invalid. The response is considered invalid if the ProducedAt time stamp in the OCSP response exceeds or precedes the current NetScaler clock time by the amount of time specified. Range: 0–86400. Default: 300.

signingCert (Signing Certificate)

Certificate-key pair used to sign OCSP requests. If this parameter is not set, the requests are not signed. Maximum value: 32.

insertClientCert (Client Certificate Insertion)

Include the complete client certificate in the OCSP request. Possible values: YES, NO. Default: NO.

useNonce (Nonce)

Enables the OCSP nonce extension, which is designed to prevent replay attacks.

certKey

The name of the certificate-key pair to bind.

ocspResponder

The name of the OCSP responder to which the certificate-key pair is bound to.

priority

Priority of the OCSP responder.

Range: 0–64000.

sslvserver

The name of the SSL virtual server that the certificate key is bound to.

certkeyname

The name of the certificate.

CA

CA certificate.

ocspCheck

OCSP check is mandatory or optional.

Note: When both OCSP and CRL check are set to optional, OCSP check is used by default. However, if a usable OCSP responder is not available, CRL check is used.

To configure an OCSP responder by using the configuration utility

1. In the navigation pane, expand SSL, and then click OCSP Responder.
2. In the details pane, do one of the following:
   - To create a new responder, click Add.
   - To modify an existing responder, select the responder, and then click Open.
3. In the Create OCSP Responder or Configure OCSP Responder dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring an OCSP Responder" as shown:
   - Name*
   - URL*
   - Cache
   - Time-out
   - Batching—To enable batching of OCSP requests, select this check box.
   - Batching Depth
   - Batching Delay
   - Trust Responses—To disable signature checks by the OCSP responder, select this check box.
   - Certificate
   - Produced At Time Skew
   - Request Time-out
   - Signing Certificate
   - Nonce
   - Client Certificate Insertion

   * A required parameter
4. Click Create or OK, and then click Close.
5. In the OCSP Responder pane, click the responder that you just configured and verify that the settings displayed at the bottom of the screen are correct.
6. In the navigation pane, click Certificates.
7. In the details pane, select a certificate and click OCSP Bindings.

8. In the OCSP Binding Details for certificate:certkey dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring an OCSP Responder" as shown:

   - OCSP Responder Name—ocspResponder. If an OCSP responder is not already bound to the certificate-key pair, click Insert OCSP Responder and select a name from the OCSP Responder Name drop-down list.

   - Priority—priority
9. To bind a different certificate-key pair, click Unbind OCSP Responder, and then click Insert OCSP Responder and select a name from the OCSP Responder Name drop-down list. Verify that the settings displayed at the bottom of the screen are correct.
10. Click OK.
11. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
12. Select the virtual server to bind the certificate key to, and click Open.
13. In the Configure Virtual Server (SSL Offload) dialog box, click SSL Settings.
14. In the Available pane, select a certificate.
15. In the Add drop-down list select As CA.
16. To make OCSP check mandatory, in the Configured pane, in the Check drop-down list, select OCSP Mandatory.
17. Click OK.

Configuring Client Authentication

In a typical SSL transaction, the client that is connecting to a server over a secure connection checks the validity of the server by checking the server's certificate before initiating the SSL transaction. In some cases, however, you might want to configure the server to authenticate the client that is connecting to it.

With client authentication enabled on an SSL virtual server, the NetScaler appliance asks for the client certificate during the SSL handshake. The appliance checks the certificate presented by the client for normal constraints, such as the issuer signature and expiration date.

Note: For the NetScaler to verify issuer signatures, the certificate of the CA that issued the client certificate must be installed on the NetScaler and bound to the virtual server that the client is transacting with.

If the certificate is valid, the NetScaler allows the client to access all secure resources. But if the certificate is invalid, the NetScaler drops the client request during the SSL handshake.

The NetScaler verifies the client certificate by first forming a chain of certificates, starting with the client certificate and ending with the root CA certificate for the client (for example, VeriSign). The root CA certificate may contain one or more intermediate CA certificates (if the client certificate is not directly issued by the root CA).

Before you enable client authentication on the NetScaler, make sure that a valid client certificate is installed on the client. Then, enable client authentication for the virtual server that will handle the transactions. Finally, bind the certificate of the CA that issued the client certificate to the virtual server on the NetScaler.

Note: The NetScaler appliance supports a certificate-key pair size of 512 to 4096 bits. The certificate must be signed by using one of the following hash algorithms:

- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

A NetScaler virtual appliance supports certificates of up to the following sizes:

- 4096-bit server certificate on the virtual server
- 4096-bit client certificate on the service
- 4096-bit CA certificate

- 2048-bit certificate on the physical server
- 2048-bit client certificate (if client authentication is enabled on the virtual server)

Providing the Client Certificate

Before you configure client authentication, a valid client certificate must installed on the client. A client certificate includes details about the specific client system that will create secure sessions with the NetScaler appliance. Each client certificate is unique and should be used by only one client system.

Whether you obtain the client certificate from a CA, use an existing client certificate, or generate a client certificate on the NetScaler appliance, you must convert the certificate to the correct format. On the NetScaler, certificates are stored in either the PEM or DER format and must be converted to PKCS#12 format before they are installed on the client system. After converting the certificate and transferring it to the client, system, make sure that it is installed on that system and configured for the client application that will be part of the SSL transactions (for example, the web browser).

For instructions on how to convert a certificate from PEM or DER format to PKCS#12 format, see Converting SSL Certificates for Import or Export.

For instructions on how to generate a client certificate, see Generating Self-Signed Certificates.

Enabling Client-Certificate-Based Authentication

By default, client authentication is disabled on the NetScaler appliance, and all SSL transactions proceed without authenticating the client. You can configure client authentication to be either optional or mandatory as part of the SSL handshake.

If client authentication is optional, the NetScaler requests the client certificate but proceeds with the SSL transaction even if the client presents an invalid certificate. If client authentication is mandatory, the NetScaler terminates the SSL handshake if the SSL client does not provide a valid certificate.

Caution: Citrix recommends that you define proper access control policies before changing client-certificate-based authentication check to optional.

Note: Client authentication is configured for individual SSL virtual servers, not globally.

To enable client-certificate-based authentication by using the command line interface

At the command prompt, type the following commands to enable the client-certificate-based authentication and verify the configuration:

- set ssl vserver <vServerName> [-clientAuth (ENABLED | DISABLED)] [-clientCert (MANDATORY | OPTIONAL)]
- show ssl vserver <vServerName>

Example

```
> set ssl vserver vssl -clientAuth ENABLED -clientCert Mandatory
 Done
> show ssl vserver vssl

        Advanced SSL configuration for VServer vssl:
        DH: DISABLED
        Ephemeral RSA: ENABLED         Refresh Count: 0
        Session Reuse: ENABLED         Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: ENABLED    Client Cert Required: Mandatory
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED
```

1) CertKey Name: sslckey Server Certificate

1) Policy Name: client_cert_policy Priority: 0

1) Cipher Name: DEFAULT
Description: Predefined Cipher Alias
Done

Parameters for configuring client certificate-based authentication

vServerName

The name of the NetScaler virtual server through which the client will access a physical server.

clientAuth

Enable or disable client authentication. Possible values: ENABLED, DISABLED. Default: DISABLED.

clientCert

Type of client authentication. Possible values: MANDATORY, OPTIONAL.

To enable client-certificate-based authentication by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. Select the virtual server for which you want to configure client certificate-based authentication, and then click Open.
3. Click the SSL Settings tab, and then click SSL Parameters.
4. In the Others group, select the Client Authentication check box.
5. In Client Certificate, select Mandatory.

   Note: To configure optional client authentication in Client Certificate, click Optional.
6. Click OK, and in the Configure Virtual Server (SSL Offload) dialog box, click OK. The virtual server is now configured for client authentication.

Binding CA Certificates to the Virtual Server

A CA whose certificate is present on the NetScaler appliance must issue the client certificate used for client authentication. You must bind this certificate to the NetScaler virtual server that will carry out client authentication.

You must bind the CA certificate to the SSL virtual server in such a way that the NetScaler can form a complete certificate chain when it verifies the client certificate. Otherwise, certificate chain formation fails and the client is denied access even if its certificate is valid.

You can bind CA certificates to the SSL virtual server in any order. The NetScaler forms the proper order during client certificate verification.

For example, if the client presents a certificate issued by **CA_A**, where **CA_A** is an intermediate CA whose certificate is issued by **CA_B**, whose certificate is in turn issued by a trusted root CA, **Root_CA**, a chain of certificates that contain all three of these certificates must be bound to the virtual server on the NetScaler.

For instructions on binding one or more certificates to the virtual server, see Binding the Certificate-key Pair to the SSL Based Virtual Server.

For instructions on creating a chain of certificates, see Creating a Chain of Certificates.

Customizing the SSL Configuration

Once your basic SSL configuration is operational, you can customize some of the parameters that are specific to the certificates being used in SSL transactions. You can also enable and disable session reuse and client authentication, and you can configure redirect responses for cipher and SSLv2 protocol mismatches.

You can also customize SSL settings for two NetScaler appliances in a High Availability configuration, and you can synchronize settings, certificates and keys across those appliances.

These settings will depend on your network deployment and the type of clients you expect will connect to your servers.

Configuring Diffie-Hellman (DH) Parameters

If you are using ciphers on the NetScaler that require a DH key exchange to set up the SSL transaction, enable DH key exchange on the NetScaler and configure other settings based on your network.

To list the ciphers for which DH parameters must be set by using the NetScaler command line, type: `sh cipher DH`.

To list the ciphers for which DH parameters must be set by using the configuration utility, navigate to Traffic Management > SSL > Cipher Groups, and double-click DH.

For details on how to enable DH key exchange, see Generating a Diffie-Hellman (DH) Key.

To configure DH Parameters by using the command line interface

At the command prompt, type the following commands to configure DH parameters and verify the configuration:

- set ssl vserver <vserverName> -dh <Option> -dhCount <RefreshCountValue> -filepath <string>
- show ssl vserver <vServerName>

Example

```
> set ssl vserver vs-server -dh ENABLED  -dhFile /nsconfig/ssl/ns-server.cert -dhCount 1000
  Done
> show ssl vserver vs-server

        Advanced SSL configuration for VServer vs-server:
        DH: ENABLED
        Ephemeral RSA: ENABLED          Refresh Count: 1000
        Session Reuse: ENABLED          Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)      Cipher Name: DEFAULT
```

Description: Predefined Cipher Alias
Done

Parameters for configuring DH parameters

dh (Enable DH Param)

Enable or disable DH key exchange. Possible values: ENABLED, DISABLED. Default: DISABLED.

dhCount (Refresh Count)

The number of interactions, between the client and the NetScaler, after which the DH private-public pair is regenerated. A value of zero (0) specifies infinite use (no refresh). Possible values: 0, or a number greater than 500. Default: 0.

dhFile (File Path)

The absolute path and file name of the DH parameter file to be installed. The default path is /nsconfig/ssl.

To configure DH Parameters by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. Select the virtual server for which you want to customize SSL settings, and then click **Open**.
3. On the SSL Settings tab, click SSL Parameters.
4. In the Configure SSL Params dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring DH parameters” as shown:
   - Enable DH Param*
   - Refresh Count
   - File Path*

   * A required parameter
5. Click OK, and in the Configure Virtual Server (SSL Offload) dialog box, click OK. The DH parameters are now configured.

Configuring Ephemeral RSA

Ephemeral RSA allows export clients to communicate with the secure server even if the server certificate does not support export clients (1024-bit certificate). If you want to prevent export clients from accessing the secure web object and/or resource, you need to disable ephemeral RSA key exchange.

By default, this feature is enabled on the NetScaler appliance, with the refresh count set to zero (infinite use).

Note:

The ephemeral RSA key is automatically generated when you bind an export cipher to an SSL or TCP-based SSL virtual server or service. When you remove the export cipher, the eRSA key is not deleted but reused at a later date when another export cipher is bound to an SSL or TCP-based SSL virtual server or service. The eRSA key is deleted when the system restarts.

To configure Ephemeral RSA by using the command line interface

At the command prompt, type the following commands to configure ephemeral RSA and verify the configuration:

- set ssl vserver <vServerName> -eRSA (enabled | disabled) -eRSACount <positive_integer>
- show ssl vserver <vServerName>

Example

```
> set ssl vserver vs-server -eRSA ENABLED -eRSACount 1000
 Done
> show ssl vserver vs-server

        Advanced SSL configuration for VServer vs-server:
        DH: DISABLED
        Ephemeral RSA: ENABLED         Refresh Count: 1000
        Session Reuse: ENABLED         Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED
```

1) Cipher Name: DEFAULT
Description: Predefined Cipher Alias
Done

Parameters for configuring Ephemeral RSA

eRSA (Enable Ephemeral RSA)

The state of Ephemeral RSA key exchange support for the SSL virtual server.

Possible values: ENABLED, DISABLED

Default value: ENABLED

eRSACount (Refresh Count)

The refresh count for the re-generation of RSA public-key and private-key pair. Zero means infinite usage (no refresh)

Note:

The '-eRSA' argument must be enabled if this argument is specified.

Default value: 0

Minimum value: 0

Maximum value: 65534

To configure Ephemeral RSA by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. Select the virtual server for which you want to customize SSL settings, and then click Open.
3. On the SSL Settings tab, click SSL Parameters.
4. In the Configure SSL Params dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring Ephemera RSA” as shown:
   - Enable Ephemeral RSA*
   - Refresh Count*

   * A required parameter
5. Click OK, and in the Configure Virtual Server (SSL Offload) dialog box, click OK. The ephemeral RSA parameters are now configured.

Configuring Session Reuse

For SSL transactions, establishing the initial SSL handshake requires CPU-intensive public key encryption operations. Most handshake operations are associated with the exchange of the SSL session key (client key exchange message). When a client session is idle for some time and is then resumed, the SSL handshake is typically conducted all over again. With session reuse enabled, session key exchange is avoided for session resumption requests received from the client.

Session reuse is enabled on the NetScaler appliance by default. Enabling this feature reduces server load, improves response time, and increases the number of SSL transactions per second (TPS) that can be supported by the server.

To configure session reuse by using the command line interface

At the command prompt, type the following commands to configure session reuse and verify the configuration:

- set ssl vserver <vServerName> -sessReuse (ENABLED | DISABLED) -sessTimeout <positive_integer>
- show ssl vserver <vServerName>

Example

```
> set ssl vserver vs-ssl -sessreuse enabled -sesstimeout 600
 Done

> show ssl vserver vs-ssl

        Advanced SSL configuration for VServer vs-ssl:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 1000
        Session Reuse: ENABLED          Timeout: 600 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)      CertKey Name: Auth-Cert-1       Server Certificate

1)      Cipher Name: DEFAULT
        Description: Predefined Cipher Alias
```

Done

Parameters for configuring Session Reuse

sessReuse (Enable Session Reuse)

Enable or disable the Session Reuse feature on the NetScaler appliance. Possible values: ENABLED, DISABLED. Default: ENABLED.

sessTimeout (Time-out)

Time in seconds up to which the session should be kept active. Any session resumption request received after the time out period will require a fresh SSL handshake and establishment of a new SSL session.

To configure session reuse by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. Select the virtual server for which you want to customize SSL settings, and then click Open.
3. On the SSL Settings tab, click SSL Parameters.
4. In the Configure SSL Params dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring Session Reuse” as shown:
   - Enable Session Reuse*
   - Time-out

   * A required parameter
5. Click OK, and in the Configure Virtual Server (SSL Offload) dialog box, click OK.

Configuring Cipher Redirection

During the SSL handshake, the SSL client (usually a web browser) announces the suite of ciphers that it supports, in the configured order of cipher preference. From that list, the SSL server then selects a cipher that matches its own list of configured ciphers.

If the ciphers announced by the client do not match those configured on the SSL server, the SSL handshake fails, and the failure is announced by a cryptic error message displayed in the browser. These messages rarely mention the exact cause of the error.

With cipher redirection, you can configure an SSL virtual server to deliver accurate, meaningful error messages when an SSL handshake fails. When SSL handshake fails, the NetScaler appliance redirects the user to a previously configured URL or, if no URL is configured, displays an internally generated error page.

To configure cipher redirection by using the command line interface

At the command prompt, type the following commands to configure cipher redirection and verify the configuration:

- set ssl vserver <vServerName> -cipherRedirect < ENABLED | DISABLED> -cipherURL < URL>
- show ssl vserver <vServerName>

Example

```
> set ssl vserver vs-ssl -cipherRedirect ENABLED -cipherURL http://redirectURl
 Done
> show ssl vserver vs-ssl

        Advanced SSL configuration for VServer vs-ssl:
        DH: DISABLED
        Ephemeral RSA: ENABLED         Refresh Count: 1000
        Session Reuse: ENABLED         Timeout: 600 seconds
        Cipher Redirect: ENABLED       Redirect URL: http://redirectURl
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)      CertKey Name: Auth-Cert-1       Server Certificate

1)      Cipher Name: DEFAULT
```

Description: Predefined Cipher Alias
Done

Parameters for configuring Cipher Redirection

vServerName

The name of the SSL based virtual server that you are configuring cipher redirection for.

cipherRedirect (Enable Cipher Redirect)

Enable or disable redirection based on cipher mismatch between the client and the NetScaler. Possible values: ENABLED, DISABLED. Default: DISABLED.

cipherURL (Redirect URL)

The URL of the page to which the client must be redirected in case of a cipher mismatch. This is typically a page that has a clear explanation of the error or an alternate location that the transaction can continue from.

To configure cipher redirection by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. Select the virtual server for which you want to customize SSL settings, and then click Open.
3. On the SSL Settings tab, click SSL Parameters.
4. In the Configure SSL Params dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring cipher redirection” as shown:
   - Enable Cipher Redirect
   - Redirect URL
5. Click OK, and in the Configure Virtual Server (SSL Offload) dialog box, click OK. The NetScaler is now configured to redirect clients in case of a cipher suite mismatch.

Configuring SSLv2 Redirection

For an SSL transaction to be initiated, and for successful completion of the SSL handshake, the server and the client should agree on an SSL protocol that both of them support. If the SSL protocol version supported by the client is not acceptable to the server, the server does not go ahead with the transaction, and an error message is displayed.

You can configure the server to display a precise error message (user-configured or internally generated) advising the client on the next action to be taken. Configuring the server to display this message requires that you set up SSLv2 redirection.

To configure SSLv2 redirection by using the command line interface

At the command prompt, type the following commands to configure SSLv2 redirection and verify the configuration:

- set ssl vserver <vServerName> [-sslv2Redirect (ENABLED | DISABLED) [-sslv2URL <URL>]]
- show ssl vserver <vServerName>

Example

```
> set ssl vserver vs-ssl -sslv2Redirect ENABLED -sslv2URL http://sslv2URL
 Done
> show ssl vserver vs-ssl

        Advanced SSL configuration for VServer vs-ssl:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 1000
        Session Reuse: ENABLED          Timeout: 600 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: ENABLED Redirect URL: http://sslv2URL
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)      CertKey Name: Auth-Cert-1       Server Certificate

1)      Cipher Name: DEFAULT
        Description: Predefined Cipher Alias
 Done
```

Parameters for configuring SSLv2 redirection

vServerName

The name of the SSL based virtual server that you are configuring SSLv2 redirection for.

sslv2Redirect (Enable SSLv2 Redirect)

Enable or disable redirection based on the SSL protocol mismatch between the client and the NetScaler. Possible values: ENABLED, DISABLED. Default: DISABLED.

sslv2URL (SSLv2 URL)

The URL of the page to which the client must be redirected in case of a protocol mismatch. This is typically a page that has a clear explanation of the error, or an alternative location from which the transaction can continue.

To configure SSLv2 redirection by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. Select the virtual server for which you want to customize SSL settings, and then click Open.
3. On the SSL Settings tab, click SSL Parameters.
4. In the Configure SSL Params dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring SSLv2 redirection” as shown:
   - Enable SSLv2 Redirect
   - SSLv2 URL
5. Click OK, and in the Configure Virtual Server (SSL Offload) dialog box, click OK. The NetScaler is now configured to redirect clients that only support SSLv2 protocol.

Configuring SSL Protocol Settings

The NetScaler appliance supports the SSLv2, SSLv3, and TLSv1 protocols. Each of these can be set on the appliance as required by your deployment and the type of clients that will connect to the appliance.

To configure SSL protocol support by using the command line interface

At the command prompt, type the following commands to configure SSL protocol support and verify the configuration:

- set ssl vserver <vServerName> -ssl2 (ENABLED | DISABLED) -ssl3 (ENABLED | DISABLED) -tls1 (ENABLED | DISABLED) -tls11 (ENABLED | DISABLED) -tls12 (ENABLED | DISABLED)

- show ssl vserver <vServerName>

Example

```
> set ssl vserver vs-ssl -tls11 ENABLED -tls12 ENABLED
 Done
> sh ssl vs vs-ssl

                Advanced SSL configuration for VServer vs-ssl:
      DH: DISABLED
      Ephemeral RSA: ENABLED                    Refresh Count: 0
      Session Reuse: ENABLED                    Timeout: 120 seconds
      Cipher Redirect: DISABLED
      SSLv2 Redirect: DISABLED
      ClearText Port: 0
      Client Auth: DISABLED
      SSL Redirect: DISABLED
      Non FIPS Ciphers: DISABLED
      SNI: DISABLED
      SSLv2: DISABLED      SSLv3: ENABLED    TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2: ENABLED
      Push Encryption Trigger: Always
      Send Close-Notify: YES

      1 bound certificate:
1)     CertKey Name: mycert  Server Certificate

      1 configured cipher:
1)     Cipher Name: DEFAULT
      Description: Predefined Cipher Alias
Done
```

Parameters for configuring SSL protocol settings

vServerName

The name of the SSL based virtual server for which you are configuring SSL protocol settings.

tls1 (TLSv1)

Enable or disable support for the TLSv1 protocol on the NetScaler appliance. Possible values: ENABLED, DISABLED. Default: ENABLED.

tls11 (TLSv1.1)

Enable or disable support for the TLSv1.1 protocol on the NetScaler appliance. Possible values: ENABLED, DISABLED. Default: ENABLED.

tls12 (TLSv1.2)

Enable or disable support for the TLSv1.2 protocol on the NetScaler appliance. Possible values: ENABLED, DISABLED. Default: ENABLED.

ssl2 (SSLv2)

Enable or disable support for the SSLv2 protocol on the NetScaler appliance. Possible values: ENABLED, DISABLED. Default: DISABLED.

ssl3 (SSLv3)

Enable or disable support for the SSLv3 protocol on the NetScaler appliance. Possible values: ENABLED, DISABLED. Default: ENABLED.

To configure SSL protocol support by using the configuration Utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. Select the virtual server for which you want to customize SSL settings, and then click Open.
3. On the SSL Settings tab, click SSL Parameters.
4. In the Configure SSL Params dialog box, in the SSL Protocol group, select any of the following protocol options that you want to enable:
   - TLSv1.2
   - TLSv1.1
   - TLSv1
   - SSLv3
   - SSLv2
5. Click OK, and in the Configure Virtual Server (SSL Offload) dialog box, click OK.

Configuring Close-Notify

A close-notify is a secure message that indicates the end of SSL data transmission. A close-notify setting is required at the global level. This setting applies to all virtual servers, services, and service groups. For information about the global setting, see Configuring Advanced SSL Settings.

In addition to the global setting, you can set the close-notify parameter at the virtual server, service, or service group level. You therefore have the flexibility of setting the parameter for one entity and unsetting it for another entity. However, make sure that you set this parameter at the global level. Otherwise, the setting at the entity level does not apply.

To configure close-notify at the entity level by using the command line interface

At the command prompt, type any of the following commands to configure close-notify and verify the configuration:

1. To configure close-notify at the virtual server level, type:
   - set ssl vserver <vServerName> -sendCloseNotify (**YES** | **NO**)
   - show ssl vserver <vServerName>
2. To configure close-notify at the service level, type:
   - set ssl service <serviceName> -sendCloseNotify (**YES** | **NO**)
   - show ssl service <serviceName>
3. To configure close-notify at the service group level, type:
   - set ssl serviceGroup <serviceGroupName> -sendCloseNotify (**YES** | **NO**)
   - show ssl serviceGroup <serviceGroupName>

Example

```
> set ssl vserver sslvsvr -sendCloseNotify YES
 Done
```

To configure close-notify at the entity level by using the configuration utility

1. In the navigation pane, expand SSL Offload.
2. Click Virtual Servers or Services or Service Groups.
3. Select the virtual server, service, or service group for which you want to customize SSL settings, and then click Open.
4. On the SSL Settings tab, click SSL Parameter.
5. In the Configure SSL Params dialog box, select Send Close-Notify.
6. Click OK, and in the Configure Virtual Server (SSL Offload) dialog box, click OK.

Configuring Advanced SSL Settings

Advanced customization of your SSL configuration addresses specific issues. You can use the set ssl parameter command or the configuration utility to specify the following:

- Quantum size to be used for SSL transactions.
- CRL memory size.
- OCSP cache size.
- Deny SSL renegotiation.
- Set the PUSH flag for decrypted, encrypted, or all records.
- Drop requests if the client initiates the handshake for one domain and sends an HTTP request for another domain.
- Set the time after which encryption is triggered.

  Note: The time that you specify applies only if you use the set ssl vserver command or the configuration utility to set timer-based encryption.

To configure advanced SSL settings by using the command line interface

At the command prompt, type the following commands to configure advanced SSL settings and verify the configuration:

- set ssl parameter [-quantumSize <quantumSize>] [-crlMemorySizeMB <positive_integer>] [-strictCAChecks (YES | NO)] [-sslTriggerTimeout <positive_integer>] [-sendCloseNotify (YES | NO)] [-encryptTriggerPktCount <positive_integer>] [-denySSLReneg <denySSLReneg>] [-insertionEncoding (Unicode|UTF-8)] [-ocspCacheSize <positive_integer>][- pushFlag <positive_integer>] [- dropReqWithNoHostHeader (YES | NO)] [-pushEncTriggerTimeout <positive_integer>]
- show ssl parameter

Example

```
> set ssl parameter -quantumSize 8 -crlMemorySizeMB 256 -strictCAChecks no -sslt
iggerTimeout 100 -sendClosenotify no -encryptTriggerPktCount 45 -denySSLReneg no
-insertionEncoding unicode -ocspCacheSize 10 -pushFlag 3 -dropReqWithNoHostHeader YES  -pushEncTriggerT
 Done

> show ssl parameter
Advanced SSL Parameters
```

```
----------------------
      SSL quantum size:              8 kB
      Max CRL memory size:           256 MB
      Strict CA checks:              NO
      Encryption trigger timeout     100 mS
      Send Close-Notify              NO
      Encryption trigger packet count:       45
      Deny SSL Renegotiation         NO
      Subject/Issuer Name Insertion Format:   Unicode
      OCSP cache size:       10 MB
        Push flag:     0x3 (On every decrypted and encrypted record)
                       Strict Host Header check for SNI enabled SSL sessions:         YES
                        PUSH encryption trigger timeout 100 ms
 Done
```

Parameters for configuring advanced SSL settings

quantumSize (SSL quantum size (Kbytes))

SSL quantum size to be used for SSL transactions on the appliance.

Possible values: 4096, 8192, 16384. Default: 8192.

crlMemorySizeMB (Max CRL memory size (Mbytes))

Maximum memory size to be used for certificate revocation lists.

Minimum value: 10. Maximum value: 1024. Default: 256.

strictCAChecks (Strict CA checks)

Enable strict CA certificate checks on the appliance.

Possible values: YES, NO. Default: NO.

sslTriggerTimeout (Encryption trigger timeout (10 mS ticks))

Encryption trigger timeout value, in milliseconds.

Note: There may be a delay of up to 10 ms from the specified timeout value before the packet is pushed into the queue.

Minimum value: 1. Maximum value: 200. Default: 100.

sendCloseNotify (Send Close-Notify)

Enable sending an SSL Close-Notify message to the client at the end of a transaction.

Possible values: YES, NO. Default: YES.

encryptTriggerPktCount (Encryption trigger packet count)

Number of queued packets that force encryption to occur.

Minimum value: 10. Maximum value: 50. Default: 45.

denySSLReneg (Deny SSL Renegotiation)

Deny renegotiation in specified circumstances. Possible values:

NO—Allow SSL renegotiation.

FRONTEND_CLIENT—Deny secure and nonsecure SSL renegotiation initiated by the client.

FRONTEND_CLIENTSERVER—Deny secure and nonsecure SSL renegotiation initiated by the client and by the NetScaler (during policy-based clientAuth).

ALL—Deny secure and nonsecure SSL renegotiation for the above two cases and for server initiated renegotiation.

NONSECURE—Deny nonsecure SSL renegotiation, to address the vulnerability described in RFC 5746. This option is not supported on the MPX FIPS appliances.

Default: NO.

insertionEncoding (Encoding type)

Encoding method used to insert the subject or issuer's name in HTTP requests to backend servers.

Possible values: Unicode, UTF-8. Default: Unicode.

ocspCacheSize (OCSP cache size(Mbytes))

Size, per packet engine, in megabytes, of the OCSP cache. The actual maximum value for this value is clamped at 10% of packet engine memory. Maximum packet engine memory is 4GB. Therefore, if you have enough memory to give all packet engines 4GB of memory, the maximum value here would be approximately 410 MB.

Minimum value: 0. Maximum value: 512. Default: 10.

pushFlag (PUSH Flag Insertion)

Insert PUSH flag into decrypted, encrypted, or all records. If the PUSH flag is set to a value other than 0, the buffered records are forwarded on the basis of the value of the PUSH flag. Possible values:

0—Auto (PUSH flag is not set).

1—Insert PUSH flag into every decrypted record.

2—Insert PUSH flag into every encrypted record.

3—Insert PUSH flag into every decrypted and encrypted record.

Possible values: 0, 1, 2, 3. Default: 0.

dropReqWithNoHostHeader (Drop requests for SNI enabled SSL sessions if Host header is absent)

Host header check for SNI enabled sessions. If this check is enabled and the HTTP request does not contain the Host header for SNI enabled session, the request is dropped.

Possible values: YES, NO. Default: NO.

pushEncTriggerTimeout (PUSH encryption trigger timeout (msec))

Encryption trigger timeout value. The timeout value that is applied when timer option is specified in the set ssl vserver –pushEncTrigger command.

Minimum value: 1. Maximum value: 200. Default: 1.

To configure advanced SSL settings by using the configuration utility

1. In the navigation pane, click SSL.
2. In the details pane, under Settings, click Change advanced SSL settings.
3. In the Change advanced SSL settings dialog box, set the following parameters:
   - SSL quantum size (Kbytes)
   - Max CRL memory size (Mbytes)
   - Encryption trigger timeout (10 mS ticks)
   - Encryption trigger packet count
   - Deny SSL Renegotiation
   - OCSP cache size(Mbytes)
   - Encoding type
   - PUSH encryption trigger timeout (msec)
   - Strict CA checks
   - Send Close-Notify
   - PUSH Flag Insertion
   - Drop requests for SNI enabled SSL sessions if Host header is absent
4. Click OK. The parameters you selected are now enabled on the appliance.

PUSH Flag-Based Encryption Trigger Mechanism

The encryption trigger mechanism that is based on the PSH TCP flag now enables you to do the following:

- Merge consecutive packets in which the PSH flag is set into a single SSL record, or ignore the PSH flag.
- Perform timer-based encryption, in which the time-out value is set globally by using the set ssl parameter -pushEncTriggerTimeout <positive_integer> command.

To configure PUSH flag-based encryption by using the command line interface

At the command prompt, type the following commands to configure PUSH flag-based encryption and verify the configuration:

- set ssl vserver <vServerName> [-pushEncTrigger <pushEncTrigger>]
- show ssl vserver

Example

```
Advanced SSL configuration for VServer v1:
        DH: DISABLED
        Ephemeral RSA: ENABLED                  Refresh Count: 0
        Session Reuse: ENABLED                  Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        SSLv2: DISABLED         SSLv3: ENABLED          TLSv1: ENABLED
        Push Encryption Trigger: Always
```

Parameters for configuring PUSH flag-based encryption

pushEncTrigger

Trigger encryption based on the value of the PUSH flag.

Possible values:

- **Always.** Any PUSH packet triggers encryption.
- **Ignore.** Ignore PUSH packet for triggering encryption.
- **Merge.** For a consecutive sequence of PUSH packets, the last PUSH packet triggers encryption.
- **Timer.** PUSH packet triggering encryption is delayed by the time defined in the set ssl parameter command. Possible values: Always, Ignore, Merge, Timer. Default:

Always.

To configure PUSH flag-based encryption by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. Select the virtual server for which you want to customize PUSH-flag based encryption, and then click Open.
3. On the SSL Settings tab, click SSL Parameters.
4. In the Configure SSL Params dialog box, select a value for the PUSH Encryption Trigger parameter. For descriptions of the values, see “Parameters for configuring PSH flag-based encryption.”
5. Click OK and, in the Configure Virtual Server (SSL Offload) dialog box, again click OK. The PSH flag-based encryption trigger is now configured.

Synchronizing Configuration Files in a High Availability Setup

In a high availability (HA) set up, the primary NetScaler appliance in the HA pair automatically synchronizes with the secondary appliance in the pair. In the synchronization process, the secondary copies the primary's /nsconfig/ssl/ directory, which is the default location for storing the certificates and keys for SSL transactions. Synchronization occurs at one-minute intervals and every time a new file is added to the directory.

To synchronize files in a high availability setup by using the command line interface

At the command prompt, type the following command:

sync HA files [<Mode>]

Example

sync HA files SSL

Parameters for synchronizing files in a high availability set up

mode

The type of synchronization to be performed. The following options are available:

- **All.** Synchronizes all data.
- **Bookmarks.** Synchronizes all Access Gateway bookmarks.
- **SSL.** Synchronizes all the SSL certificates and keys that are defined on the NetScaler appliance.

To synchronize files in a high availability setup by using the configuration utility

1. In the navigation pane, click SSL.
2. In the details pane, under Tools, click Start file synchronization.
3. In the Start file synchronization dialog box, in the Mode drop-down list, select the appropriate type of synchronization (for example, SSL certificates and Keys), and then click OK.

Managing Server Authentication

Since the NetScaler appliance performs SSL offload and acceleration on behalf of a web server, the appliance does not usually authenticate the Web server's certificate. However, you can authenticate the server in deployments that require end-to-end SSL encryption.

In such a situation, the NetScaler becomes the SSL client, carries out a secure transaction with the SSL server, verifies that a CA whose certificate is bound to the SSL service has signed the server certificate, and checks the validity of the server certificate.

To authenticate the server, you must first enable server authentication and then bind the certificate of the CA that signed the server's certificate to the SSL service on the NetScaler. When binding the certificate, you must specify the bind as CA option.

To enable (or disable) server certificate authentication by using the command line interface

At the command prompt, type the following commands to enable server certificate authentication and verify the configuration:

- set ssl service <serviceName> -serverAuth (ENABLED | DISABLED)
- show ssl service <serviceName>

Example

```
> set ssl service ssl-service-1 -serverAuth ENABLED
 Done
> show ssl service ssl-service-1

      Advanced SSL configuration for Back-end SSL Service ssl-service-1:
      DH: DISABLED
      Ephemeral RSA: DISABLED
      Session Reuse: ENABLED        Timeout: 300 seconds
      Cipher Redirect: DISABLED
      SSLv2 Redirect: DISABLED
      Server Auth: ENABLED
      SSL Redirect: DISABLED
      Non FIPS Ciphers: DISABLED
      SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)     Cipher Name: ALL
       Description: Predefined Cipher Alias
 Done
```

Parameters for enabling or disabling server certificate authentication

serviceName

The name of the service for which you are configuring server certificate authentication.

serverAuth

Enable or disable server authentication. This is used when you configure end-to-end SSL encryption to verify the authenticity of the server.

To enable (or disable) server certificate authentication by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Services.
2. Select the service for which you want to enable server authentication, and then click Open.
3. In Configure Service dialog box, on the SSL Settings tab, click SSL Parameters.
4. In the Others group, select Server Authentication.
5. Click OK. Server authentication is now enabled for the service.

To bind the CA certificate to the service by using the command line interface

At the command prompt, type the following commands to bind the CA certificate to the service and verify the configuration:

- bind ssl service <serviceName> -certkeyName <string> -CA
- show ssl service <serviceName>

Example

```
> bind ssl service ssl-service-1 -certkeyName samplecertkey -CA
 Done
> show ssl service ssl-service-1

      Advanced SSL configuration for Back-end SSL Service ssl-service-1:
      DH: DISABLED
      Ephemeral RSA: DISABLED
      Session Reuse: ENABLED        Timeout: 300 seconds
      Cipher Redirect: DISABLED
```

```
        SSLv2 Redirect: DISABLED
        Server Auth: ENABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)      CertKey Name: samplecertkey     CA Certificate          CRLCheck: Optional

1)      Cipher Name: ALL
        Description: Predefined Cipher Alias
 Done
```

Parameters for managing server authentication

serviceName

The name of the service for which server authentication is configured.

certkeyName

The name of the certificate key pair that is bound to the SSL service.

CA

Specifies that the certificate-key pair being bound belongs to a Certificate Authority that has signed the server certificate.

Configuring User-Defined Cipher Groups on the NetScaler Appliance

A cipher group is a set of cipher suites that you bind to an SSL virtual server, service, or service group on the NetScaler appliance. A cipher suite comprises a protocol, a key exchange (Kx) algorithm, an authentication (Au) algorithm, an encryption (Enc) algorithm, and a message authentication code (Mac) algorithm. Your appliance ships with a predefined set of cipher groups. When you create a SSL service or SSL service group, the ALL cipher group is automatically bound to it. However, when you create an SSL virtual server or a transparent SSL service, the DEFAULT cipher group is automatically bound to it. In addition, you can create a user-defined cipher group and bind it to an SSL virtual server, service, or service group.

Note: If your MPX appliance does not have any licenses, then only the EXPORT cipher is bound to your SSL virtual server, service, or service group.

To create a user-defined cipher group, first you create a cipher group and then you bind ciphers or cipher groups to this group. If you specify a cipher alias or a cipher group, all the ciphers in the cipher alias or group are added to the user-defined cipher group. You can also add individual ciphers (cipher suites) to a user-defined group. However, you cannot modify a predefined cipher group. Before removing a cipher group, unbind all the cipher suites in the group.

If you bind a cipher group to an SSL virtual server, service, or service group, the ciphers are appended to the existing ciphers that are bound to the entity. To bind a specific cipher group to the entity, you must first unbind the ciphers or cipher group that is bound to the entity and then bind the specific cipher group. For example, to bind only the AES cipher group to an SSL service, you perform the following steps:

1. Unbind the default cipher group ALL that is bound by default to the service when the service is created.

   ```
   unbind ssl service <service name> -cipherName ALL
   ```

2. Bind the AES cipher group to the service

   ```
   bind ssl service <Service name> -cipherName AE
   ```

If you want to bind the cipher group DES in addition to AES, at the command prompt, type:

- `bind ssl service <service name> -cipherName DES`

Note: The free NetScaler virtual appliance supports only the DH cipher group.

To configure a user-defined cipher group by using the command line interface

At the command prompt, type the following commands to add a cipher group, or to add ciphers to a previously created group, and verify the settings:

- add ssl cipher <cipherGroupName>
- bind ssl cipher <cipherGroupName> -cipherName <string>
- show ssl cipher <cipherGroupName>

Example

```
 > add ssl cipher test
 Done
> bind ssl cipher test -cipherName SSLv2
 Done
> show ssl cipher test
1)      Cipher Name: SSL2-RC2-CBC-MD5
Description: SSLv2 Kx=RSA      Au=RSA  Enc=RC2(128)  Mac=MD5
2)      Cipher Name: SSL2-RC4-MD5
Description: SSLv2 Kx=RSA      Au=RSA  Enc=RC4(128)  Mac=MD5
3)      Cipher Name: SSL2-DES-CBC3-MD5
Description: SSLv2 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=MD5
4)      Cipher Name: SSL2-DES-CBC-MD5
Description: SSLv2 Kx=RSA      Au=RSA  Enc=DES(56)   Mac=MD5
5)      Cipher Name: SSL2-RC4-64-MD5
Description: SSLv2 Kx=RSA      Au=RSA  Enc=RC4(64)   Mac=MD5
6)      Cipher Name: SSL2-EXP-RC4-MD5
Description: SSLv2 Kx=RSA(512) Au=RSA  Enc=RC4(40)   Mac=MD5  Export
7)      Cipher Name: SSL2-EXP-RC2-CBC-MD5
Description: SSLv2 Kx=RSA(512) Au=RSA  Enc=RC2(40)   Mac=MD5  Export
 Done
```

To unbind ciphers from a cipher group by using the command line interface

At the command prompt, type the following commands to unbind ciphers from a user-defined cipher group, and verify the settings:

- show ssl cipher <cipherGroupName>
- unbind ssl cipher <cipherGroupName> -cipherName <string>
- show ssl cipher <cipherGroupName>

Example

```
> show ssl cipher test
1) Cipher Name: SSL2-RC2-CBC-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
2) Cipher Name: SSL2-RC4-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
3) Cipher Name: SSL2-DES-CBC3-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5
4) Cipher Name: SSL2-DES-CBC-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5
5) Cipher Name: SSL2-RC4-64-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=RC4(64) Mac=MD5
6) Cipher Name: SSL2-EXP-RC4-MD5
Description: SSLv2 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 Export
7) Cipher Name: SSL2-EXP-RC2-CBC-MD5
Description: SSLv2 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 Export
Done

> unbind ssl cipher test -cipherName SSL2-RC2-CBC-MD5

> show ssl cipher test
1) Cipher Name: SSL2-RC4-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
2) Cipher Name: SSL2-DES-CBC3-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5
3) Cipher Name: SSL2-DES-CBC-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5
4) Cipher Name: SSL2-RC4-64-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=RC4(64) Mac=MD5
5) Cipher Name: SSL2-EXP-RC4-MD5
Description: SSLv2 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 Export
6) Cipher Name: SSL2-EXP-RC2-CBC-MD5
Description: SSLv2 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 Export
Done
```

To remove a cipher group by using the command line interface

Note: You cannot remove a built-in cipher group. Before removing a user-defined cipher group, make sure that the cipher group is empty.

At the command prompt, type the following commands to remove a user-defined cipher group, and verify the configuration:

- rm ssl cipher <userDefCipherGroupName> [<cipherName> ...]
- show ssl cipher <cipherGroupName>

Example

```
> rm ssl cipher test
Done

> sh ssl cipher test
ERROR: No such resource [cipherGroupName, test]
```

Parameters for configuring a user-defined cipher group

userDefCipherGroupName (Cipher Group Name)

The name of the user-defined cipher group. If the cipher group does not exist on the appliance, a new group with the specified name is created, and the ciphers are added to this group. If a group identified by userDefCipherGroupName already exists, the ciphers are added to it. This is a required parameter. Maximum Length: 39 characters.

cipherName (Available/Configured Cipher Groups/Ciphers)

The individual cipher name(s), a user-defined cipher group, or a predefined (built-in) cipher alias to be added to or removed from the user-defined cipher group. This is a required parameter. Maximum Length: 39 characters.

To configure a user-defined cipher group by using the configuration utility

1. In the navigation pane, expand SSL, and then click Cipher Groups.
2. In the details pane, do one of the following:
   - To create a new cipher group, click Add.
   - To modify an existing cipher group, select the cipher group, and then click Open.
3. If creating a new cipher group, in the Create Cipher Group dialog box, in the Cipher Group Name box, type a name for the new cipher group.
4. In the Create Cipher Group or View Cipher Group dialog box, do any or all of the following:
   - Select a cipher group or alias in the Available Cipher Groups list and click Add to move the group to the Configured Cipher Groups list.
   - Select a cipher group or alias in the Available Cipher Groups list, then select ciphers from the Available Ciphers list, and then click Add to move the selected ciphers to the Configured Ciphers list.
   - To move a cipher group or cipher from the Configured list to the Available list, select the group or cipher and click Remove.
5. Click Create, and then click Close. If you created a new cipher group, it appears in the Cipher Groups pane.

To bind a cipher group to an SSL virtual server, service, or service group by using the command line interface

At the command prompt, type one of the following:

- bind ssl vserver <vServerName> -cipherName <string>
- bind ssl service <serviceName> -cipherName <string>
- bind ssl serviceGroup <serviceGroupName> -cipherName <string>

Examples

```
> bind ssl vserver ssl_vserver_test -cipherName test
Done
bind ssl service  nshttps -cipherName test
Done
> bind ssl servicegroup  ssl_svc  -cipherName test
Done
```

Parameters for Binding a Cipher Group to an SSL Virtual Server, Service, or Service Group

vServerName (Name)

The name of the SSL virtual server to which the cipher suite is to be bound. Maximum Length: 127 characters.

vServer

Set the -vServer flag, which specifies that the cipher operation is performed on an SSL virtual server. (The configuration utility sets this parameter transparently.)

serviceName (Service Name)

The name of the SSL service to which the cipher suite is to be bound. Maximum Length: 127 characters.

service

Set the -service flag, which specifies that the cipher operation is performed on an SSL service or service group. (The configuration utility sets this parameter transparently.)

serviceGroupName (Service Group Name)

The name of the SSL service group to which the cipher suite is to be bound. Maximum Length: 127 characters.

cipherName

A cipher suite can consist of an individual cipher name, the predefined cipher-alias name, or user-defined cipher group name. This is a required parameter. Maximum Length: 39 characters.

To bind a cipher group to an SSL virtual server, service, or service group by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers, Services, or Service Groups.
2. In the details pane, select the virtual server, service, or service group to bind the cipher to, and then click Open.
3. In the Configure Virtual Server (SSL Offload), Configure Service, or Configure Service Group dialog box, on the SSL Settings tab, click Ciphers.
4. In the SSL-Offload - Configure Ciphers, Service - Configure Ciphers, or Service Group - Configure Ciphers dialog box, do one or both of the following:
   - To bind a cipher group, select a cipher group or alias from the Available Cipher Groups list, and then click Add. To unbind a group, select the cipher group or alias from the Configured Cipher Groups list, and then click Remove.
   - To bind a cipher, select a cipher group or alias from the Available Cipher Groups list, then select ciphers from the Available Ciphers list, and then click Add. To unbind a cipher. select the cipher from the Configured Ciphers list, and then click Remove.

   Note: To override an existing cipher or cipher group, drag and drop the configured cipher or cipher group to a new location in the Configured Ciphers list or the Configured Cipher Groups list so that it precedes the cipher or cipher group to be overridden.
5. Click OK to close the dialog box, and then click OK again.

Configuring SSL Actions and Policies

An SSL policy evaluates incoming traffic and applies a predefined action to requests that match a rule (expression). You have to configure the actions before creating the policies, so that you can specify an action when you create a policy. To put a policy into effect, you must either bind it to a virtual server on the appliance, so that it applies only to traffic flowing through that virtual server, or bind it globally, so that it applies to all traffic flowing through the appliance.

SSL actions define SSL settings that you can apply to the selected requests. You associate an action with one or more policies. Data in client connection requests or responses is compared to a rule specified in the policy, and the action is applied to connections that match the rule (expression).

You can configure classic policies with classic expressions and default syntax policies with default syntax expressions for SSL. For a complete description of these expressions, how they work, and how to configure them manually, see Policy Configuration and Reference.

Note: Users who are not experienced in configuring policies at the NetScaler command line usually find using the configuration utility to be considerably easier.

You can associate a user-defined action or a built-in action to a default syntax policy. Classic policies allow only user-defined actions. In default syntax policy, you can also group policies under a policy label, in which case they are applied only when invoked from another policy.

Common uses of SSL actions and policies include per-directory client authentication, support for Outlook web access, and SSL-based header insertions. SSL-based header insertions contain SSL settings required by a server whose SSL processing has been offloaded to the NetScaler appliance.

Configuring User-Defined Actions for SSL Policies

SSL policies require that you create an action before creating a policy, so that you can specify the actions when you create the policies. In SSL default syntax policies, you can also use the built-in actions. For more information about built-in actions, see Configuring Built-in SSL Actions.

To configure an SSL action by using the command line interface

At the command prompt, type the following commands to configure an action and verify the configuration:

- add SSL action <name> -clientAuth(DOCLIENTAUTH | NOCLIENTAUTH) -clientCert (ENABLED | DISABLED) certHeader <string> -clientHeader <string> -clientCertSerialNumber (ENABLED | DISABLED) -certSerialHeader <string> **-clientCertSubject** (ENABLED | DISABLED) -certSubjectHeader <string> -clientCertHash (ENABLED | DISABLED) -certHashHeader <string> -clientCertIssuer (ENABLED | DISABLED) -certIssuerHeader <string> -sessionID (ENABLED | DISABLED) -sessionIDheader <string> -cipher (ENABLED | DISABLED) -cipherHeader <string> -clientCertNotBefore (ENABLED | DISABLED) **-certNotBeforeHeader** <string> -clientCertNotAfter (ENABLED | DISABLED) -certNotAfterHeader <string> -OWASupport (ENABLED | DISABLED)

- show ssl action [<name>]

Example

```
> add ssl action Action-SSL-ClientCert -clientCert ENABLED -certHeader "X-Client-Cert"
 Done
> show ssl action Action-SSL-ClientCert
1)      Name: Action-SSL-ClientCert
        Data Insertion Action:
       Cert Header: ENABLED          Cert Tag: X-Client-Cert
 Done
```

Parameters for configuring an SSL action

name (Name)

The name of the SSL action. Maximum Length: 127 characters. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-)

characters.

clientAuth (Client Authentication)

Perform client certificate authentication. Possible values: ENABLED, DISABLED.

clientCert (Client Certificate)

Insert the entire client certificate into the HTTP header of the request being sent to the web server. The certificate is inserted in the ASCII (PEM) format. Possible values: ENABLED, DISABLED.

certHeader (Certificate Tag)

The name of the header into which the client certificate is inserted.

clientCertSerialNumber (Client Certificate Serial Number)

Insert the entire client serial number into the HTTP header of the request being sent to the web server. Possible values: ENABLED, DISABLED.

certSerialHeader (Serial Number Tag)

The name of the header into which the client serial number is inserted.

clientCertSubject (Client Certificate Subject (DN))

Insert the client certificate subject, also known as the distinguished name (DN), into the HTTP header of the request being sent to the web server. Possible values: ENABLED, DISABLED.

clientSubjectHeader (Subject Tag)

The name of the header into which the client certificate subject is inserted.

clientCertHash (Client Certificate Hash)

Insert the certificate signature (hash) into the HTTP header of the request being sent to the web server. Possible values: ENABLED, DISABLED.

certHashHeader (Hash Tag)

The name of the header into which the client certificate signature (hash) is inserted.

clientCertIssuer (Client Certificate Issuer)

Insert the certificate issuer into the HTTP header of the request being sent to the web server. Possible values: ENABLED, DISABLED.

certIssuerHeader (Issuer Tag)

The name of the header into which the client certificate issuer details are inserted.

sessionID (Session ID)

Insert the SSL session ID into the HTTP header of the request being sent to the web server. Every SSL connection that the client and the NetScaler share has a unique ID that identifies the specific connection. Possible values: ENABLED, DISABLED.

sessionIDHeader (Session ID Tag)

The tag name to be used while inserting the Session ID into the HTTP header. Maximum length: 31 characters.

cipher (Cipher Suite)

Insert the cipher suite negotiated by the client and the NetScaler for the particular SSL session into the HTTP header of the request being sent to the web server. The NetScaler will insert the cipher-suite name, SSL protocol, export or non-export string, and cipher strength bit, depending on the type of browser connecting to the SSL virtual server or service (for example, Cipher-Suite: RC4- MD5 SSLv3 Non-Export 128-bit). Possible values: ENABLED, DISABLED.

cipherHeader (Cipher Tag)

The name of the header into which the name of the cipher suite is inserted.

clientCertNotBefore (Client Certificate Not Before Date)

Insert the date from which the certificate is valid into the HTTP header of the request being sent to the web server. Every certificate is configured with the date and time from which it is valid. Possible values: ENABLED, DISABLED.

certNotBeforeHeader (Not Before Tag)

The name of the header into which to insert the date and time from which the certificate is valid.

clientCertNotAfter (Client Certificate Not After Date)

Insert the date of expiry of the certificate into the HTTP header of the request being sent to the web server. Every certificate is configured with the date and time at which the certificate expires. Possible values: ENABLED, DISABLED.

certNotAfterHeader (Not After Tag)

The name of the header into which the certificate's expiry date is inserted.

OWASupport (Outlook Web Access)

If the system is in front of an Outlook Web Access (OWA) server, insert a special header field, 'FRONT-END-HTTPS: ON', into the HTTP requests going to the OWA server. Possible values: ENABLED, DISABLED.

To configure an SSL action by using the configuration utility

1. In the navigation pane, expand SSL, and then click Policies.
2. On the Actions tab, in the details pane, click Add.
3. In the Create SSL Action dialog box, set the following parameters:
   - Name*
   - Client Authentication
   - Client Certificate
   - Certificate Tag
   - Client Certificate Serial Number
   - Serial Number Tag
   - Client Certificate Subject (DN)
   - Subject Tag
   - Client Certificate Hash
   - Hash Tag
   - Client Certificate Issuer
   - Issuer Tag
   - Session ID
   - Session ID Tag
   - Cipher Suite
   - Cipher Tag
   - Client Certificate Not Before Date
   - Not Before Tag
   - Client Certificate Not After Date
   - Not After Tag
   - Outlook Web Access

   * A required parameter
4. Click Create, and then click Close.

Configuring SSL Policies

Policies on the NetScaler help identify specific connections that you want to process. The processing is based on the actions that are configured for that particular policy. Once you create the policy and configure an action for it, you must either bind it to a virtual server on the NetScaler, so that it applies only to traffic flowing through that virtual server, or bind it globally, so that it applies to all traffic flowing through any virtual server configured on the NetScaler.

The NetScaler SSL feature supports both classic policies and default syntax policies . For a complete description of classic and default syntax expressions, how they work, and how to configure them manually, see Policy Configuration and Reference.

Note: Users who are not experienced in configuring policies at the NetScaler command line will usually find using the configuration utility considerably easier.

Configuring an SSL Default Syntax Policy

An SSL default syntax policy defines a control or a data action to be performed on requests. SSL policies can therefore be categorized as control policies and data policies:

- **Control policy**. A control policy uses a control action, such as forcing client authentication.

  Note: In release 10.5 or later, deny SSL renegotiation (denySSLReneg) is set, by default, to ALL. However, control policies, such as CLIENTAUTH, trigger a renegotiation handshake. If you use such policies, you must set denySSLReneg to NO.

- **Data policy**. A data policy uses a data action, such as inserting some data into the request.

The essential components of a policy are an expression and an action. The expression identifies the requests on which the action is to be performed. SSL policies use the default expression syntax or the classic expression syntax. For information about expressions and how to configure them, see Policy Configuration and Reference.

You can configure a default syntax policy with a built-in action or a user-defined action. You can configure a policy with a built-in action without creating a separate action. However, to configure a policy with a user-defined action, first configure the action and then configure the policy.

You can specify an additional action, called an UNDEF action, to be performed in the event that applying the expression to a request has an undefined result.

To configure an SSL default syntax policy by using the command line interface

At the command prompt, type:

add ssl policy <name> -rule <expression> -Action <string> [-undefAction <string>] [-comment <string>]

Parameters for configuring SSL default syntax policies

name (Name)

The name of the SSL policy. Maximum Length: 127 characters. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

rule (Expression)

The expression that sets the condition for application of the SSL policy. Maximum Length: 1499 characters.

Action (Request Action)

The name of the action to be performed on the request. Available built-in actions: NOOP, RESET, DROP, CLIENTAUTH, and NOCLIENTAUTH. Maximum Length: 127 characters.

undefAction (Undefined-Result Action)

The name of the action to be performed when the result of rule evaluation is undefined. Possible values for control policies: CLIENTAUTH, NOCLIENTAUTH, NOOP, RESET, DROP. Possible values for data policies: NOOP, RESET or DROP. Default: NOOP.

comment (Comments)

Comments associated with this policy. Maximum Length: 255 characters.

To configure an SSL default syntax policy by using the configuration utility

1. In the navigation pane, expand SSL, and then click Policies.
2. In the details pane, click Policies, and then click Add.
3. In the Create SSL Policy dialog box, set the following parameters:
   - Name*
   - Request Action*
   - Undefined-Result Action
   - Expression
   - Comments

   * A required parameter
4. Click Create, and then click Close.
5. On the Policies tab, verify that the settings displayed for the policy that you just configured are correct.

Configuring Built-in Actions for SSL Default Syntax Policies

Unless you need only the built-in actions in your policies, you have to create the actions before creating the policies, so that you can specify the actions when you create the policies. The built-in actions are of two types, control actions and data actions. You use control actions in control policies, and data actions in data policies.

The built-in control actions are:

- CLIENTAUTH—Perform client certificate authentication.
- NOCLIENTAUTH—Do not perform client certificate authentication.

The built-in data actions are:

- RESET—Close the connection by sending a RST packet to the client.
- DROP—Drop all packets from the client. The connection remains open until the client closes it.
- NOOP—Forward the packet without performing any operation on it.

You can create user-defined data actions. For example, if you enable client authentication, you can create an SSL action to insert client-certificate data into the request header before forwarding the request to the web server. For more information about user-defined actions, see Configuring User-Defined SSL Actions.

If a policy evaluation results in an undefined state, an UNDEF action is performed. For either a data policy or a control policy, you can specify RESET, DROP, or NOOP as the UNDEF action. For a control policy, you also have the option of specifying CLIENTAUTH or NOCLIENTAUTH.

Examples of built-in actions in a policy

In the following example, if the client sends a cipher other than an EXPORT category cipher, the NetScaler appliance requests client authentication. The client has to provide a valid certificate for a successful transaction.

```
add ssl policy pol1 -rule CLIENT.SSL.CIPHER_EXPORTABLE.NOT -reqAction CLIENTAUTH
```

The following examples assume that client authentication is enabled.

If the version in the certificate provided by the user matches the version in the policy, no action is taken and the packet is forwarded:

```
add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -reqAction NOOP
```

If the version in the certificate provided by the user matches the version in the policy, the connection is dropped:

```
add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -reqAction DROP
```

If the version in the certificate provided by the user matches the version in the policy, the connection is reset:

```
add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -reqAction RESET
```

Configuring SSL Policy Labels

Policy labels are holders for policies. A policy label helps in managing a group of policies, called a policy bank, which can be invoked from another policy. SSL policy labels can be control labels or data labels, depending on the type of policies that are included in the policy label. You can add only data policies in a data policy label and only control policies in a control policy label. To create the policy bank, you bind policies to the label and specify the order of evaluation of each policy relative to others in the bank of policies for the policy label. At the NetScaler command line, you enter two commands to create a policy label and bind policies to the policy label. In the configuration utility, you select options from a dialog box.

To create an SSL policy label and bind policies to the label by using the command line interface

At the command prompt, type:

- add ssl policylabel <labelName> -type (CONTROL | DATA)
- bind ssl policylabel <labelName> <policyName> <priority> [<gotoPriorityExpression>] [-invoke (<labelType> <labelName>)]

Example

```
add ssl policylabel cpl1 -type CONTROL
add ssl policylabel dpl1 -type DATA
bind ssl policylabel cpl1 -policyName ctrlpol -priority 1
bind ssl policylabel dpl1 -policyName datapol -priority 1
```

Parameters for configuring SSL policy labels

labelName (Name)

The name of the SSL policy label to be created. Maximum Length: 127 characters. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Type (Type)

The type of policy that the policy label can hold. Possible values: CONTROL, DATA.

To configure an SSL policy label and bind policies to the label by using the configuration utility

1. In the navigation pane, expand SSL, and then click Policy Labels.
2. In the details pane, click Add.
3. In the Create new SSL Policy Label dialog box, set the following parameters:
   - Name*
   - Type*

   * A required parameter
4. Click Insert Policy, and select from the following:
   - **Policy Name**. The name of an existing policy.
   - **New policy**. Invokes the policy creation editor.
5. Click Create, and then click Close.
6. On the Policies tab, verify that the settings displayed for the policy that you just configured are correct.

Configuring Per-Directory Client Authentication

If you create an action specifying client-side authentication on a per-directory basis, a client identified by a policy associated with the action is not authenticated as part of the initial SSL handshake. Instead, authentication is carried out every time the client wants to access a specific directory on the web server.

For example, if you have multiple divisions in the company, where each division has a folder in which all its files are stored, and you want to know the identity of each client that tries to access files from a particular directory, such as the finance directory, you can enable per-directory client authentication for that directory.

To enable per-directory client authentication, first configure client authentication as an SSL action, and then create a policy that identifies the directory that you want to monitor. When you create the policy, specify your client-authentication action as the action associated with the policy. Then, bind the policy to the SSL virtual server that will receive the SSL traffic.

To create an SSL action and a policy to enable client authentication by using the command line interface

At the command prompt, type the following commands to create an SSL action to enable to client authentication and verify the configuration:

- add ssl action <name> [-clientAuth (DOCLIENTAUTH | NOCLIENTAUTH)]
- show ssl action [<name>]
- add ssl policy <name> -rule <expression> [-action <string>] [-undefAction <string>] [-comment <string>]
- show ssl policy [<name>]

Example

```
> add ssl action ssl-action-1 -clientAuth DOCLIENTAUTH
 Done
> show ssl action ssl-action-1
1)      Name: ssl-action-1
       Client Authentication Action: DOCLIENTAUTH
                              Hits: 0
                         Undef Hits: 0
                            Action Reference Count: 1
 Done
```

```
> add ssl policy ssl-pol-1 -rule 'REQ.HTTP.METHOD==GET' -reqaction ssl-action-1
> sh ssl policy ssl-pol-1
                        Name: ssl-pol-1
                        Rule: REQ.HTTP.METHOD == GET
                        Action: ssl-action-1
                        UndefAction: Use Global
                      Hits: 0
                      Undef Hits: 0
 Done
```

Parameters for enabling client authentication

name (Name)

The name for the new SSL action. Maximum Length: 127

This is a mandatory argument.

clientAuth (Client Authentication)

Set action to do client certificate authentication or no authentication.

DOCLIENTAUTH: Perform client certificate authentication.

NOCLIENTAUTH: No client certificate authentication.

Possible values: DOCLIENTAUTH, NOCLIENTAUTH

To create an SSL action to enable client authentication by using the configuration utility

1. In the navigation pane, expand SSL, and then click Policies.
2. In the details pane, on the Actions tab, click Add.
3. In the Create SSL Action dialog box, set values for the following parameters:
   - Name*
   - Client Authentication

   * A required parameter
4. Click Create, and then click Close.

To create and bind an SSL policy to enable client authentication by using the configuration utility

1. In the navigation pane, expand SSL, and then click Policies.
2. In the details pane, on the Policies tab, click Add.
3. In the Create SSL Policy dialog box, set values for the following parameters:
   - Name*
   - Request Action*

   * A required parameter
4. Click Add Expression to add an expression.
5. Click Create, and then click Close.
6. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
7. In the details pane, select a virtual server, and then click Open.
8. In the Configure Virtual Server (SSL Offload) dialog box, click SSL Policies.
9. In the Bind/Unbind SSL Policies dialog box, click Insert Policy, and from the list select the policy that you want to bind to the virtual server.

Configuring Support for Outlook Web Access

If your SSL configuration is offloading SSL transactions from an Outlook Web Access (OWA) server, you must insert a special header field, FRONT-END-HTTPS: ON, in all HTTP requests directed to the OWA servers. This is required for the OWA servers to generate URL links as https:// instead of http://.

When you enable support for OWA on the NetScaler, the header is automatically inserted into the specified HTTP traffic, and you do not need to configure a specific header insertion. Use SSL policies to identify all traffic directed to the OWA server.

Note: You can enable Outlook Web Access support for HTTP-based SSL virtual servers and services only. You cannot apply it to TCP-based SSL virtual servers and services.

To enable OWA support, first configure OWA support as an SSL action, and then create a policy that identifies the virtual servers or services for which you want to enable OWA support. When you create the policy, specify your OWA support action as the action associated with the policy. Then, bind the policy to the SSL virtual server that will receive the SSL traffic.

To create an SSL action and a policy to enable OWA support by using the command line interface

At the command prompt, type the following commands to create an SSL action to enable OWA support and verify the configuration:

- add ssl action <name> -OWASupport (ENABLED | DISABLED)
- show ssl action [<name>]
- add ssl policy <name> -rule <expression> [-action <string>] [-undefAction <string>] [-comment <string>]
- show ssl policy [<name>]

Example

```
> add ssl action ssl-action-2 -OWASupport ENABLED
 Done
> show ssl action ssl-action-2
1)      Name: ssl-action-2
       Type: Data Insertion
       OWA Support: ENABLED
                          Hits: 0
```

```
                    Undef Hits: 0
                       Action Reference Count: 1
 Done
> add ssl policy ssl-pol -rule 'REQ.HTTP.METHOD == GET' -reqaction ssl-action-2
Done
> sh ssl policy ssl-pol
                    Name: ssl-pol
                    Rule: REQ.HTTP.METHOD == GET
                    Action: ssl-action-2
                    UndefAction: Use Global
                    Hits: 0
                    Undef Hits: 0
Done
```

Parameters for enabling support for Outlook Web Access

name (Name)

The name for the new SSL action. Maximum Length: 127

OWASupport (Outlook Web Access)

The state of Outlook Web-Access support. If the system is in front of an Outlook Web Access (OWA) server, a special header field, 'FRONT-END-HTTPS: ON', needs to be inserted in the HTTP requests going to the OWA server.

To create an SSL action to enable OWA support by using the configuration utility

1. In the navigation pane, expand SSL, and then click Policies.
2. On the Actions tab, in the details pane, click Add.
3. In the Create SSL Action dialog box, set the following parameters:
   - Name*
   - Outlook Web Access

   * A required parameter
4. Click Create, and then click Close.

   Note: Outlook Web Access support is applicable only for SSL virtual server based configurations and transparent SSL service based configurations and not for SSL configurations with back-end encryption.

To create and bind an SSL policy to enable OWA support by using the configuration utility

1. In the navigation pane, expand SSL, and then click Policies.
2. In the details pane, on the Policies tab, click Add.
3. In the Create SSL Policy dialog box, set values for the following parameters:
   - Name*
   - Request Action*

   * A required parameter
4. Click Add Expression to add an expression.
5. Click Create, and then click Close.
6. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
7. In the details pane, select a virtual server, and then click Open.
8. In the Configure Virtual Server (SSL Offload) dialog box, click SSL Policies.
9. In the Bind/Unbind SSL Policies dialog box, click Insert Policy, and from the list select the policy that you want to bind to the virtual server.

Configuring SSL-Based Header Insertion

Because the NetScaler appliance offloads all SSL-related processing from the servers, the servers receive only HTTP traffic. In some circumstances, the server needs certain SSL information. For example, security audits of recent SSL transactions require the client subject name (contained in an X509 certificate) to be logged on the server.

Such data can be sent to the server by inserting it into the HTTP header as a name-value pair. You can insert the entire client certificate, if required, or only the specific fields from the certificate, such as the subject, serial number, issuer, certificate hash, SSL session ID, cipher suite, or the not-before or not-after date used to determine certificate validity.

You can enable SSL-based insertion for HTTP-based SSL virtual servers and services only. You cannot apply it to TCP-based SSL virtual servers and services. Also, client authentication must be enabled on the SSL virtual server, because the inserted values are taken from the client certificate that is presented to the virtual server for authentication.

To configure SSL-based header insertion, first create an SSL action for each specific set of information to be inserted, and then create policies that identify the connections for which you want to insert the information. As you create each policy, specify the action that you want associated with the policy. Then, bind the policies to the SSL virtual servers that will receive the SSL traffic.

The following example uses default syntax policies. In the following example, a control policy (ctrlpol) is created to perform client authentication if a request is received for the URL /testsite/file5.html. A data policy (datapol) is created to perform an action (act1) if client authentication is successful, and an SSL action (act1) is added to insert the certificate details and issuer's name in the request before forwarding the request. For other URLs, client authentication is disabled. The policies are then bound to an SSL virtual server (ssl_vserver) that receives the SSL traffic.

Command-line example of configuring SSL-based header insertion

For descriptions of the parameters used in the following commands, see Parameters for configuring an SSL action and Parameters for configuring SSL policies:

Example

```
> add ssl action act1 -clientCert ENABLED -certHeader mycert -clientcertissuer ENABLED -certIssuerHeader m
> add ssl policy datapol -rule HTTP.REQ.URL.EQ(\"/testsite/file5.html\") -action act1
> add ssl policy ctrlpol -rule HTTP.REQ.URL.EQ(\"/testsite/file5.html\") -action CLIENTAUTH
> bind ssl vserver ssl_vserver -policyName ctrlpol -priority 1
> bind ssl vserver ssl_vserver -policyName datapol -priority 1
 Done
```

To configure SSL-based header insertion by using the configuration utility

1. In the navigation pane, expand SSL, and then click Policies.
2. In the details pane, on the Actions tab, click Add.
3. In the Create SSL Action dialog box, set the following parameters (for descriptions of the parameters, see Parameters for Configuring an SSL Action):
   - Name*
   - Client Certificate
   - Certificate Tag
   - Client Certificate Issuer
   - Issuer Tag

   * A required parameter
4. Click Create, and then click Close.
5. On the tab, click Add to create a control policy.
6. In the Create SSL Policy dialog box, set the following parameters (for descriptions of the parameters, see Parameters for configuring SSL policies):
   - Name*
   - Expression
   - Request Action

   * A required parameter
7. Click Create, and then click Close.
8. Create a data policy by repeating steps 5 through 7.
9. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
10. In the details pane, from the list of virtual servers, select the virtual server to which you want to bind the SSL policies, and then click Open.
11. In the Configure Virtual Server (SSL Offload) dialog box, click SSL Settings, and then click SSL Policies.
12. In the Bind/Unbind SSL Policies dialog box, click Insert Policy. Under Policy Name, select the policy that you created in steps 5 through 7.
13. Click OK, and then click Close. A message appears in the status bar, stating that the policy has been bound successfully.
14. Repeat steps 12 and 13 and select the policy that you created in step 8.

Binding SSL Policies to a Virtual Server

The SSL policies that are configured on the NetScaler appliance need to be bound to a virtual server that intercepts traffic directed to the virtual server. If the incoming data matches any of the rules configured in the SSL policy, the policy is triggered and the action associated with it is carried out.

You can also bind SSL policies globally or to custom bind points on the NetScaler appliance. For more information about binding policies on the appliance, see Policy Configuration and Reference.

To bind an SSL policy to a virtual server by using the command line interface

At the command prompt, type the following command to bind an SSL policy to a virtual server and verify the configuration:

- bind ssl vserver <vServerName> -policyName <string> [-priority <positive_integer>]
- show ssl vserver <vServerName>

Example

```
> bind ssl vserver vs-server -policyName ssl-policy-1 -priority 10
 Done
> show ssl vserver vs-server

        Advanced SSL configuration for VServer vs-server:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 1000
        Session Reuse: ENABLED          Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 80
        Client Auth: DISABLED
        SSL Redirect: ENABLED
        SSL-REDIRECT Port Rewrite: ENABLED
        Non FIPS Ciphers: DISABLED
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)      Policy Name: ssl-policy-1       Priority: 10

1)      Cipher Name: DEFAULT
        Description: Predefined Cipher Alias
 Done
```

Parameters for binding SSL policies to a virtual server

vServerName

The name of the SSL virtual server to which the SSL policy needs to be bound.

This is a mandatory argument. Maximum Length: 127

policyName

The name of the SSL policy. Maximum Length: 127

priority

Priority. Minimum value: 0

Maximum value: 64000

To bind an SSL policy to a virtual server by using the configuration utility

1. In the navigation pane, expand SSL Offload, and then click Virtual Servers.
2. In the details pane, from the list of virtual servers, select the virtual server to which you want to bind the SSL policy, and then click Open.
3. In the Configure Virtual Server (SSL Offload) dialog box, on the Policies tab, in the details pane, click Insert Policy.
4. Under Policy Name, select the policy that you want to bind to the virtual server.
5. Click OK, and then click Close. A message appears in the status bar, stating that the policy has been bound successfully.

Binding SSL Policies Globally

Globally bound policies are evaluated after all policies bound to services, virtual servers, or other NetScaler bind points are evaluated.

To globally bind an SSL policy by using the command line interface

At the command prompt, type the following command to bind a global SSL policy and verify the configuration:

- bind ssl global - policyName <string> [- priority <positive_integer>]
- show ssl global

Example

```
> bind ssl global -policyName Policy-SSL-2 -priority 90
Done
> sh ssl global
1) Name: Policy-SSL-2 Priority: 90
2) Name: Policy-SSL-1 Priority: 100
Done
```

Parameters for globally binding an SSL policy

policyName (Policy Name)

The name of the SSL policy. Maximum Length: 127.

priority (Priority)

A numeric value that indicates when this policy is evaluated relative to others. A lower priority is evaluated before a higher one.

To bind a global SSL policy by using the configuration utility

1. In the navigation pane, expand SSL, and then click Policies.
2. In the details pane, click Global Bindings.
3. In the Bind/Unbind SSL Policies to Global dialog box, click Insert Policy.
4. In the Policy Name drop-down list, select a policy.
5. Optionally, drag the entry to a new position in the policy bank to automatically update the priority level.
6. Click OK. A message appears in the status bar, stating that the policy has been bound successfully.

Commonly Used SSL Configurations

SSL deployments typically use some version of one or more of the following configurations:

- SSL Offloading with End-to-End Encryption
- Transparent SSL Acceleration
    - Service-based Transparent SSL Acceleration
    - Virtual Server-based Acceleration with a Wildcard IP Address (*:443)
    - SSL VIP-based Transparent Access with End-To-End Encryption
- SSL Acceleration with HTTP on the Front-End and SSL on the Back-End
- SSL Offloading with Other-TCP Protocols
    - SSL_TCP Based Offloading with End-to-End Encryption
    - Backend Encryption for TCP Based Data
- SSL Bridging

Configuring SSL Offloading with End-to-End Encryption

A simple SSL offloading setup terminates SSL traffic (HTTPS), decrypts the SSL records, and forwards the clear text (HTTP) traffic to the back-end web servers. However, the clear text traffic is vulnerable to being spoofed, read, stolen, or compromised by individuals who succeed in gaining access to the back-end network devices or web servers.

You can, therefore, configure SSL offloading with end-to-end security by re-encrypting the clear text data and using secure SSL sessions to communicate with the back-end Web servers.

Additionally, you can configure the back-end SSL transactions so that the NetScaler appliance uses SSL session multiplexing to reuse existing SSL sessions with the back-end web servers, thus avoiding CPU-intensive key exchange (full handshake) operations. This reduces the overall number of SSL sessions on the server, and therefore accelerates the SSL transaction while maintaining end-to-end security.

To configure SSL Offloading with end-to-end encryption, add SSL based services that represent secure servers with which the NetScaler appliance will carry out end-to-end encryption. Then create an SSL based virtual server, and create and bind a valid certificate-key pair to the virtual server. Bind the SSL services to the virtual server to complete the configuration.

For details on adding SSL based services, see Configuring Services.

For details on adding an SSL virtual server, see Configuring an SSL Based Virtual Server.

For details on creating a certificate-key pair, see Adding a Certificate-Key Pair.

For details on binding a certificate-key pair to a virtual server, see Binding the Certificate Key Pair to the SSL Based Virtual Server.

For details on binding services to a virtual server, see Binding Services to the SSL Based Virtual Server.

Example

Create two SSL based services, Service-SSL-1 and Service-SSL-2, with IP addresses 10.102.20.30 and 10.102.20.31 and both using port 443.

Then create an SSL based virtual server, Vserver-SSL-2 with an IP address of 10.102.10.20.

Next, create a certificate-key pair, CertKey-1 and bind it to the virtual server.

Bind the SSL services to the virtual server to complete the configuration.

Table 1. Entities in the SSL Offloading with End-to-End Encryption Example

Entity	Name	Value
SSL Service	Service-SSL-1	10.102.20.30
	Service-SSL-2	10.102.20.31
SSL Based Virtual Server	Vserver-SSL-2	10.102.10.20
Certificate - Key Pair	Certkey-1	

Configuring Transparent SSL Acceleration

Note: You need to enable L2 mode on the NetScaler appliance for transparent SSL acceleration to work.

Transparent SSL acceleration is useful for running multiple applications on a secure server with the same public IP, and also for SSL acceleration without using an additional public IP.

In a transparent SSL acceleration setup, the NetScaler appliance is transparent to the client, because the IP address at which the appliance receives requests is the same as the Web server's IP address.

The NetScaler offloads SSL traffic processing from the Web server and sends either clear text or encrypted traffic (depending on the configuration) to the web server. All other traffic is transparent to the NetScaler and is bridged to the Web server. Therefore, other applications running on the server are unaffected.

There are three modes of transparent SSL acceleration available on the NetScaler:

- Service-based transparent access, where the service type can be SSL or SSL_TCP.
- Virtual server-based transparent access with a wildcard IP address (*:443).
- SSL VIP-based transparent access with end-to-end encryption.

Note: An SSL_TCP service is used for non-HTTPS services (for example SMTPS and IMAPS).

Service-based Transparent SSL Acceleration

To enable transparent SSL acceleration using the SSL service mode, configure an SSL or an SSL_TCP service with the IP address of the actual back-end Web server. Instead of a virtual server intercepting SSL traffic and passing it on to the service, the traffic is now directly passed on to the service, which decrypts the SSL traffic and sends clear text data to the back-end server.

The service-based mode allows you to configure individual services with a different certificate, or with a different clear text port. Also, you can also select individual services for SSL acceleration.

You can apply service-based transparent SSL acceleration to data that uses different protocols, by setting the clear text port of the SSL service to the port on which the data transfer between the SSL service and the back-end server occurs.

To configure service-based transparent SSL acceleration, first enable both the SSL and the load balancing features. Then create an SSL based service and configure its clear text port. After the service is created, create and bind a certificate-key pair to this service.

For details on configuring the clear text port for an SSL based service, see "Configuring Advanced SSL Settings."

For details on creating a certificate-key pair and binding a certificate-key pair to a service, see "Adding a Certificate-Key Pair."

Example

Enable SSL offloading and load balancing.

Create an SSL based service, Service-SSL-1 with the IP address 10.102.20.30 using port 443 and configure its clear text port.

Next, create a certificate-key pair, CertKey-1 and bind it to the SSL service.

Table 1. Entities in the Service-based Transparent SSL Acceleration

Entity	Name	Value
SSL Service	Service-SSL-1	102.20.30
Certificate - Key Pair	Certkey-1	

Virtual Server-based Acceleration with a Wildcard IP Address (*:443)

You can use an SSL virtual server in the wildcard IP address mode if when you want to enable SSL acceleration for multiple servers that host the secure content of a Web site. In this mode, a single-digital certificate is enough for the entire secure Web site, instead of one certificate per virtual server. This results in significant cost savings on SSL certificates and renewals. The wildcard IP address mode also enables centralized certificate management.

To configure global transparent SSL acceleration on the NetScaler appliance, create a *:443 virtual server, which is a virtual server that accepts any IP address associated with port 443. Then, bind a valid certificate to this virtual server, and also bind all services to which the virtual server is to transfer. Such a virtual server can use the SSL protocol for HTTP-based data or the SSL_TCP protocol for non-HTTP-based data.

To configure virtual server-based acceleration with a wildcard IP address

1. Enable SSL, as described in "Enabling SSL Processing."
2. Enable load balancing, as described in "Load Balancing."
3. Add an SSL based virtual server (see "Configuring an SSL-Based Virtual Server" for the basic settings), and set the clearTextPort parameter (described in "Configuring Advanced SSL Settings)."
4. Add a certificate-key pair, as described in "Adding a Certificate-Key Pair."

   Note: The wildcard server will automatically learn the servers configured on the NetScaler, so you do not need to configure services for a wildcard virtual server.

Example

After enabling SSL offloading and load balancing, create an SSL based wildcard virtual server with IP address set to * and port number 443, and configure its clear text port (optional).

If you specify the clear text port, decrypted data will be sent to the backend server on that particular port. Otherwise, encrypted data will be sent to port 443.

Next, create an SSL certificate key pair, CertKey-1 and bind it to the SSL virtual server.

Table 2. Entities in the Virtual Server-based Acceleration with a Wildcard IP Address Example

Entity	Name	IP Address	Port
SSL Based Virtual Server	Vserver-SSL-Wildcard	*	443
Certificate - Key Pair	Certkey-1		

SSL VIP-based Transparent Access with End-To-End Encryption

You can use an SSL virtual server for transparent access with end-to-end encryption if you have no clear text port specified. In such a configuration, the NetScaler terminates and offloads all SSL processing, initiates a secure SSL session, and sends the encrypted data, instead of clear text data, to the web servers on the port that is configured on the wildcard virtual server.

Note: In this case, the SSL acceleration feature runs at the back-end, using the default configuration, with all 34 ciphers available.

To configure SSL VIP based transparent access with end-to-end encryption, Follow instructions for Configuring a Virtual Server-based Acceleration with a Wildcard IP Address (*:443), but do not configure a clear text port on the virtual server.

Configuring SSL Acceleration with HTTP on the Front End and SSL on the Back End

In certain deployments, you might be concerned about network vulnerabilities between the NetScaler appliance and the backend servers, or you might need complete end-to-end security and interaction with certain devices that can communicate only in clear text (for example, caching devices).

In such cases, you can set up an HTTP virtual server that receives data from clients that connect to it at the front end and hands the data off to a secure service, which securely transfers the data to the web server.

To implement this type of configuration, you configure an HTTP virtual server on the NetScaler and bind SSL based services to the virtual server. The NetScaler receives HTTP requests from the client on the configured HTTP virtual server, encrypts the data, and sends the encrypted data to the web servers in a secure SSL session.

To configure SSL acceleration with HTTP on the front-end and SSL on the back-end, first enable the load balancing and SSL features on the NetScaler. Then, add SSL based services that represent secure servers to which the NetScaler appliance will send encrypted data. Finally, add an HTTP based virtual server and bind the SSL services to this virtual server.

Example

Enable load balancing and SSL acceleration on the NetScaler.

After enabling load balancing and SSL acceleration, create two SSL based services, Service-SSL-1 and Service-SSL-2, with IP addresses 10.102.20.30 and 10.102.20.31, and both using port 443.

Then create an HTTP based virtual server, Vserver-HTTP-1, with an IP address of 10.102.10.20.

Bind the SSL services to the virtual server to complete the configuration.

Table 1. Entities in the SSL Acceleration with HTTP on the Front End and SSL on the Back End Example

Entity	Name	Value
SSL Service	Service-SSL-1	10.102.20.30
	Service-SSL-2	10.102.20.31
HTTP Based Virtual Server	Vserver-HTTP-1	10.102.10.20

SSL Offloading with Other TCP Protocols

In addition to the secure HTTP (HTTPS) protocol, NetScaler appliances support SSL acceleration for other TCP-based secure protocols. However, only simple requests and response-based TCP application protocols are supported. Applications such as FTPS, that insert the server's IP address and port information in their payloads, are not currently supported.

Note: The STARTTLS feature for SMTP is currently not supported.

The NetScaler supports SSL acceleration for Other TCP protocols with and without end-to-end encryption.

To configure SSL offloading with Other TCP protocols, create a virtual server of type SSL_TCP, bind a certificate-key pair and TCP based services to the virtual server, and configure SSL actions and policies based on the type of traffic expected and the acceleration to be provided.

Follow the instructions in Configuring SSL Offloading, but create an SSL_TCP virtual server instead of an SSL virtual server, and configure TCP services instead of HTTP services.

SSL_TCP Based Offloading with End-to-End Encryption

To configure SSL_TCP-based offloading with end-to-end encryption, both the virtual server that intercepts secure traffic and the services that it forwards the traffic to must be of type SSL_TCP.

Configure SSL_TCP-based offloading as described in Configuring SSL Offloading with End-to-End Encryption, but create an SSL_TCP virtual server instead of an SSL virtual server.

Backend Encryption for TCP Based Data

Some deployments might require the NetScaler appliance to encrypt TCP data received as clear text and send the data securely to the back end servers.

To provide SSL acceleration with back-end encryption for clear text TCP traffic arriving from the client, create a TCP based virtual server and bind it to SSL_TCP based services.

To configure end-to-end encryption for TCP-based data, follow the procedure described in Configuring the SSL feature with HTTP on the Front-End and SSL on the Back-End, but create a TCP virtual server instead of an HTTP virtual server.

Configuring SSL Bridging

An SSL bridge configured on the NetScaler appliance enables the appliance to bridge all secure traffic between the SSL client and the SSL server. The appliance does not offload or accelerate the bridged traffic, nor does it perform encryption or decryption. Only load balancing is done by the appliance. The SSL server must handle all SSL-related processing. Features such as content switching, SureConnect, and cache redirection do not work, because the traffic passing through the appliance is encrypted.

Because the appliance does not carry out any SSL processing in an SSL bridging setup, there is no need for SSL certificates.

Citrix recommends that you use this configuration only if an acceleration unit (for example, a PCI-based SSL accelerator card) is installed in the web server to handle the SSL processing overhead.

Before you configure SSL bridging, first enable SSL and load balancing on the appliance. Then, create SSL_Bridge services and bind them to an SSL_Bridge virtual server. Configure the load balancing feature to maintain server persistency for secure requests.

Example

After enabling SSL and load balancing, create two servers, s1 and s2. Create two SSL_Bridge services, sc1 and src2. Create an SSL_Bridge virtual server and bind the SSL_Bridge services to the virtual server to complete the configuration. At the command line, type:

```
enable ns feature SSL LB
add server s1 10.102.1.101
add server s2 10.102.1.102
add service src1 s1 SSL_BRIDGE 443
add service src2 s2 SSL_BRIDGE 443
add lb vserver ssl_bridge_vip SSL_BRIDGE 10.102.1.200 443
bind lb vserver ssl_bridge_vip src1
bind lb vserver ssl_bridge_vip src2
```

Configuring the SSL Feature for Commonly Used Deployment Scenarios

Some of the most commonly deployed NetScaler SSL configurations are for load balancing secure data, applying content switching to secure data, and monitoring secure data:

- Configuring an SSL Virtual Server for Load Balancing.
- Configuring a Secure Content Switching Server.
- Configuring SSL Monitoring when Client Authentication is Enabled on the Backend Service.

Configuring an SSL Virtual Server for Load Balancing

A virtual server configured to load balance incoming secure data first decrypts the data and then selects a web server as determined by the configured load balancing policies. The NetScaler appliance then sends the decrypted data to the selected server, using a mapped IP address as the source IP address.

To configure load balancing on the appliance, you must first create an SSL-based load balancing virtual server and two or more HTTP-based services. You then bind the services and an SSL certificate to the virtual server. If no load balancing policy or method is configured, the default, LEASTCONNECTION, method is used.

Example

```
> add service ssl1 10.102.29.252 HTTP 80
> add service ssl2 10.102.29.253 HTTP 80
> add lb vserver vssl  SSL 10.102.29.133 443
> bind lb vserver vssl ssl1
> bind lb vserver vssl ssl2
> add ssl certKey sslckey -cert server_cert.pem -key server_key.pem -password ssl
> bind ssl vserver vssl certkeyName sslckey
> show ssl vserver vssl

Advanced SSL configuration for VServer vssl:
      DH: DISABLED
      Ephemeral RSA: ENABLED         Refresh Count: 0
      Session Reuse: ENABLED         Timeout: 120 seconds
      Cipher Redirect: DISABLED
      SSLv2 Redirect: DISABLED
      ClearText Port: 0
      Client Auth: DISABLED
      SSL Redirect: DISABLED
      Non FIPS Ciphers: DISABLED
      SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)     CertKey Name: sslckey   Server Certificate

1)     Cipher Name: DEFAULT
      Description: Predefined Cipher Alias
 Done
```

Configuring a Secure Content Switching Server

An SSL-based content switching virtual server first decrypts the secure data and then redirects the data to appropriately configured servers as determined by the type of content and the configured content switching policies. The packets sent to the server have a mapped IP address as the source IP address.

The following example shows the steps to configure two address-based virtual servers to perform load balancing on the HTTP services. One virtual server, Vserver-LB-HTML, load balances the dynamic content (cgi, asp), and the other, Vserver-LB-Image, load balances the static content (gif, jpeg). The load-balancing method used is the default, LEASTCONNECTION. A content switching SSL virtual server, Vserver-CS-SSL, is then configured to perform SSL acceleration and switching of HTTPS requests on the basis of configured content switching policies.

Example

```
> enable ns feature lb cs ssl
> add lb vserver Vserver-LB-HTML http 10.1.1.2 80
> add lb vserver Vserver-LB-Image http 10.1.1.3 80
> add service s1 10.1.1.4 http 80
> add service s2 10.1.1.5 http 80
> add service s3 10.1.1.6 http 80
> add service s4 10.1.1.7 http 80
> bind lb vserver Vserver-LB-HTML s1
> bind lb vserver Vserver-LB-HTML s2
> bind lb vserver Vserver-LB-Image s3
> bind lb vserver Vserver-LB-Image s4
> add cs vserver Vserver-CS-SSL ssl 10.1.1.1 443
> add cs policy pol1 -url "*.cgi"
> add cs policy pol2 -url "*.asp"
> add cs policy pol3 -url "*.gif"
> add cs policy pol4 -url "*.jpeg"
> bind cs vserver Vserver-CS-SSL -policyName pol1 Vserver-LB-HTML
> bind cs vserver Vserver-CS-SSL -policyName pol2 Vserver-LB-HTML
> bind cs vserver Vserver-CS-SSL -policyName pol3 Vserver-LB-Image
> bind cs vserver Vserver-CS-SSL -policyName pol4 Vserver-LB-Image
> add certkey mykey -cert /nsconfig/ssl/ns-root.cert -key /nsconfig/ssl/ns-root.key
> bind certkey Vserver-CS-SSL mykey
>
> show cs vserver Vserver-CS-SSL
      Vserver-CS-SSL (10.1.1.1:443) - SSL Type: CONTENT
      State: UP
      Last state change was at Tue Jul 13 02:11:37 2010
      Time since last state change: 0 days, 00:02:12.440
      Client Idle Timeout: 180 sec
      Down state flush: ENABLED
```

Disable Primary Vserver On Down : DISABLED
State Update: DISABLED
Default: Content Precedence: RULE
Vserver IP and Port insertion: OFF
Case Sensitivity: ON
Push: DISABLED Push VServer:
Push Label Rule: none

Configuring SSL Monitoring when Client Authentication is Enabled on the Backend Service

Consider a scenario in which you need to load balance servers that require SSL client certificates to validate clients. For this deployment, you need to create an SSL service on the NetScaler appliance, add an HTTPS monitor, add a certificate-key pair, bind this certificate-key pair to the SSL service, and then bind the https monitor to this service. You can use this https monitor to perform health checks on the backend services.

To configure SSL monitoring with client certificate

1. Open an SSH connection to the appliance by using an SSH client, such as PuTTY.
2. Log on the appliance by using the administrator credentials.
3. Add an SSL service. At the command prompt, type:

   add service <name> <serverName> <serviceType> <port>
4. Add an https monitor. At the command prompt, type:

   add lb monitor <name> <type>
5. Add the certificate-key pair that is going to be used as the client cert for that SSL service. At the command prompt, type:

   add ssl certKey <certkeyName> -cert <string> -key <string>
6. Bind this certkey to the SSL service. At the command prompt, type:

   bind ssl service <serviceName> -certkeyName <string>
7. Bind the https monitor to the SSL service. At the command prompt, type:

   bind lb monitor <monitorName> <serviceName>

Now, when the appliance tries to probe the backend service on which client authentication is enabled, the backend service will request a certificate as part of the SSL handshake. When the appliance returns the certificate-key bound in step 6 above, the monitor probe will succeed.

Example

```
add service svc_k 10.102.145.30 SSL 443
add lb monitor sslmon HTTP -respCode 200 -httpRequest "GET /testsite/file5.html" -secure YES
add ssl certKey ctest -cert client_rsa_1024.pem -key client_rsa_1024.ky
bind ssl service svc_k -certkeyName ctest
bind lb monitor sslmon svc_k
> show service svc_k
     svc_k (10.102.145.30:443) - SSL
     State: UP
     Last state change was at Tue Jan 10 13:12:24 2012
     Time since last state change: 0 days, 00:09:37.890
     Server Name: 10.102.145.30
     Server ID : 0 Monitor Threshold : 0
     Max Conn: 0 Max Req: 0 Max Bandwidth: 0 kbits
     Use Source IP: NO
     Client Keepalive(CKA): NO
     Access Down Service: NO
     TCP Buffering(TCPB): NO
     HTTP Compression(CMP): NO
     Idle timeout: Client: 180 sec Server: 360 sec
     Client IP: DISABLED
     Cacheable: NO
     SC: OFF
     SP: OFF
     Down state flush: ENABLED
     Appflow logging: ENABLED

1) Monitor Name: sslmon
     State: UP Weight: 1
     Probes: 1318 Failed [Total: 738 Current: 0]
     Last response: Success - HTTP response code 200 received.
     Response Time: 0.799 millisec
  Done
>
> show ssl service svc_k
          Advanced SSL configuration for Back-end SSL Service svc_k:
     DH: DISABLED
     Ephemeral RSA: DISABLED
     Session Reuse: ENABLED Timeout: 300 seconds
     Cipher Redirect: DISABLED
     SSLv2 Redirect: DISABLED
     Server Auth: DISABLED
     SSL Redirect: DISABLED
     Non FIPS Ciphers: DISABLED
     SNI: DISABLED
     SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
1) CertKey Name: ctest Client Certificate

1) Cipher Name: ALL
  Description: Predefined Cipher Alias
Done
```

Ciphers Supported by the NetScaler Appliance

Your NetScaler appliance ships with a predefined set of cipher groups. Table 1 lists the ciphers that are part of the DEFAULT cipher group and are therefore bound by default to an SSL virtual server. Table 2 lists the other ciphers currently supported by the NetScaler appliance. To use ciphers that are not part of the DEFAULT cipher group, you have to explicitly bind them to an SSL virtual server. You can also create a user-defined cipher group to bind to the SSL virtual server. For more information about creating a user-defined cipher group, see Configuring User-Defined Cipher Groups on the NetScaler Appliance.

Note:

- NetScaler MPX appliances support TLS protocol versions 1.1 and 1.2.
- Support for TLS protocol versions 1.1 and 1.2 is not available on a FIPS appliance or on a NetScaler virtual appliance.
- Support for TLS protocol versions 1.1 and 1.2 is available on an SDX appliance, but only on an instance-by-instance basis. To support TLS protocol versions 1.1 and 1.2 on an SDX appliance, you must assign at least one SSL chip to the instance when you provision it.

Table 1. Ciphers That the NetScaler Appliance Supports by Default

Cipher Suite	Protocol	Key Exchange Algorithm	Authentication Algorithm	Encryption Algorithm (Key Size)	Message Authentication Code (MAC) Algorithm
SSL3-RC4-MD5	SSLv3 TLSv1 TLSv1.1 TLSv1.2	RSA	RSA	RC4(128)	MD5
SSL3-RC4-SHA	SSLv3 TLSv1 TLSv1.1 TLSv1.2	RSA	RSA	RC4(128)	SHA1

SSL3-DES-CBC3-SHA	SSLv3 TLSv1 TLSv1.1 TLSv1.2	RSA	RSA	3DES(168)	SHA1
TLS1-AES-256-CBC-SHA	SSLv3 TLSv1 TLSv1.1 TLSv1.2	RSA	RSA	AES(256)	SHA1
TLS1-AES-128-CBC-SHA	SSLv3 TLSv1 TLSv1.1 TLSv1.2	RSA	RSA	AES(128)	SHA1
SSL3-EDH-DSS-DES-CBC3-SHA	SSLv3 TLSv1	DH	DSS	3DES(168)	SHA1
TLS1-DHE-DSS-RC4-SHA	TLSv1	DH	DSS	RC4(128)	SHA1
TLS1-DHE-DSS-AES-256-CBC-SHA	SSLv3 TLSv1	DH	DSS	AES(256)	SHA1
TLS1-DHE-DSS-AES-128-CBC-SHA	SSLv3 TLSv1	DH	DSS	AES(128)	SHA1
SSL3-EDH-RSA-DES-CBC3-SHA	SSLv3 TLSv1 TLSv1.1 TLSv1.2	DH	RSA	3DES(168)	SHA1
TLS1-DHE-RSA-AES-256-CBC-SHA	SSLv3 TLSv1 TLSv1.1 TLSv1.2	DH	RSA	AES(256)	SHA1

TLS1-DHE-RSA-AES-128-CBC-SHA	SSLv3 TLSv1 TLSv1.1 TLSv1.2	DH	RSA	AES(128)	SHA1

Table 2. Additional Ciphers Supported by the NetScaler Appliance

Cipher Suite	Protocol	Key Exchange Algorithm	Authentication Algorithm	Encryption Algorithm (Key Size)	Message Authentication Code (MAC) Algorithm
SSL3-DES-CBC-SHA	SSLv3 TLSv1 TLSv1.1	RSA	RSA	DES(56)	SHA1
TLS1-EXP1024-RC4-SHA	TLSv1	RSA(1024)	RSA	RC4(56)	SHA1 Export
SSL3-EXP-RC4-MD5	SSLv3 TLSv1	RSA(512)	RSA	RC4(40)	MD5 Export
SSL3-EXP-DES-CBC-SHA	SSLv3 TLSv1	RSA(512)	RSA	DES(40)	SHA1 Export
SSL3-EXP-RC2-CBC-MD5	SSLv3 TLSv1	RSA(512)	RSA	RC2(40)	MD5 Export
SSL2-RC4-MD5	SSLv2	RSA	RSA	RC4(128)	MD5
SSL2-DES-CBC3-MD5	SSLv2	RSA	RSA	3DES(168)	MD5
SSL2-RC2-CBC-MD5	SSLv2	RSA	RSA	RC2(128)	MD5
SSL2-DES-CBC-MD5	SSLv2	RSA	RSA	DES(56)	MD5
SSL2-RC4-64-MD5	SSLv2	RSA	RSA	RC4(64)	MD5
SSL2-EXP-RC4-MD5	SSLv2	RSA(512)	RSA	RC4(40)	MD5 Export
SSL3-EDH-DSS-DES-CBC-SHA	SSLv3 TLSv1	DH	DSS	DES(56)	SHA1
TLS1-EXP1024-DHE-DSS-DES-CBC-SHA	TLSv1	DH(1024)	DSS	DES(56)	SHA1 Export
TLS1-EXP1024-DHE-DSS-RC4- SHA	TLSv1	DH(1024)	DSS	RC4(56)	SHA1 Export
SSL3-EXP-EDH-DSS-DES-CBC-SHA	SSLv3 TLSv1	DH(512)	DSS	DES(40)	SHA1 Export

SSL3-EDH-RSA-DES-CBC-SHA	SSLv3 TLSv1 TLSv1.1	DH	RSA	DES(56)	SHA1
SSL3-EXP-EDH-RSA-DES-CBC-SHA	SSLv3 TLSv1	DH(512)	RSA	DES(40)	DES(40)
TLS1-EXP1024-RC4-MD5	TLSv1	RSA(1024)	RSA	RC4(56)	MD5 Export
TLS1-EXP1024-RC2-CBC-MD5	TLSv1	RSA(1024)	RSA	RC2(56)	MD5 Export
SSL2-EXP-RC2-CBC-MD5	SSLv2	RSA(512)	RSA	RC2(40)	MD5 Export
SSL3-ADH-RC4-MD5	SSLv3 TLSv1 TLSv1.1	DH	None	RC4(128)	MD5
SSL3-ADH-DES-CBC-SHA	SSLv3 TLSv1 TLSv1.1	DH	None	DES(56)	SHA1
SSL3-ADH-DES-CBC3-SHA	SSLv3 TLSv1 TLSv1.1	DH	None	3DES(168)	SHA1
TLS1-ADH-AES-128-CBC-SHA	SSLv3 TLSv1 TLSv1.1	DH	None	AES(128)	SHA1
TLS1-ADH-AES-256-CBC-SHA	SSLv3 TLSv1 TLSv1.1	DH	None	AES(256)	SHA1
SSL3-EXP-ADH-RC4-MD5	SSLv3 TLSv1	DH(512)	None	RC4(40)	MD5 Export
SSL3-EXP-ADH-DES-CBC-SHA	SSLv3 TLSv1	DH(512)	None	DES(40)	SHA1 Export

On a NetScaler platform that does not have N3 chips and is configured to negotiate EDH ciphers by using TLS version 1.0 with a DH key of 2048 bits, the SSL handshake fails in either of the following scenarios:

- Client authentication is enabled and the appliance receives a client certificate of 4096 bits.

- End-to-end encryption is configured and the appliance receives a server certificate of 4096 bits.

Use the show ns hardware command to find out if your appliance has N3 chips.

Example

```
> sh hardware
        Platform: NSMPX-22000 16*CPU+24*IX+12*E1K+2*E1K+4*CVM N3 2200100
        Manufactured on: 8/19/2013
        CPU: 2900MHZ
        Host Id: 1006665862
        Serial no: ENUK6298FT
        Encoded serial no: ENUK6298FT
 Done
```

FIPS

The Federal Information Processing Standard (FIPS), issued by the US National Institute of Standards and Technologies, specifies the security requirements for a cryptographic module used in a security system. The NetScaler FIPS appliance complies with the second version of this standard, FIPS-140-2.

Note: Henceforth, all references to FIPS imply FIPS-140-2.

The FIPS appliance is equipped with a tamper-proof (tamper-evident) cryptographic module—and a Cavium CN1620-NFBE3-2.0-G on the MPX 9700/10500/12500/15500 FIPS appliances—designed to comply with the FIPS 140-2 Level-2 specifications. The Critical Security Parameters (CSPs), primarily the server's private-key, are securely stored and generated inside the cryptographic module, also referred to as the Hardware Security Module (HSM). The CSPs are never accessed outside the boundaries of the HSM. Only the superuser (nsroot) can perform operations on the keys stored inside the HSM.

The following table summarizes the differences between standard NetScaler and NetScaler FIPS appliances.

Setting	NetScaler appliance	NetScaler FIPS appliance
Key storage	On the hard disk	On the FIPS card
Cipher support	All ciphers	FIPS approved ciphers
Accessing keys	From the hard disk	Not accessible

Configuring a FIPS appliance involves configuring the HSM immediately after completing the generic configuration process. You then create or import a FIPS key. After creating a FIPS key, you should export it for backup. You might also need to export a FIPS key so that you can import it to another appliance. For example, configuring FIPS appliances in a high availability (HA) setup requires transferring the FIPS key from the primary node to the secondary node immediately after completing the standard HA setup.

You can upgrade the firmware version on the FIPS card from version 4.6.0 to 4.6.1, and you can reset an HSM that has been locked to prevent unauthorized logon. Only FIPS approved ciphers are supported on a NetScaler FIPS appliance.

Configuring the HSM

Before you can configure the HSM of your NetScaler FIPS appliance, you must complete the initial hardware configuration. For more information, see Initial Configuration.

Configuring the HSM of your NetScaler FIPS appliance erases all existing data on the HSM. To configure the HSM, you must be logged on to the appliance as the superuser (nsroot account). The HSM is preconfigured with default values for the Security Officer (SO) password and User password, which you use to configure the HSM or reset a locked HSM.

Important: Do not perform the set ssl fips command without first resetting the FIPS card and restarting the MPX FIPS appliance.

Although the FIPS appliance can be used with the default password values, you should modify them before using it. The HSM can be configured only when you log on to the appliance as the superuser and specify the SO and User passwords.

Important: Due to security constraints, the appliance does not provide a means for retrieving the SO password. Store a copy of the password safely. Should you need to reinitialize the HSM, you will need to specify this password as the old SO password.

Before initializing the HSM, you can upgrade to the latest build of the software. To upgrade to the latest build, see Upgrading or Downgrading the System Software.

After upgrading, verify that the /nsconfig/fips directory has been successfully created on the appliance.

To configure the HSM on an MPX 9700/10500/12500/15500 FIPS appliances by using the command line interface

After logging on to the appliance as the superuser and completing the initial configuration, at the command prompt, type the following commands to configure the HSM and verify the configuration:

1. show ssl fips
2. reset ssl fips
3. reboot -warm
4. set ssl fips -initHSM `Level-2` <newSOpassword> <oldSOpassword> <userPassword> [-hsmLabel <string>]
5. save ns config
6. reboot -warm

7. show ssl fips

Example

```
show fips
FIPS Card is not configured
Done
reset fips
reboot
Are you sure you want to restart NetScaler (Y/N)? [N]:y
set ssl fips -initHSM Level-2 sopin12345 so12345 user123 -hsmLabel cavium
This command will erase all data on the FIPS card. You must save the configuration
(saveconfig) after executing this command.

Do you want to continue?(Y/N)y
Done
save ns config
reboot
Are you sure you want to restart NetScaler (Y/N)? [N]:y
show fips
      FIPS HSM Info:
HSM Label            : NetScaler FIPS
Initialization       : FIPS-140-2 Level-2
HSM Serial Number    : 2.1G1008-IC000021
HSM State            : 2

Firmware Version     : 1.1
Firmware Release Date  : Jun04,2010

Max FIPS Key Memory    : 3996
Free FIPS Key Memory   : 3994
Total SRAM Memory      : 467348
Free SRAM Memory       : 62564
Total Crypto Cores     : 3
Enabled Crypto Cores   : 1
Done
```

Parameters for configuring the HSM

initHSM

The FIPS initialization level. The appliance currently supports Level-2 (FIPS 140-2 Level-2). Possible value: Level 2.

hsmLabel

The label to identify the Hardware Security Module (HSM). Maximum Length: 31.

newSOpassword

The security officer password that will be in effect after you have configured the HSM. Maximum length on MPX 9700/10500/12500/15500 FIPS appliances: 14 characters.

oldSOpassword

The old security office password. Default on MPX 9700/10500/12500/15500 FIPS appliances: so12345.

userPassword

The user password. Default on MPX 9700/10500/12500/15500 FIPS appliances: user123. Maximum length on MPX 9700/10500/12500/15500 FIPS appliances: 14 characters.

To configure the HSM on an MPX 9700/10500/12500/15500 FIPS appliances by using the configuration utility

1. In the navigation pane, expand SSL, and then click FIPS. In the details pane, verify that the message "FIPS card is not configured" appears.
2. In the details pane, on the FIPS Infotab, click Reset FIPS.
3. In the navigation pane, click System.
4. In the details pane, click Reboot.
5. In the details pane, on the FIPS Info tab, click Initialize HSM.
6. In the Initialize HSM dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring the HSM” as shown:
   - Security Officer (SO) Password*—new SO password
   - Old SO Password*—old SO password
   - User Password*—user password
   - Level—initHSM (Currently set to Level2 and cannot be changed)
   - HSM Label—hsmLabel

   *A required parameter
7. Click OK.
8. In the details pane, click Save.
9. In the navigation pane, click System.
10. In the details pane, click Reboot.
11. Under FIPS HSM Info, verify that the information displayed for the FIPS HSM that you just configured is correct.

Creating and Transferring FIPS Keys

After configuring the HSM of your FIPS appliance, you are ready to create a FIPS key. The FIPS key is created in the appliance's HSM. You can then export the FIPS key to the appliance's CompactFlash card as a secured backup. Exporting the key also enables you to transfer it by copying it to the /flash of another appliance and then importing it into the HSM of that appliance.

Instead of creating a FIPS key, you can import an existing FIPS key or import an external key as a FIPS key. If you are adding a certificate-key pair of 2048 bits on the MPX 9700/10500/12500/15500 FIPS appliances, make sure that you have the correct certificate and key pair.

Note: If you are planning an HA setup, make sure that the FIPS appliances are configured in an HA setup before creating a FIPS key.

Creating a FIPS Key

Before creating a FIPS key, make sure that the HSM is configured.

To create a FIPS key by using the configuration utility

1. In the navigation pane, expand SSL, and then click FIPS.
2. In the details pane, on the FIPS Keys tab, click Add.
3. In the Create FIPS Key dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for Creating a FIPS Key” as shown:
   - FIPS Key Name*—fipsKeyName
   - Modulus*—modulus
   - Exponent*—exponent

   *A required parameter
4. Click Create, and then click Close.
5. On the FIPS Keys tab, verify that the settings displayed for the FIPS key that you just created are correct.

Parameters for Creating a FIPS Key

fipsKeyName

The object name for the FIPS key. Maximum Length: 31.

modulus

The modulus of the key to be created. The modulus value should be a multiple of 64. Possible values on MPX 9700/10500/12500/15500 FIPS appliances: 1024, 2048.

exponent

The exponent value for the key to be created. Possible values: 3 (Hex: 0x3), F4 (Hex: 0x00001). Default: 3.

To create a FIPS key by using the command line interface

At the command prompt, type the following commands to create a FIPS key and verify the settings:

- create ssl fipsKey <fipsKeyName> -modulus <positive_integer> [-exponent (3 | F4)]
- show ssl fipsKey [<fipsKeyName>]

Example

```
create fipskey Key-FIPS-1 -modulus 2048 -exponent 3
show ssl fipsKey Key-FIPS-1
FIPS Key Name: Key-FIPS-1 Modulus: 2048   Public Exponent: 3 (Hex: 0x3)
```

Exporting a FIPS Key

Citrix recommends that you create a backup of any key created in the FIPS HSM. If a key in the HSM is deleted, there is no way to create the same key again, and all the certificates associated with it are rendered useless.

In addition to exporting a key as a backup, you might need to export a key for transfer to another appliance.

The following procedure provides instructions on exporting a FIPS key to the /nsconfig/ssl folder on the appliance's CompactFlash and securing the exported key by using a strong asymmetric key encryption method.

To export a FIPS key by using the command line interface

At the command prompt, type:

export ssl fipsKey <fipsKeyName> -key <string>

Example

export fipskey Key-FIPS-1 -key Key-FIPS-1.key

Parameters for exporting a FIPS key

fipsKeyName

The name of the FIPS key to be exported. Maximum Length: 31.

key

The path and file name in which to store the exported key. Maximum Length: 63. Default path: /nsconfig/ssl/.

To export a FIPS key by using the configuration utility

1. In the navigation pane, expand SSL, and then click FIPS.
2. In the details pane, on the FIPS Keys tab, click Export.
3. In the Export FIPS key to a file dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for exporting a FIPS key” as shown:
   - FIPS Key Name*—fipsKeyName
   - File Name*—key (To put the file in a location other than the default, you can either specify the complete path or click the Browse button and navigate to a location.)

   *A required parameter
4. Click Export, and then click Close.

Importing an Existing FIPS Key

To use an existing FIPS key with your FIPS appliance, you need to transfer the FIPS key from the hard disk of the appliance into its HSM.

Note: To avoid errors when importing a FIPS key, make sure that the name of the key imported is the same as the original key name when it was created.

To import a FIPS key on the MPX 9700/10500/12500/15500 FIPS appliances by using the command line interface

At the command prompt, type the following commands to import a FIPS key and verify the settings:

- import ssl fipsKey <fipsKeyName> -key <string> -inform SIM -exponent (F4 | 3)
- show ssl fipskey <fipsKeyName>

Example

```
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform SIM -exponent F4
show ssl fipskey key-FIPS-2
FIPS Key Name: Key-FIPS-2 Modulus: 2048   Public Exponent: F4 (Hex value 0x10001)
```

Parameters for importing an existing FIPS key

fipsKeyName (FIPS Key Name)

The name of the FIPS key to be imported. Maximum Length: 31.

key (Key File Name)

The name of the key file. By default, the file is placed in the /nsconfig/ssl/ directory. If you want to put the file in a different location, include the complete path.

inform (Input Format)

The input format of the key file. Possible values:

- SIM—Secure Information Management; used when a FIPS key is imported.
- PEM—Privacy Enhanced Mail; used on the MPX 9700/10500/12500/15500 FIPS appliances when a non-FIPS key is imported.

Default: SIM

exponent (Exponent)

The exponent value for the FIPS key to be imported. Possible values: 3 and F4. Default: F4. The exponent is required only on the MPX 9700/10500/12500/15500 FIPS appliances.

To import a FIPS key by using the configuration utility

1. In the navigation pane, expand SSL, and then click FIPS.
2. In the details pane, on the FIPS Keys tab, click Import.
3. In the Import as a FIPS Key dialog box, select FIPS key file and set values for the following parameters:
   - FIPS Key Name*
   - Key File Name*—To put the file in a location other than the default, you can either specify the complete path or click Browse and navigate to a location.
   - Exponent*

   *A required parameter
4. Click Import, and then click Close.
5. On the FIPS Keys tab, verify that the settings displayed for the FIPS key that you just imported are correct.

Importing External Keys

In addition to transferring FIPS keys that are created within the NetScaler appliance's HSM, you can transfer external private keys (such as those created on a standard NetScaler, Apache, or IIS) to a FIPS NetScaler appliance. External keys are created outside the HSM, by using a tool such as OpenSSL. Before importing an external key into the HSM, copy it to the appliance's flash drive under /nsconfig/ssl.

Importing an external key as a FIPS key on the MPX 9700/10500/12500/15500 FIPS appliances by using the command line interface

On the MPX 9700/10500/12500/15500 FIPS appliances, the -exponent parameter in the import ssl fipskey command is not required while importing an external key. The correct public exponent is detected automatically when the key is imported, and the value of the -exponent parameter is ignored.

The NetScaler FIPS appliance does not support external keys with a public exponent other than 3 or F4.

You do not need a wrap key on the MPX 9700/10500/12500/15500 FIPS appliances.

You cannot import an external, encrypted FIPS key directly to an MPX 9700/10500/12500/15500 FIPS appliance. To import the key you need to first decrypt the key, and then import it. To decrypt the key, at the shell prompt, type:

```
openssl rsa -in <EncryptedKey.key> > <DecryptedKey.out>
```

To import an external key as a FIPS key to an MPX 9700/10500/12500/15500 FIPS appliance by using the command line interface

1. Copy the external key to the appliance's flash drive.
2. If the key is in .pfx format, you must first convert it to PEM format. At the command prompt, type:
   - convert ssl pkcs12 <output file> -import -pkcs12File <input .pfx file name> -password <password>
3. At the command prompt, type the following commands to import the external key as a FIPS key and verify the settings:
   - import ssl fipsKey <fipsKeyName> - key <string> - inform PEM
   - show ssl fipskey<fipsKeyName>

Example

```
convert ssl pkcs12 iis.pem -password 123456 -import -pkcs12File iis.pfx
import fipskey Key-FIPS-2 -key iis.pem -inform PEM
show ssl fipskey key-FIPS-2
FIPS Key Name: Key-FIPS-2 Modulus: 0   Public Exponent: F4 (Hex value 0x10001)
```

Note: The modulus is incorrectly displayed as zero in the above example. The discrepancy does not affect SSL functionality.

To import an external key as a FIPS key to an MPX 9700/10500/12500/15500 FIPS appliance by using the configuration utility

1. If the key is in .pfx format, you must first convert it to PEM format.
   a. In the navigation pane, click SSL.
   b. In the details pane, under Tools, click Import PKCS#12.
   c. In the Import PKCS12 File dialog box, set the following parameters:
      - Output File Name*
      - PKCS12 File Name*—Specify the .pfx file name.
      - Import Password*
      - Encoding Format

      *A required parameter
2. In the navigation pane, expand SSL, and then click FIPS.
3. In the details pane, on the FIPS Keys tab, click Import.
4. In the Import as a FIPS Key dialog box, select PEM file, and set values for the following parameters:
   - FIPS Key Name*
   - Key File Name*—To put the file in a location other than the default, you can either specify the complete path or click Browse and navigate to a location.

   *A required parameter
5. Click Import, and then click Close.
6. On the FIPS Keys tab, verify that the settings displayed for the FIPS key that you just imported are correct.

Configuring FIPS Appliances in a High Availability Setup

You can configure two appliances in a high availability (HA) pair as FIPS appliances. For information about configuring an HA setup, see High Availability.

Note: Citrix recommends that you use the configuration utility (GUI) for this procedure. If you use the command line (CLI), make sure that you carefully follow the steps as listed in the procedure. Changing the order of steps or specifying an incorrect input file might cause inconsistency that requires that the appliance be restarted. In addition, if you use the CLI, the create ssl fipskey command is not propagated to the secondary node. When you execute the command with the same input values for modulus size and exponent on two different FIPS appliances, the keys generated are not identical. You have to create the FIPS key on one of the nodes and then transfer it to the other node. But if you use the configuration utility to configure FIPS appliances in an HA setup, the FIPS key that you create is automatically transferred to the secondary node. The process of managing and transferring the FIPS keys is known as secure information management (SIM).

Important: On the MPX 9700/10500/12500/15500 FIPS appliances, the HA setup should be completed within six minutes. If the process takes longer than six minutes, the internal timer of the FIPS card expires and the following error message appears:

ERROR: Operation timed out or repeated, please wait for 10 mins and redo the SIM/HA configuration steps.

If this message appears, restart the appliance or wait for 10 minutes, and then repeat the HA setup procedure.

In the following procedure, appliance A is the primary node and appliance B is the secondary node.

To configure FIPS appliances in a high availability setup by using the command line interface

1. **On appliance A**, open an SSH connection to the appliance by using an SSH client, such as PuTTY.
2. Log on to the appliance, using the administrator credentials.
3. Initialize appliance A as the source appliance. At the command prompt, type:

   init ssl fipsSIMsource <certFile>
4. Copy this <certFile> file to appliance B, in the /nconfig/ssl folder.
5. **On appliance B**, open an SSH connection to the appliance by using an SSH client, such as PuTTY.
6. Log on to the appliance, using the administrator credentials.
7. Initialize appliance B as the target appliance. At the command prompt, type:

   init ssl fipsSIMtarget <certFile> <keyVector> <targetSecret>
8. Copy this <targetSecret> file to appliance A.
9. **On appliance A**, enable appliance A as the source appliance. At the command prompt, type:

   enable ssl fipsSIMSource <targetSecret> <sourceSecret>
10. Copy this <sourceSecret> file to appliance B.
11. **On appliance B**, enable appliance B as the target appliance. At the command prompt, type:

    enable ssl fipsSIMtarget <keyVector> <sourceSecret>
12. **On appliance A**, create a FIPS key, as described in Creating a FIPS Key.
13. Export the FIPS key to the appliance's hard disk, as described in Exporting a FIPS Key.
14. Copy the FIPS key to the hard disk of the secondary appliance by using a secure file transfer utility, such as SCP.
15. **On appliance B**, import the FIPS key from the hard disk into the HSM of the appliance, as described in Importing an Existing FIPS Key.

To configure FIPS appliances in a high availability setup by using the configuration utility

1. On the appliance to be configured as the source appliance, in the navigation pane, expand SSL, and then click FIPS.
2. In the details pane, on the FIPS Info tab, click Enable SIM.
3. In the Enable HA Pair for SIM dialog box, in the Certificate File Name text box, type the file name, with the path to the location at which the FIPS certificate should be stored on the source appliance.
4. In the Key Vector File Name text box, type the file name, with the path to the location at which the FIPS key vector should be stored on the source appliance.
5. In the Target Secret File Name text box, type the location for storing the secret data on the target appliance.
6. In the Source Secret File Name text box, type the location for storing the secret data on the source appliance.
7. Click OK. The FIPS appliances are now configured in HA mode.
8. Create a FIPS key, as described in Creating a FIPS Key. The FIPS key is automatically transferred from the primary to the secondary.

Example

In the following example, source.cert is the certificate on the source appliance, stored in the default directory, /nsconfig/ssl. This certificate must be transferred to the same location (/nsconfig/ssl) on the target appliance. The file target.secret is created on the target appliance and copied to the source appliance. The file source.secret is created on the source appliance and copied to the target appliance.

On the source appliance

```
init fipsSIMsource /nsconfig/ssl/source.cert
```

On the target appliance

```
init fipsSIMtarget /nsconfig/ssl/source.cert /nsconfig/ssl/target.key /nsconfig/ssl/target.secret
```

On the source appliance

```
enable fipsSIMsource /nsconfig/ssl/target.secret /nsconfig/ssl/source.secret
```

On the target appliance

```
enable fipsSIMtarget /nsconfig/ssl/target.key /nsconfig/ssl/source.secret
```

On the source appliance

```
create ssl fipskey fips1 -modulus 2048 -exponent f4
export fipskey fips1 -key /nsconfig/ssl/fips1.key
```

Copy this key into the hard disk of the target appliance.

On the target appliance

```
import fipskey fips1 -key /nsconfig/ssl/fips1.key
```

The following diagram summarizes the transfer process.

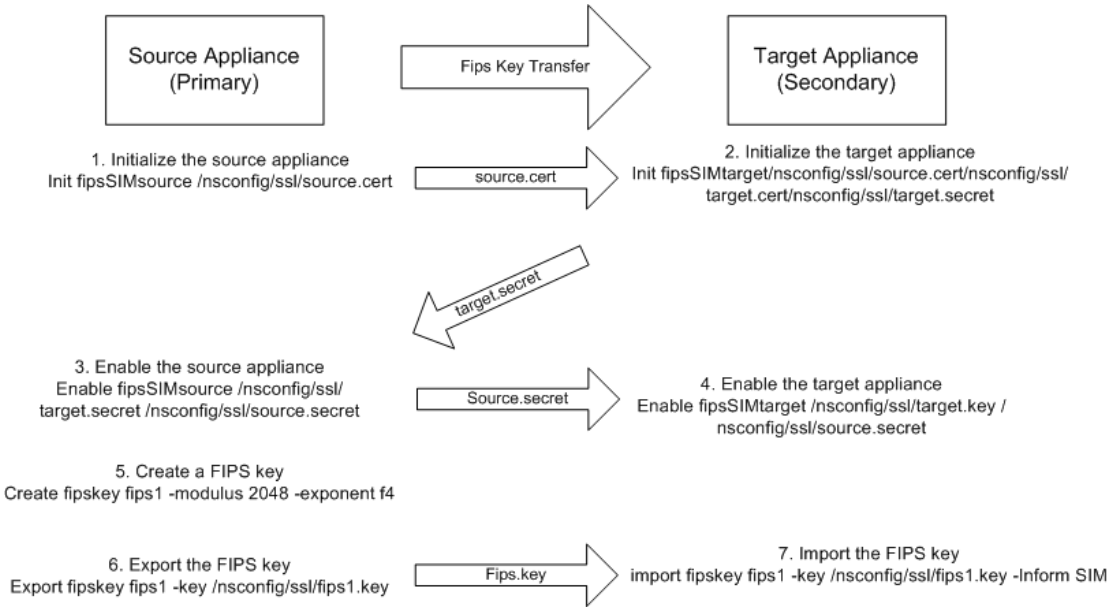


Figure 1. Transferring the FIPS Key-Summary

Resetting a Locked HSM

The HSM becomes locked (no longer operational) if you change the SO password, restart the appliance without saving the configuration, and make three unsuccessful attempts to change the password. This is a security measure for preventing unauthorized access attempts and changes to the HSM settings.

Important: To avoid this situation, save the configuration after initializing the HSM.

If the HSM is locked, you must reset the HSM and restart the appliance to restore the default passwords. You can then use the default passwords to access the HSM and configure it with new passwords. When finished, you must save the configuration and restart the appliance.

Caution: Do not reset the HSM unless it has become locked.

To reset a locked HSM by using the command line interface

At the command prompt, type the following commands to reset and re-initialize a locked HSM:

- reset ssl fips
- reboot -warm
- set ssl fips -initHSM `Level-2` <new SO password> <old SO password> <user password> [-hsmLabel <string>]
- save ns config
- reboot -warm

Example

```
reset fips
reboot -warm
set fips -initHSM Level-2 newsopin123 sopin123 userpin123 -hsmLabel NSFIPS
saveconfig
reboot -warm
```

Note: The SO and User passwords are the default passwords.

To reset a locked HSM by using the configuration utility

1. In the navigation pane, expand SSL, and then click FIPS.
2. In the details pane, on the FIPS Info tab, click Reset FIPS.
3. Configure the HSM, as described in Configuring the HSM.
4. In the details pane, click Save.

FIPS Approved Algorithms and Ciphers

The FIPS approved algorithms are:

Key-Exchange algorithms

- RSA

Cipher algorithms

- SSL3-DES-CBC3-SHA
- TLS1-AES-256-CBC-SHA
- TLS1-AES-128-CBC-SHA

Note: RC4 (ARC4) is not a FIPS-approved algorithm.

SSL virtual server is marked UP only when default ciphers (FIPS) are configured.

NetScaler Web 2.0 Push

Modern web applications, also referred to as web 2.0 applications, provide highly responsive interfaces that generate asynchronous updates that can impose an additional load on a server. Typically, asynchronous notifications are sent by using HTTP and server push techniques, such as long-polling and streaming response, which enable servers to push the notifications to clients. These techniques require the servers to maintain a large number of TCP/IP connections, which provides low latency but results in low bandwidth. As the number of clients increases, the servers are overloaded with connections kept open for each client. Further, the large number of connections terminating on the server requires kernel resources and memory for data structures like protocol control blocks, socket descriptors, and socket buffers.

With the NetScaler Web 2.0 push feature, you can use the NetScaler appliance as a proxy server to offload long-lived client TCP connections and maintain relatively fewer, reusable connections to the server. NetScaler Web 2.0 push is application agnostic, with the flexibility to work seamlessly with various technologies and configurations used for asynchronous messaging. It can be extended to co-exist with developing technologies, and it preserves backward compatibility. NetScaler Web 2.0 Push is also scalable, with support for multiple NetScaler appliances.

With the NetScaler Web 2.0 push feature, the NetScaler appliance multiplexes and manages the exchange of data reliably and securely, reducing the number of server-side connections across potentially millions of persistent client connections. For every HTTP, HTTPS, or SSL transaction, the appliance can de-link and rebalance the server farm to distribute client requests across multiple servers.

The NetScaler Web 2.0 Push feature reduces the number of server-side connections across millions of persistent client connections.

Web 2.0 Push Applications

With modern Web applications, termed broadly as Web 2.0 applications, servers use AJAX technologies such as polling to maintain up-to-date information about the client. Polling enables an AJAX application to periodically poll the server for updates. For example, a chat based application can poll a Web server every 10 seconds for any chat updates. To get such updates from the Web server, the client browser periodically opens a connection to the Web server.

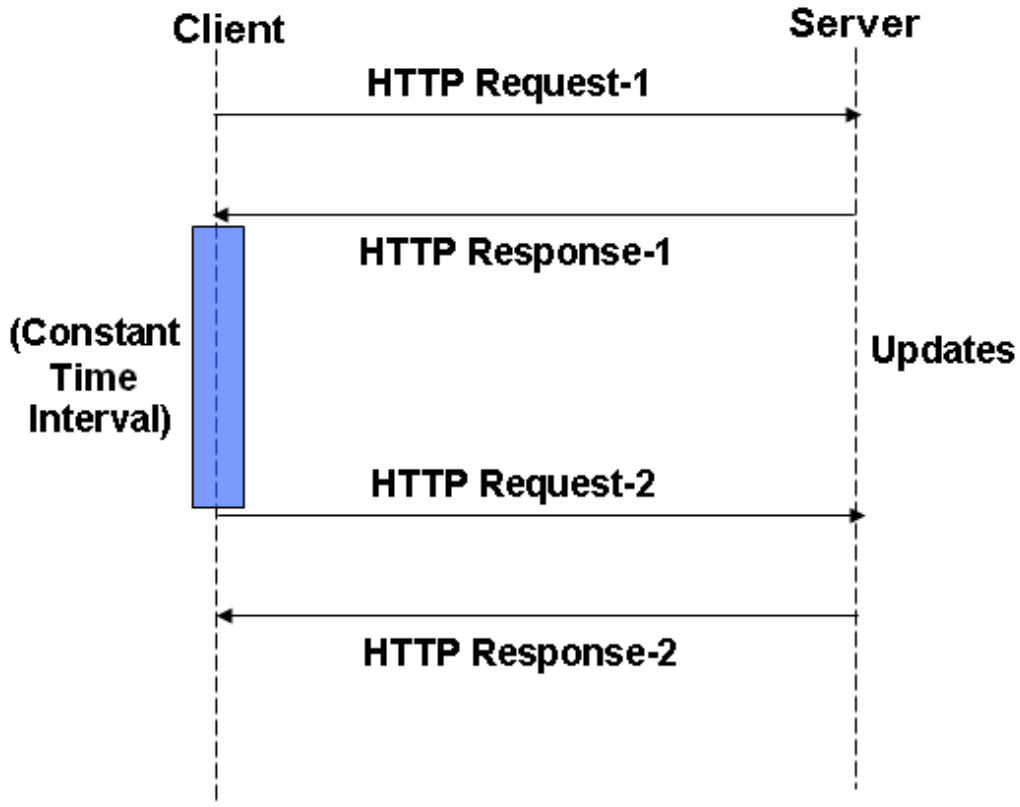


Figure 1. Polling Technique

Such frequent polling can overload the server. Also, if you deploy the AJAX application on a Web server with low resources and a large number of simultaneous users poll the server for updates, the network can become saturated, with significant degradation in the server performance. And if there is no update from the server, the client requests overload the server for a void response.

To avoid such problems, server push technology often uses a long polling technique. Long polling enables the client application to open a persistent connection to the server and wait for the server to push updates when available.

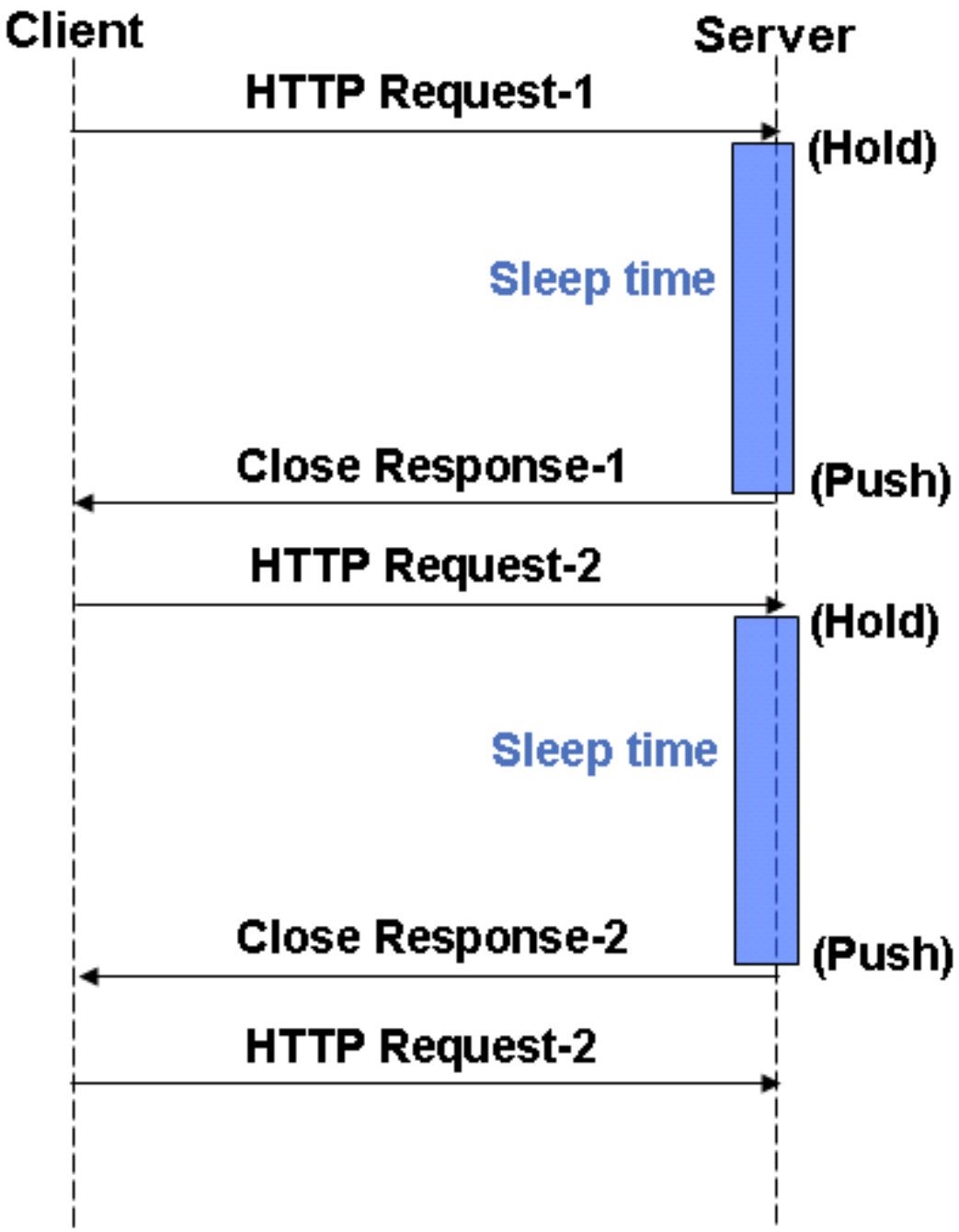


Figure 2. Long Polling Technique

If your server supports asynchronous request processing, long polling is a scalable technique. However, long polling can hold the server connections until updates are available. For example, if 1,000 AJAX applications open one long polled connection, 1,000 threads hold the server while waiting for updates.

Another technique, called HTTP streaming, is identical to the long polling technique except that the connection is not closed after the server pushes the updates. The AJAX application sends a single request and receives chunks of responses (partial responses) over the same connection. With HTTP streaming, the browsers and server do not open or close the connection. Therefore, HTTP streaming significantly reduces the network latency.

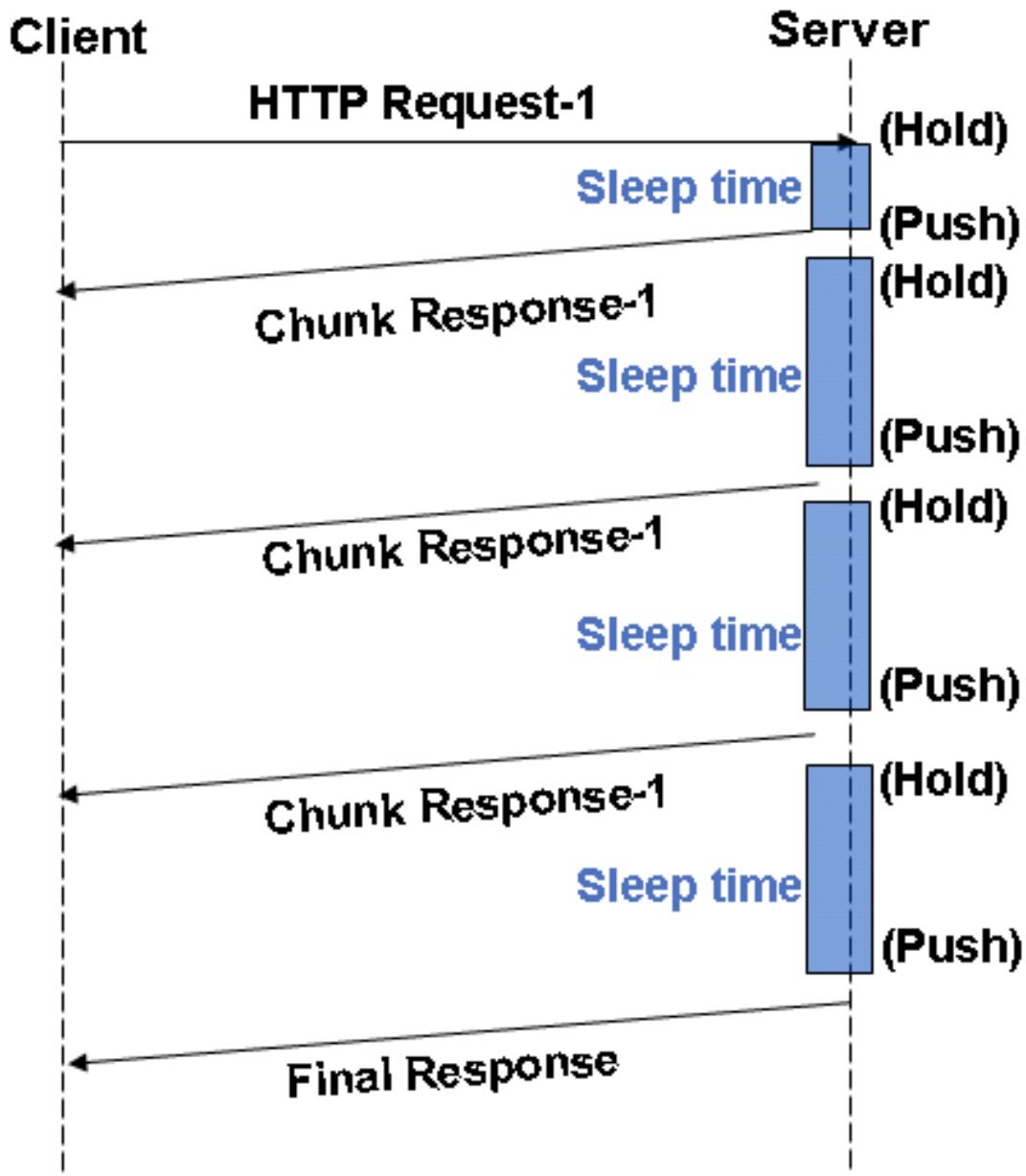


Figure 3. HTTP Streaming Technique

In HTTP streaming, as in long polling techniques, if the server frequently pushes updates, the performance of the network and the AJAX applications are significantly degraded and the client may lose the updates. If your AJAX application opens both long polling and HTTP streaming connections to the same Web server, other AJAX applications cannot open connections to the server, because the browser blocks such connections.

NetScaler Web 2.0 push uses connection labeling to overcome the limitations of long polling and HTTP streaming.

How Web 2.0 Push Works

The NetScaler Web 2.0 push feature enables the server to label a client connection and subsequently identify and send data over that labeled connection. With NetScaler Web 2.0 push enabled, the client first establishes a TCP/IP connection and connects to the NetScaler appliance. The appliance uses the configured load balancing method or content switching policy to select a Web server to which to open a connection and send the client request. The server interacts with the client and uses either authentication or a previously established cookie to identify the client.

When the NetScaler appliance receives a request with push enabled, it initiates the labeling protocol with the Web server. This protocol enables the Web server to label the connection and defer the response. The protocol also enables the server to process other requests without invoking push processing. The Web server (referred to as a *notification server*) uses the label to send updates to the client through the NetScaler appliance when the updates become available. Servers can choose to push multiple updates over a single TCP connection or open one connection per update.

Note: The set of Web servers that respond to requests from the NetScaler does not necessarily include the notification servers that push updates to client.

A central component of a NetScaler Web 2.0 push configuration is a push virtual server, which is a load balancing virtual server with service type PUSH or SSL_PUSH. The NetScaler appliance uses the push virtual server to expose the message push protocol to the Web servers. A server uses the protocol to push asynchronous messages to connected clients. A push virtual server exposes a simple REST interface for posting updates.

Important: For the NetScaler Web 2.0 Push feature to work correctly, you must configure the NetScaler appliance as a proxy for the traffic between the clients and servers. You can use multiple NetScaler appliances to scale up your connection management.

For each transaction, the NetScaler Web 2.0 push feature maintains a state machine, which manages the actions of the transaction. The state machine has the following states:

- Waiting for Request State (Q)-A connection has been established between the client and the NetScaler appliance. The appliance waits in this state until the client sends a request.
- Waiting for Server Response State (R) -A request has been received from the client and forwarded to a Web server. The appliance waits in this state for the server to respond.
- Waiting for Asynchronous Messages State (A) -The appliance is waiting for asynchronous messages that the notification servers push to the push virtual server.

Until the client establishes a connection with the NetScaler appliance's load balancing or content switching virtual server, the initial state of the transaction is Q. When the appliance receives a request, it forwards the request to the server, and the transaction moves to state R.

If the appliance receives a deferred response (also called a *labeled response*), the transaction moves to state A. In this state, if the appliance receives a push message through the message push protocol, it processes the message and forwards the message to

the client. If this message is marked as the last message, the appliance closes the transaction and moves to state Q. If not, the transaction remains in state A.

The push virtual server can manage long-polling and streaming responses from the server. Each update that the server sends to the push virtual server has a flag (with query parameters) that indicates whether there are updates from the server. When the flag indicates that the updates from the server are unavailable, the NetScaler appliance performs one of the following functions:

1. If the client uses HTTP 1.1 protocol and multiple updates are received from the server, the appliance sends a chunked response to the client and appends a zero chunk to the final response. If the first response itself has the flag set, the content length itself is sent as the response.

2. If the client uses HTTP 1.0 protocol and multiple updates are received from the server, then just the contents of the chunked response or the body of the content length response is sent to the client and the connection is terminated. If the first response itself has the flag set then, the content length itself is sent as the response.

The appliance sends a content-length response regardless of which HTTP version the client uses. The connection-labeling and message-push protocols, which identify the client and the server connections, provide the basic functionality of the NetScaler Web 2.0 push feature.

Understanding NetScaler Web 2.0 Push Protocol

For the NetScaler Web 2.0 Push feature to work correctly, the NetScaler appliance must label the client connection and then identify and send the deferred response from the server over the labeled connection. For this purpose, the Web 2.0 push feature uses the connection labeling and the message push protocols.

Connection Labeling Protocol

The connection labeling protocol is used between the server and the NetScaler appliance to label the client connection. After a label is negotiated, the Web server includes the label in the update that is sent to the client.

The appliance forwards a request to the server after adding an X-NS-PUSHVSERVER header containing the IP address and port of the push virtual server. The server either responds to this request with an HTTP response or defers the response. If the server defers the response, it labels the connection with an X-NS-DEFERRABLE header, which indicates that the connection is deferred.

A policy configured on the load balancing or content switching virtual server enables the NetScaler appliance to extract the label from the response. The appliance uses the information in the label to send the push message (update) to the push virtual server, which sends the response on the corresponding client connection.

Note: For any update from the Web server, the NetScaler does not support rewrite and compression.

When a server receives a request that it is deferrable, it sends an HTTP 200 OK response with the X-NS-DEFERRABLE header, which indicates to the NetScaler appliance that the push feature should be applied to the request. The appliance removes the X¤NS-DEFERRABLE header, sends the response to the client, and waits for updates. For example:

```
HTTP/1.1 200 OK
Date: Wed, 25 Aug 2010 18:22:47 GMT
Server: Apache/2.0.61 (FreeBSD) PHP/5.2.5 with Suhosin-Patch mod_ssl/2.0.61
OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
X-NS-DEFERRABLE: YES
X-NS-SERVERLABEL: 04c2442bcb7c4b5f826d41a623e374e!
Content-Length: 0
Content-Type: text/plain;charset=UTF-8
```

Message Push Protocol

The message push protocol is used between a notification server and the NetScaler appliance to enable the notification server to send a notification to a previously labeled client connection.

Web servers use the message push protocol to push asynchronous messages to connected clients. The push protocol is built as a REST interface, exposed through the push virtual server on the NetScaler appliance. The server connects to the push virtual server and sends a request to the appliance. The BODY of the request contains the payload to be sent to the client. Additionally, the request identifies the label for the target client connection and the last message of the response.

When the NetScaler appliance receives the deferred response from the server, it sends the response to the client as a single HTTP chunk and sends a 200 OK response with the XML information to the server. If the message is marked as the last message of the response, the NetScaler also closes the HTTP response on the server.

Note: If the NetScaler is aware of the content length, it may send a response specifying the Content-Length, instead of a chunk. This enables the NetScaler to manage both HTTP streaming and long-polling responses.

Notification from Server to Push Server

```
POST /CLIENT/V10/04c2442bcb7c4b5f826d41a623e374e!?MSG_END=0  HTTP/1.1
Host: 10.102.80.66:8080
Content-Length: 6
```

Response from Push vserver to the server

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset="UTF-8"
Content-Length: 130
<?xml version="1.0" encoding="UTF-8"?>
<CLIENTINFO>
  <CLIENT ID="04c2442bcb7c4b5f826d41a623e374e!" INFO="SUCCESS" />
</CLIENTINFO>
```

Configuring Web 2.0 Push

To configure NetScaler Web 2.0 push, you must first enable the feature. Then, create a push virtual server and associate it with a load balancing or content switching virtual server. Once you have a working configuration, you can customize it to suit your deployment.

You can also monitor the Web 2.0 push configuration by viewing statistics about the push virtual server and the other entities, such as the load balancing or the content switching virtual servers, that are part of the configuration.

Enabling NetScaler Web 2.0 Push

You have to enable the NetScaler Web 2.0 push feature before you can use it. Before enabling the feature, you must have the appropriate license installed on the NetScaler appliance. With the feature disabled, you can configure NetScaler Web 2.0 push entities, such as the push virtual server, but the entities will not work until the feature is enabled.

To enable NetScaler Web 2.0 push by using the command line interface

At the command prompt, type:

enable ns feature push

If NetScaler Web 2.0 Push is not licensed or disabled, the push virtual server state is DOWN.

To enable NetScaler Web 2.0 Push by using the configuration utility

1. In the navigation pane, expand System, and then click Settings.
2. In the details pane, under Modes and Features, click Change advanced features.
3. In the Configure advanced features dialog box, select the NetScaler Push check box, and then click OK.
4. At the Enable/Disable Feature(s)? prompt, click Yes.

Creating a NetScaler Web 2.0 Push Virtual Server

A push virtual server enables the NetScaler appliance to multiplex and manage the exchange of data (server push) reliably, securely, and in a scalable manner. It enables the notification server to send a notification to a previously labeled client connection by using the message push protocol. The notification servers push the out-of-band updates to the push virtual server. When the clients access the load balancing or the content switching virtual servers, the push virtual server uses the labeling protocol to label the deferred clients.

You can add, modify, and remove push virtual servers, however, you cannot bind services to the push virtual server.

To create a NetScaler Web 2.0 Push virtual server by using the command line interface

At a command prompt, type the following commands to create a push virtual server and verify the configuration:

- add lb vserver <name> <serviceType> <IPAddress> <Port>
- show lb vserver <name>

Example

```
add lb vserver Vserver-Push-1 PUSH 10.102.29.162 80
show lb vserver Vserver-Push-1
```

Parameters for creating a push virtual server

name

The name of the push virtual server being created. This alphanumeric string is required and cannot be changed after the virtual server is created. Must not exceed 127 characters, and leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

IPAddress

The IP address of the push virtual server being configured. This is a mandatory parameter.

serviceType

The type of data transferred between the NetScaler appliance and the client. SSL_PUSH service type encrypts the traffic between the NetScaler and the client. Use PUSH service type for HTTP requests. Possible values: PUSH, SSL_PUSH.

Note: For an SSL_PUSH virtual server, you need to bind a certificate-key pair. For details about binding a certificate-key pair to the virtual server, see SSL Offload and Acceleration.

port

The TCP port on which the virtual server listens. This is a mandatory argument. Must be a positive number not greater than 65535. Minimum value: 1.

To create a NetScaler Web 2.0 Push virtual server by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, click Add.
3. In the Name, Port, and IP Address text boxes, type a name for the push virtual server, a port, and an IP address (for example, **Vserver-Push-1**, **80**, and **10.102.29.162**).
4. In Protocol, select either SSL_PUSH or PUSH.
5. Click Create, and then click Close. The push virtual server you created appears in the Load Balancing Virtual Servers pane.

To remove a push virtual server, use the rm lb vserver command that takes only the name parameter.

Configuring a Load Balancing or Content Switching Virtual Server

After creating a push virtual server, you need to associate it with the load balancing or content switching virtual servers. For details about creating a load balancing virtual server, see "Creating a Virtual Server." Also, for details about creating a content switching setup, see "Creating Content Switching Virtual Servers."

Once you have created the load balancing or content switching virtual servers, you must associate them with the push virtual server.

To configure a load balancing virtual server or content switching virtual server for NetScaler Web 2.0 push by using the command line interface

At the command prompt, type the following commands to configure a load balancing virtual server for NetScaler Web 2.0 push. To configure a content switching virtual server, replace set lb vserver with set cs vserver.

set lb vserver <name> <ServiceType> <IPAddress> <Port> -push (ENABLED | DISABLED) -pushVserver <PushVservername> -pushLabel <Expression> -pushMultiClients (YES | NO)

Examples

set lb vserver Vserver-LB-1 HTTP 10.102.29.161 80 -push ENABLED - pushVserver PushVserver1 -pushLabel "H

set cs vserver Vserver-CS-1 HTTP 10.102.29.161 80 -push ENABLED - pushVserver PushVserver1 -pushLabel "H

To modify or remove a load balancing or content switching virtual server by using the command line interface

- To modify a virtual server, type the set lb vserver or set cs vserver command, the name of the virtual server, and the parameters to be changed, with their new values.
- To remove a virtual server, type the rm lb vserver or rm cs vserver command and the name of the load balancing or content switching virtual server.

Parameters for configuring a load balancing virtual server

push

Enable the NetScaler appliance to process traffic with the push virtual server. Possible values: ENABLED, DISABLED. Default: DISABLED

pushVserver

The name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the client-facing load balancing virtual server.

pushLabel

An expression for extracting the label from the response from server. The string can be either an existing rule name (configured by using the add rule command) or an in-line expression with a maximum of 64 characters. Default value: NONE.

pushMultiClients

Allow multiple Web 2.0 connections from the same client to connect to the virtual server and expect updates. Possible values: YES, NO. Default value: NO.

To create a load balancing virtual server for NetScaler Web 2.0 Push by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure push virtual server (for example, Vserver-LB-1), and click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, on the Advanced tab, click the arrow next to Push to expand it. Then, in the Push VServer list, select the push virtual server and click OK.

   Note: To create a content switching virtual server for NetScaler Web 2.0 Push by using the configuration utility, in the navigation pane, expand Content Switching, click Virtual Servers, Then, perform steps 2 and 3.

Monitoring the Configuration

To monitor the NetScaler Web 2.0 push configuration, you need to view the statistics of the push virtual servers and load balancing entities. This is useful for troubleshooting.

For instructions on how to display statistics of load balancing entities, see "Load Balancing." Available statistics include labeled connections, push labeled connections, and deferred requests.

To view the properties of the push virtual server by using the command line interface

At the command prompt, type:

show lb vserver <PushVserverName>

Example

show lb vserver Vserver-Push-1

Customizing the NetScaler Web 2.0 Push Configuration

Once your basic Web 2.0 Push configuration is operational, you can customize it by setting a time-out value for idle client connections and configuring URL redirects.

Setting a Time-out Value for Idle Client Connections

Once a client connects to the push virtual server, you can configure the virtual server to close any idle client connections after a configured time period.

To configure a time-out value, use the cltTimeout parameter, which specifies the time, in seconds, after which the NetScaler appliance closes any idle client connections. The default value is 180sec for HTTP/SSL-based services and 9000sec for TCP-based services.

To set a time out value for idle client connections by using the command line interface

At the command prompt, type:

set lb vserver <PushVserverName> [-cltTimeout <secs>]

Example

```
set lb vserver Vserver-Push-1 -cltTimeout 100
```

To set a time-out value for idle client connections by using the configuration utility

1. In the navigation pane, expand Load Balancing and click Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure virtual server port insertion (for example, **Vserver-Push-1**), and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, click the Advanced tab.
4. In the Client Time-out (secs) text box, type the timeout value (for example, **100**).
5. Click OK.

Redirecting Client Requests to an Alternative URL

You can configure a URL to which to redirect HTTP or HTTPS client requests when the push virtual server is down or disabled. This URL can be a local or a remote link. The NetScaler appliance uses HTTP 302 redirect to redirect client requests.

Redirects can be absolute URLs or relative URLs. If the configured redirect URL contains an absolute URL, the HTTP redirect is sent to the configured location, regardless of the URL specified in the incoming HTTP request. If the configured redirect URL contains only a domain name (relative URL), the incoming URL is appended to the domain configured in the redirect URL.

The domain specified in the redirect URL must not be the same as the domain specified in the domain name argument of a content switching policy. If the same domain is specified in both arguments, the request is redirected continuously to the same unavailable virtual server in the NetScaler appliance, and the user cannot get the requested content.

To configure a virtual server to redirect the client request to a URL by using the command line interface

At the command prompt, type:

set lb vserver <name> -redirectURL URLValue

Example

set lb vserver Vserver-Push-1 -redirectURL http://www.newdomain.com/mysite/maintenance

To configure a virtual server to redirect the client request to a URL by using the configuration utility

1. In the navigation pane, expand Load Balancing, and then click Virtual Servers.
2. In the details pane, select the push virtual server for which you want to configure redirect URL (for example, Vserver-Push-1), and then click Open.
3. On the Advanced tab, in the Redirect URL text box, type the URL (for example, **http://www.newdomain.com/mysite/maintenance**).
4. Click OK.

Reference Material

2015-05-18 16:58:51 UTC

Contents

Reference Material

You can refer to the following documentation for quick reference:

- Command Reference
- Documentation Library

Note: We are in the process of transitioning reference documentation to Citrix eDocs. The following reference documentation is available in Citrix Knowledge Center (http://support.citrix.com/productdocs/). When you click these links, you will leave the site. We recommend that you book mark this site so you can easily return to it.

- NetScaler Developer's Guide
- NetScaler Log Message Reference
- NetScaler SNMP OID Reference
- NetScaler Glossary

Command Reference

Provides basic information of the NetScaler command line interface and also provides the commands to configure and retrieve details of the appliance.

Command Reference

Provides basic information of the NetScaler command line interface and also provides the commands to configure and retrieve details of the appliance.

AAA Commands

This group of commands can be used to perform operations on the following entities:

- aaa
- aaa user
- aaa group
- aaa preauthenticationaction
- aaa preauthenticationpolicy
- aaa stats
- aaa session
- aaa radiusParams
- aaa ldapParams
- aaa tacacsParams
- aaa certParams
- aaa parameter
- aaa preauthenticationparameter
- aaa global

aaa

stat aaa

Synopsis

stat aaa [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display aaa statistics

aaa user

[add | rm | set | bind | unbind | show]

add aaa user

Synopsis

add aaa user <userName> {-password }

Description

Add an AAA user.

Parameters

userName

The name of the user.

password

Enter this keyword to create or change the user's password. The entered password is not displayed. If no password is given for a new user then the user will be authenticated externally.

Example

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

Top

rm aaa user

Synopsis

rm aaa user <userName>

Description

Remove the AAA user.

Parameters

userName

The name of the AAA user.

Top

set aaa user

Synopsis

set aaa user <userName>

Description

Modify the parameters for the existing AAA user.

Parameters

userName

The name of the user.

password

Enter this keyword to create or change the user's password. The entered password is not displayed. If no password is given for a new user then the user will be authenticated externally.

Example

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

Top

bind aaa user

Synopsis

bind aaa user <userName> [-policy <string> [-priority <positive_integer>]]
[-intranetApplication <string>] [-urlName <string>] [-intranetIP <ip_addr> [<netmask>]]

Description

Bind the resources (policy/intranetip/intranetapplication/url) to a user.

Parameters

userName

The user name.

policy

the policy to be bound to aaa user.

intranetApplication

The intranet vpn application.

urlName

The intranet url

intranetIP

The IP address to be bound to this user and used to access the Intranet

Example

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

Top

unbind aaa user

Synopsis

unbind aaa user <userName> [-policy <string>] [-intranetApplication <string>] [-urlName <string>] [-intranetIP <ip_addr> [<netmask>]]

Description

Unbind the resource(policy/intranetip/intranetapplication/url) from an AAA user

Parameters

userName

The user name.

policy

The policy to be unbound to an aaa user.

intranetApplication

The intranet vpn application.

urlName

The intranet url

intranetIP

The Intranet IP to be unbound

Example

unbind AAA user joe -intranetip 10.102.1.123

Top

show aaa user

Synopsis

show aaa user [<userName>] [-loggedIn]

Description

Display the AAA user detail.

Parameters

userName

The user name.

loggedIn

The loggedin flag. When this flag is turned on, the system displays the names of all logged-in users. If a user name is included, the system displays whether the user is logged in or not.

Example

Example
> show aaa user joe
UserName: joe IntranetIP: 10.102.1.123

```
        Bound to groups:
                GroupName: engg
 Done
>
```

Top

aaa group

[add | rm | bind | unbind | show]

add aaa group

Synopsis

add aaa group <groupName>

Description

Add an AAA group. To associate AAA users with an AAA group, use the command "bind AAA group ... -username ...". You can bind different policies to each AAA group. Use the command "bind AAA group ... -policy ...". You can also bind ranges of Intranet IP addresses to an AAA group. For example, the administrator may want to assign pools of Intranet IP addresses to groups or departments.

Parameters

groupName

The name of the group.

Example

add aaa group group_ad

Top

rm aaa group

Synopsis

rm aaa group <groupName>

Description

Remove an AAA group. To associate AAA users with an AAA group, use the command "bind AAA group ... -username ...". You can bind different policies to each AAA group. Use the command "bind AAA group ... -policy ...". You can also bind ranges of Intranet IP addresses to an AAA group. For example, the administrator may want to assign pools of Intranet IP addresses to groups or departments.

Parameters

groupName

The name of the group . Note: Any user sessions belonging to the group are removed. The user must log in again.

Top

bind aaa group

Synopsis

bind aaa group <groupName> [-userName <string>] [-policy <string> [-priority <positive_integer>]] [-intranetApplication <string>] [-urlName <string>] [-intranetIP <ip_addr> <netmask>]

Description

Bind the resource(User/Intranet IP /Policy/Intranet Application) to a group. To associate AAA users with an AAA group, use the command "bind AAA group ... -username ...". You can bind different policies to each AAA group. Use the command "bind AAA group ... -policy ...". You can also bind ranges of Intranet IP addresses to an AAA group. For example, the administrator may want to assign pools of Intranet IP addresses to groups or departments.

Parameters

groupName

The group name.

userName

The user that the group is bound to. If the user belongs to more than one group, the group expressions are evaluated at authorization to determine the appropriate action.

policy

The policy to be bound to an AAA group.

intranetApplication

The intranet vpn application.

urlName

The intranet url.

intranetIP

The ip-block or IP address to be bound with this group. This is the block or address that will be used when members of this group access Intranet resources.

Example

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

Top

unbind aaa group

Synopsis

unbind aaa group <groupName> [-userName <string> ...] [-policy <string>] [-intranetApplication <string>] [-urlName <string>] [-intranetIP <ip_addr> <netmask>]

Description

Unbind the resource (User/Intranet IP/Policy/Intranet Application) from a group. To associate AAA users with an AAA group, use the command "bind AAA group ... -username ...". You can bind different policies to each AAA group. Use the command "bind AAA group ... -policy ...". You can also bind ranges of Intranet IP addresses to an AAA group. For example, the administrator may want to assign pools of Intranet IP addresses to groups or departments.

Parameters

groupName

The group name.

userName

The user to be unbound from the group.

policy

The policy to be unbound from the AAA group,

intranetApplication

The intranet vpn application.

urlName

The intranet url.

intranetIP

The Intranet IP to be unbound from the group

Example

unbind aaa group engg -intranetip 10.102.10.0 255.255.255.0

Top

show aaa group

Synopsis

show aaa group [<groupName>] [-loggedIn]

Description

Display details of the AAA group. To associate AAA users with an AAA group, use the command "bind AAA group ... -username ...". You can bind different policies to each AAA group. Use the command "bind AAA group ... -policy ...". You can also bind ranges of Intranet IP addresses to an AAA group. For example, the administrator may want to assign pools of Intranet IP addresses to groups or departments.

Parameters

groupName

The group name.

loggedIn

The loggedin flag. When this flag is turned on, the system displays the names of the users in a group if at least one user in the group is logged in. When used with a group name, the system lists the users in the group who are logged in.

Example

```
> show aaa group engg
      GroupName: engg

      Bound AAA users:
      UserName: joe
      UserName: jane

      Intranetip IP: 10.102.10.0      Netmask: 255.255.255.0
 Done
>
```

Top

aaa preauthenticationaction

[add | rm | set | unset | show]

add aaa preauthenticationaction

Synopsis

add aaa preauthenticationaction <name> [<preauthenticationaction>] [-killProcess <string>] [-deletefiles <string>]

Description

Add actions for end point analysis (EPA) clients before authentication.

Parameters

name

The name of the Preauthentication action.

preauthenticationaction

Deny or allow login after end point analysis results. Possible values: ALLOW, DENY

killProcess

Processes to be killed by the EPA tool.

deletefiles

Files to be deleted by EPA tool.

Top

rm aaa preauthenticationaction

Synopsis

rm aaa preauthenticationaction <name>

Description

Remove a previously created Pre-authentication action. Note that an action cannot be removed as long as it is configured in a policy.

Parameters

name

The name of the action to be removed.

Top

set aaa preauthenticationaction

Synopsis

set aaa preauthenticationaction <name> [<preauthenticationaction>] [-killProcess <string>] [-deletefiles <string>]

Description

Change properties of a Pre-authentication action.

Parameters

name

The name of the Preauthentication action.

preauthenticationaction

Deny or allow login after end point analysis results. Possible values: ALLOW, DENY

killProcess

Processes to be killed by EPA tool.

deletefiles

Files to be deleted by EPA tool.

Top

unset aaa preauthenticationaction

Synopsis

unset aaa preauthenticationaction <name> [-killProcess] [-deletefiles]

Description

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

Top

show aaa preauthenticationaction

Synopsis

show aaa preauthenticationaction [<name>]

Description

Display details of the configured Pre-authentication action(s).

Parameters

name

The name of the RADIUS action.

Top

aaa preauthenticationpolicy

[add | rm | set | show]

add aaa preauthenticationpolicy

Synopsis

add aaa preauthenticationpolicy <name> <rule> [<reqAction>]

Description

Add a Radius authentication policy. The policy defines expressions to be evaluated by the EPA tool.

Parameters

name

The name to assign to the new Pre-authentication policy.

rule

The name of the rule or expression that the policy will use.

reqAction

The name of the RADIUS action the policy will use.

Top

rm aaa preauthenticationpolicy

Synopsis

rm aaa preauthenticationpolicy <name>

Description

Remove a Pre-authentication policy.

Parameters

name

The name of the Pre-authentication policy to remove.

Top

set aaa preauthenticationpolicy

Synopsis

set aaa preauthenticationpolicy <name> [-rule <expression>] [-reqAction <string>]

Description

Change the properties of a Pre-authentication policy.

Parameters

name

The name of the policy.

rule

The new rule to be associated with the policy.

reqAction

The new Pre-authentication action to be associated with the policy.

Top

show aaa preauthenticationpolicy

Synopsis

show aaa preauthenticationpolicy [<name>]

Description

Display configured Pre-authentication policies.

Parameters

name

The name of the policy. If this option is not provided, all of the configured RADIUS policies will be displayed.

Top

aaa stats

show aaa stats

Synopsis

show aaa stats - alias for 'stat aaa'

Description

show aaa stats is an alias for stat aaa

aaa session

[show | kill]

show aaa session

Synopsis

show aaa session [-userName <string>] [-groupName <string>] [-intranetIP <ip_addr|*> [<netmask>]]

Description

Display the connections initated by the user

Parameters

userName

The user name.

groupName

The group name.

intranetIP

Intranet IP address.

Example

```
> show aaa connection
      ClintIp (ClientPort)   ->  ServerIp(ServerPort)
      ------------------------       ---------------------------
User Name: Joe

      10.102.0.39     (2318 ) -> 10.102.4.245    (443  )
      10.102.0.39     (2320 ) -> 10.102.4.245    (443  )
      10.102.0.39     (2340 ) -> 10.102.4.245    (443  )

 Done
>
```

Top

kill aaa session

Synopsis

kill aaa session [-userName <string>] [-groupName <string>] [-intranetIP <ip_addr|*> [<netmask>]] [-all]

Description

Kill the user sessions

Parameters

userName

The user name. The system will terminate the session initiated by the named user.

groupName

The group name. The system will terminate the sessions of all the users within the named group.

intranetIP

The Intranet IP address. The system will terminate all sessions using the named intranet IP address

all

Terminate the sessions of all users who are currently logged in.

Example

kill aaa session -user joe

Top

aaa radiusParams

[set | unset | show]

set aaa radiusParams

Synopsis

set aaa radiusParams [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-authTimeout <positive_integer>] {-radKey } [-radNASip (ENABLED | DISABLED)] [-radNASid <string>] [-radVendorID <positive_integer>] [-radAttributeType <positive_integer>] [-radGroupsPrefix <string>] [-radGroupSeparator <string>] [-passEncoding <passEncoding>] [-ipVendorID <positive_integer>] [-ipAttributeType <positive_integer>] [-accounting (ON | OFF)] [-pwdVendorID <positive_integer>] [-pwdAttributeType <positive_integer>]

Description

Modify the global variables for the RADIUS server. It will be used globally in SSL-VPN across all Vservers unless you create a vserver-specific configuration using authentication policies.

Parameters

serverIP

The IP address of the RADIUS server.

serverPort

The port number on which the RADIUS server is running. Default value: 1812 Minimum value: 1

authTimeout

The maximum number of seconds the system will wait for a response from the RADIUS server. Default value: 3 Minimum value: 1

radKey

The key shared between the client and the server. This information is required for the system to communicate with the RADIUS server.

radNASip

The option to send the NetScaler's IP address (NSIP) to the server as the "nasip" (Network Access Server IP) part of the Radius protocol. Possible values: ENABLED, DISABLED

radNASid

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

radVendorID

The Vendor ID for Radius group extraction. Minimum value: 1

radAttributeType

The Attribute type for Radius group extraction. Minimum value: 1

radGroupsPrefix

The groups prefix string that precedes the group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator

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

passEncoding

The option to encode the password in the Radius packets traveling from the NetScaler to the Radius server. Possible values: pap, chap, mschapv1, mschapv2 Default value: AAA_PAP

ipVendorID

The vendor ID of the attribute in the RADIUS response. The vendor ID denotes the intranet IP. The value of 0 denotes that the attribute is not vendor-encoded.

ipAttributeType

The attribute type of the remote IP address attribute in a RADIUS response. Minimum value: 1

accounting

The state of the RADIUS server to receive accounting messages. Possible values: ON, OFF

pwdVendorID

Vendor ID of the attribute in the RADIUS response which will be used to extract the user Password. Minimum value: 1

Example

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

Top

unset aaa radiusParams

Synopsis

unset aaa radiusParams [-serverIP] [-serverPort] [-authTimeout] [-radNASip] [-radNASid] [-radVendorID] [-radAttributeType] [-radGroupsPrefix] [-radGroupSeparator] [-passEncoding] [-ipVendorID] [-ipAttributeType] [-accounting] [-pwdVendorID] [-pwdAttributeType]

Description

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

Top

show aaa radiusParams

Synopsis

show aaa radiusParams

Description

Display the configured RADIUS parameters.

Example

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

Top

aaa ldapParams

[set | unset | show]

set aaa ldapParams

Synopsis

set aaa ldapParams [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-authTimeout <positive_integer>] [-ldapBase <string>] [-ldapBindDn <string>] {-ldapBindDnPassword } [-ldapLoginName <string>] [-searchFilter <string>] [-groupAttrName <string>] [-subAttributeName <string>] [-secType <secType>] [-svrType (AD | NDS)] [-ssoNameAttribute <string>] [-passwdChange (ENABLED | DISABLED)] [-nestedGroupExtraction (ON | OFF)] [-maxNestingLevel <positive_integer>] [-groupNameIdentifier <string>] [-groupSearchAttribute <string> [-groupSearchSubAttribute <string>]] [-groupSearchFilter <string>]

Description

Set the global variables for the LDAP server. It is used globally in SSL-VPN across all Vservers unless you create a vserver-specific configuration using authentication policies.

Parameters

serverIP

The IP address of the LDAP server. The default value is localhost.

serverPort

The port number on which the LDAP server is running. Default value: 389 Minimum value: 1

authTimeout

The maximum number of seconds the system will wait for a response from the LDAP server. Default value: 3 Minimum value: 1

ldapBase

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

ldapBindDn

The full distinguished name that is used to bind to the LDAP server.

ldapBindDnPassword

The password used to bind to the LDAP server.

ldapLoginName

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

searchFilter

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

groupAttrName

The attribute name for group extraction from the LDAP server

subAttributeName

The Sub-Attribute name for group extraction from LDAP server

secType

The type of communication between the system and the LDAP server. The values are: PLAINTEXT: No encryption required. TLS: To use the TLS protocol to communicate. SSL: To use the SSL Protocol to communicate. Possible values: PLAINTEXT, TLS, SSL Default value: AAA_LDAP_PLAINTEXT

svrType

The type of LDAP server. Possible values: AD, NDS Default value: AAA_LDAP_SERVER_TYPE_DEFAULT

ssoNameAttribute

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

passwdChange

Enabling this option does not block password change request.Disabling would block password change request. Possible values: ENABLED, DISABLED Default value: DISABLED

nestedGroupExtraction

Setting this option to ON enables the nested group extraction feature where the system queries the external LDAP server to determine if a group belongs to another group Possible values: ON, OFF Default value: OFF

Example

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

Top

unset aaa ldapParams

Synopsis

unset aaa ldapParams [-serverIP] [-serverPort] [-authTimeout] [-ldapBase] [-ldapBindDn] [-ldapBindDnPassword] [-ldapLoginName] [-searchFilter] [-groupAttrName] [-subAttributeName] [-secType] [-svrType] [-ssoNameAttribute] [-passwdChange] [-nestedGroupExtraction] [-maxNestingLevel] [-groupNameIdentifier] [-groupSearchAttribute] [-groupSearchSubAttribute] [-groupSearchFilter]

Description

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

Top

show aaa ldapParams

Synopsis

show aaa ldapParams

Description

Display the configured LDAP parameters.

Example

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

Top

aaa tacacsParams

[set | unset | show]

set aaa tacacsParams

Synopsis

set aaa tacacsParams [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-authTimeout <positive_integer>] {-tacacsSecret } [-authorization (ON | OFF)] [-accounting (ON | OFF)] [-auditFailedCmds (ON | OFF)]

Description

Set the global variables for the TACACS+ server. It is used globally in SSL-VPN across all Vservers unless a vserver-specific configuration is done using authentication policies.

Parameters

serverIP

The IP address of the TACACS+ server.

serverPort

The port on which the TACACS+ server is running. Default value: 49 Minimum value: 1

authTimeout

The maximum number of seconds the system will wait for a response from the TACACS+ server. Default value: 3 Minimum value: 1

tacacsSecret

The key shared between the client and the server. This information is required for the system to communicate with the TACACS+ server.

authorization

The option for streaming authorization for the TACACS+ server. Possible values: ON, OFF

accounting

The option for sending accounting messages to the TACACS+ server. Possible values: ON, OFF

auditFailedCmds

The option for sending accounting messages to the TACACS+ server. Possible values: ON, OFF

Example

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

Top

unset aaa tacacsParams

Synopsis

unset aaa tacacsParams [-serverIP] [-serverPort] [-authTimeout] [-tacacsSecret] [-authorization] [-accounting] [-auditFailedCmds]

Description

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

Top

show aaa tacacsParams

Synopsis

show aaa tacacsParams

Description

Display configured AAA TACACS+ server parameters.

Example

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

Top

aaa certParams

[set | unset | show]

set aaa certParams

Synopsis

set aaa certParams [-userNameField <string>] [-groupNameField <string>]

Description

Set the global variables for a certificate policy. It is used globally in SSL-VPN across all Vservers unless vserver-specific configuration is done using authentication policies.

Parameters

userNameField

The field in the client certificate to extract the username from. Should be of the format <field:subfield>. Allowed values for field are "Subject" and "Issuer".

groupNameField

The certificate field to extract the group from. Should be of the format <field:subfield>. Allowed values for field are "Subject" and "Issuer".

Example

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

Top

unset aaa certParams

Synopsis

unset aaa certParams [-userNameField] [-groupNameField]

Description

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

Top

show aaa certParams

Synopsis

show aaa certParams

Description

Display the configured CERT parameters.

Top

aaa parameter

[set | unset | show]

set aaa parameter

Synopsis

set aaa parameter [-enableStaticPageCaching (YES | NO)] [-defaultAuthType <defaultAuthType>] [-maxAAAUsers <positive_integer>] [-aaadnatIp <ip_addr|*>]

Description

Set the global AAA parameters. This will override the default authentication server setting.

Parameters

enableStaticPageCaching

The default state of VPN Static Page caching. If nothing is specified, the default value is set to ON. Possible values: YES, NO Default value: STATIC_PAGE_CACHING_ENABLED

defaultAuthType

The default authentication server type. If nothing is specified, the default value is set to Local. Possible values: LOCAL, LDAP, RADIUS, TACACS, CERT Default value: LOCAL_AUTH

maxAAAUsers

The maximum number of concurrent users allowed to login in to the system at any given time. Minimum value: 1 Maximum value: 65535

aaadnatIp

The source ip to be used for the traffic going to authentication servers

Example

set aaa parameter -defaultAuthType RADIUS -maxAAAUSers 100

Top

unset aaa parameter

Synopsis

unset aaa parameter [-enableStaticPageCaching] [-defaultAuthType] [-maxAAAUsers] [-aaadnatIp]

Description

Set default aaa paramter.Refer to the set aaa parameter command for meanings of the arguments.

Top

show aaa parameter

Synopsis

show aaa parameter

Description

Displays the configured AAA parameters .

Example

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

Top

aaa preauthenticationparameter

[set | unset | show]

set aaa preauthenticationparameter

Synopsis

set aaa preauthenticationparameter [-preauthenticationaction (ALLOW | DENY)] [-rule <expression>] [-killProcess <string>] [-deletefiles <string>]

Description

Sets the default end point analysis (EPA) parameters before authentication.

Parameters

preauthenticationaction

Deny or allow login after end point analysis results. Possible values: ALLOW, DENY

rule

The name of the rule, or expression, to be evaluated by the EPA tool.

killProcess

Processes to be killed by the EPA tool.

deletefiles

Files to be deleted by the EPA tool.

Top

unset aaa preauthenticationparameter

Synopsis

unset aaa preauthenticationparameter [-rule] [-preauthenticationaction] [-killProcess] [-deletefiles]

Description

Set default end point analysis(EPA) parameters before authentication. .Refer to the set aaa preauthenticationparameter command for meanings of the arguments.

Top

show aaa preauthenticationparameter

Synopsis

show aaa preauthenticationparameter

Description

Display details of the configured Pre-authentication parameter(s).

Top

aaa global

[bind | unbind | show]

bind aaa global

Synopsis

bind aaa global (-policy <string> [-priority <positive_integer>])

Description

Binds the policy globally.

Parameters

policy

The policy to be bound globally.

Example

bind aaa global -pol pol1

Top

unbind aaa global

Synopsis

unbind aaa global -policy <string>

Description

Unbind the policy globally

Parameters

policy

The policy to be unbound to the AAA user.

Top

show aaa global

Synopsis

show aaa global

Description

Display details of the configured policies aaa global.

Top

Application Commands

[import | export]

import application

Synopsis

import application <apptemplateFilename> [-appname <string>] [-deploymentFilename <input_filename>]

Description

Imports application configuration information from an AppExpert application template file. You can specify a deployment file along with the template file. A template file contains application and variable definitions. A deployment file contains information about the services, service groups, endpoints, and variables that were in the AppExpert application configuration at the time the template file was created. Template files are imported from the /nsconfig/nstemplates/applications/ directory on the appliance. Deployment files are imported from the /nsconfig/nstemplates/applications/ deployment_files directory. You cannot change the source directories, so import the template file and deployment file to their respective directories before you use the command.

Parameters

apptemplateFilename

The name of the AppExpert application template file.

appname

The name with which you want the AppExpert application to function on the NetScaler appliance. If you do not provide a name, the appliance assigns the application the name of the template file.

deploymentFilename

The name of the deployment file.

Example

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

Top

export application

Synopsis

export application <appname> [-apptemplateFilename <input_filename>] [-deploymentFilename <input_filename>]

Description

Exports application configuration information to an AppExpert application template file. A deployment file is created along with the template file. The template file contains application and variable definitions. The deployment file contains information about the services, service groups, endpoints, and variables that are in the AppExpert application configuration. The template file is exported to the /nsconfig/nstemplates/applications/ directory on the appliance. The deployment file is exported to the /nsconfig/nstemplates/applications/deployment_files directory.

Parameters

appname

The name of the AppExpert application whose configuration you want to export to a template file.

apptemplateFilename

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

deploymentFilename

The name with which you want to save the deployment file. If you do not specify a name, the string _deployment is automatically appended to the name of the template file to create the name of the deployment file.

Top

AppFlow Commands

This group of commands can be used to perform operations on the following entities:

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

appflow

stat appflow

Synopsis

stat appflow [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display AppFlow statistics.

appflow collector

[add | rm | rename | show]

add appflow collector

Synopsis

add appflow collector <name> -IPAddress <ip_addr> [-port <port>] [-netProfile <string>]

Description

Add a new AppFlow collector.

Parameters

name

Name of the AppFlow collector.

IPAddress

The IPv4 address of the AppFlow collector.

port

The UDP port on which the AppFlow collector is listening. Default value: 4739

netProfile

The IP address associated with this netprofile will be used as source IP for appflow traffic to this collector

Example

add appflow collector collector1 -IPAddress 192.168.1.40 -port 2055

Top

rm appflow collector

Synopsis

rm appflow collector <name>

Description

Remove an AppFlow collector.

Parameters

name

Name of an AppFlow collector.

Example

rm appflow collector collector1

Top

rename appflow collector

Synopsis

rename appflow collector <name>@ <newName>@

Description

Rename an AppFlow collector.

Parameters

name

The name of an AppFlow collector.

newName

The new name of the AppFlow collector.

Example

rename appflow collector old_name new_name

Top

show appflow collector

Synopsis

show appflow collector [<name>]

Description

Display details of all the AppFlow collectors configured on the system. Alternatively, to view the details of a particular AppFlow collector, specify its name.

Parameters

name

Name of an AppFlow collector.

Example

show appflow collector collector1

Top

appflow action

[add | rm | set | unset | rename | show]

add appflow action

Synopsis

add appflow action <name> -collectors <string> ... [-comment <string>]

Description

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

Parameters

name

Name of the AppFlow action to be added.

collectors

The names of AppFlow collectors associated with the AppFlow action.

comment

Comments associated with this AppFlow action.

Example

add appflow action appflow_action_1 -collectors col1 col2

Top

rm appflow action

Synopsis

rm appflow action <name>

Description

Remove a configured AppFlow action.

Parameters

name

Name of an AppFlow action.

Example

rm appflow action appflow_action_1

Top

set appflow action

Synopsis

set appflow action <name> [-collectors <string> ...] [-comment <string>]

Description

Modify an AppFlow action.

Parameters

name

The name of the AppFlow action to be modified.

collectors

The names of AppFlow collectors associated with the AppFlow action.

comment

Comments associated with this AppFlow action.

Example

set appflow action appflow_action_1 -collectors col1 col2 col3

Top

unset appflow action

Synopsis

unset appflow action <name> -comment

Description

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

Top

rename appflow action

Synopsis

rename appflow action <name>@ <newName>@

Description

Rename an AppFlow action.

Parameters

name

The name of an AppFlow action.

newName

The new name of the AppFlow action.

Example

rename appflow action old_name new_name

Top

show appflow action

Synopsis

show appflow action [<name>]

Description

Display configured AppFlow action(s).

Parameters

name

Name of an AppFlow action.

Example

1. show appflow action
   2. show appflow action appflow_action_1

Top

appflow policy

[add | rm | set | unset | rename | show]

add appflow policy

Synopsis

add appflow policy <name> <rule> <action> [-comment <string>]

Description

Add an AppFlow policy.

Parameters

name

Name of the AppFlow policy.

rule

Expression to be used by the AppFlow policy. It has to be a boolean PI rule expression.

action

AppFlow action to be used by the policy.

comment

Comments associated with this AppFlow policy.

Example

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

Top

rm appflow policy

Synopsis

rm appflow policy <name>

Description

Remove an AppFlow policy.

Parameters

name

Name of the AppFlow policy to be removed.

Example

rm appflow policy appflow_policy_1

Top

set appflow policy

Synopsis

set appflow policy <name> [-rule <expression>] [-action <string>] [-comment <string>]

Description

Set a new rule and/or action for an existing AppFlow policy. The rule flow type can change only if: . action is of NEUTRAL flow type

Parameters

name

Name of an AppFlow policy.

rule

Expression to be used by the AppFlow policy. It has to be a boolean PI rule expression.

action

AppFlow action to be used by the policy.

comment

Comments associated with this AppFlow policy.

Example

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

Top

unset appflow policy

Synopsis

unset appflow policy <name> -comment

Description

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

Top

rename appflow policy

Synopsis

rename appflow policy <name>@ <newName>@

Description

Rename an AppFlow policy.

Parameters

name

The name of an AppFlow policy.

newName

The new name of the AppFlow policy.

Example

rename appflow policy old_name new_name

Top

show appflow policy

Synopsis

show appflow policy [<name>]

Description

Display all the configured AppFlow policies.

Parameters

name

Name of an AppFlow policy.

Example

show appflow policy

Top

appflow policylabel

[add | rm | bind | unbind | rename | show]

add appflow policylabel

Synopsis

add appflow policylabel <labelName> [-policylabeltype (HTTP | OTHERTCP)]

Description

Create an AppFlow policy label.

Parameters

labelName

The name of the AppFlow policy label to be created.

policylabeltype

The type of the policy label. Possible values: HTTP, OTHERTCP Default value: NS_PLTMAP_APPFLOW_REQ

Example

add appflow policylabel appflow_pol_label

Top

rm appflow policylabel

Synopsis

rm appflow policylabel <labelName>

Description

Remove an AppFlow policy label.

Parameters

labelName

The name of the AppFlow policy label to be removed.

Example

rm appflow policylabel appflow_pol_label

Top

bind appflow policylabel

Synopsis

bind appflow policylabel <labelName> -policyName <string> -priority <positive_integer> [-gotoPriorityExpression <expression>] [-invoke (<labelType> <labelName>)]

Description

Bind an AppFlow policy to an AppFlow policy label.

Parameters

labelName

Name of an AppFlow policy label.

policyName

Name of an AppFlow policy.

Example

bind appflow policylabel appflow_pol_label -policyName appflow_pol -priority 1

Top

unbind appflow policylabel

Synopsis

unbind appflow policylabel <labelName> <policyName> [-priority <positive_integer>]

Description

Unbind an AppFlow policy from an AppFlow policy label.

Parameters

labelName

Name of an AppFlow policy label.

policyName

Name of an AppFlow policy.

Example

unbind appflow policylabel appflow_pol_label appflow_pol

Top

rename appflow policylabel

Synopsis

rename appflow policylabel <labelName>@ <newName>@

Description

Rename an AppFlow policy label.

Parameters

labelName

The name of an AppFlow policylabel.

newName

The new name of the AppFlow policylabel.

Example

rename appflow policylabel old_name new_name

Top

show appflow policylabel

Synopsis

show appflow policylabel [<labelName>]

Description

Display all AppFlow policy labels or all policies bound to an AppFlow policy label.

Parameters

labelName

The name of the AppFlow policy label.

Example

i) show appflow policylabel appflow_pol_label
ii) show appflow policylabel

Top

appflow param

[set | unset | show]

set appflow param

Synopsis

set appflow param [-templateRefresh <secs>] [-appnameRefresh <secs>] [-flowRecordInterval <secs>] [-udpPmtu <positive_integer>] [-httpUrl (ENABLED | DISABLED)] [-httpCookie (ENABLED | DISABLED)] [-httpReferer (ENABLED | DISABLED)] [-httpMethod (ENABLED | DISABLED)] [-httpHost (ENABLED | DISABLED)] [-httpUserAgent (ENABLED | DISABLED)] [-clientTrafficOnly (YES | NO)] [-httpContentType (ENABLED | DISABLED)] [-httpAuthorization (ENABLED | DISABLED)] [-httpVia (ENABLED | DISABLED)] [-httpXForwardedFor (ENABLED | DISABLED)] [-httpLocation (ENABLED | DISABLED)] [-httpSetCookie (ENABLED | DISABLED)] [-httpSetCookie2 (ENABLED | DISABLED)]

Description

Configure AppFlow parameters.

Parameters

templateRefresh

IPFIX template refresh interval (in seconds). Default value: 600 Minimum value: 60 Maximum value: 3600

appnameRefresh

Appname refresh interval (in seconds). Default value: 600 Minimum value: 60 Maximum value: 3600

flowRecordInterval

IPFIX flow record export interval (in seconds). Default value: 600 Minimum value: 60 Maximum value: 3600

udpPmtu

MTU to be used for IPFIX UDP packets. Default value: 1472 Minimum value: 128 Maximum value: 1472

httpUrl

Enable AppFlow HTTP URL logging. Possible values: ENABLED, DISABLED Default value: DISABLED

httpCookie

Enable AppFlow HTTP cookie logging. Possible values: ENABLED, DISABLED Default value: DISABLED

httpReferer

Enable AppFlow HTTP referer logging. Possible values: ENABLED, DISABLED Default value: DISABLED

httpMethod

Enable AppFlow HTTP method logging. Possible values: ENABLED, DISABLED Default value: DISABLED

httpHost

Enable AppFlow HTTP host logging. Possible values: ENABLED, DISABLED Default value: DISABLED

httpUserAgent

Enable AppFlow HTTP user-agent logging. Possible values: ENABLED, DISABLED Default value: DISABLED

clientTrafficOnly

Control whether AppFlow records should be generated only for client-side traffic. Possible values: YES, NO Default value: NO

httpContentType

Enable AppFlow HTTP Content-Type header logging. Possible values: ENABLED, DISABLED Default value: DISABLED

httpAuthorization

Enable AppFlow HTTP Authorization header logging. Possible values: ENABLED, DISABLED Default value: DISABLED

httpVia

Enable AppFlow HTTP Via header logging. Possible values: ENABLED, DISABLED Default value: DISABLED

httpXForwardedFor

Enable AppFlow HTTP X-Forwarded-For header logging. Possible values: ENABLED, DISABLED Default value: DISABLED

httpLocation

Enable AppFlow HTTP Location header logging. Possible values: ENABLED, DISABLED Default value: DISABLED

httpSetCookie

Enable AppFlow HTTP Setcookie header logging. Possible values: ENABLED, DISABLED
Default value: DISABLED

httpSetCookie2

Enable AppFlow HTTP Setcookie2 header logging. Possible values: ENABLED, DISABLED
Default value: DISABLED

Example

set appflow param -templateRefresh 240

Top

unset appflow param

Synopsis

unset appflow param [-templateRefresh] [-appnameRefresh] [-flowRecordInterval] [-udpPmtu] [-httpUrl] [-httpCookie] [-httpReferer] [-httpMethod] [-httpHost] [-httpUserAgent] [-clientTrafficOnly] [-httpContentType] [-httpAuthorization] [-httpVia] [-httpXForwardedFor] [-httpLocation] [-httpSetCookie] [-httpSetCookie2]

Description

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

Top

show appflow param

Synopsis

show appflow param

Description

Display AppFlow parameters.

Top

appflow global

[bind | unbind | show]

bind appflow global

Synopsis

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [-type <type>] [-invoke (<labelType> <labelName>)]

Description

Bind the AppFlow policy to one of the two global lists of AppFlow policies. A policy becomes active only after it is bound. All traffic will be evaluated against these two policy banks. Each bank of policies is an ordered list ordered by policies priority values. Policy Bank Evaluation The goal of evaluation is to traverse the ordered list of policies in the bank, find out which policies match and build a result set that will contain the actions of all the matching policies. While evaluating a policy if any advanced expression cannot be evaluated then UNDEF processing will get triggered. There are also other scenarios during policy traversal when UNDEF processing can get triggered. If an UNDEF event occurs while processing a policy, then (i) policy bank traversal ends, (ii) the result set of actions that was built so far is wiped out (iii) the current policy's undefAction is put in the result set and the evaluation ends.

Parameters

policyName

Name of an AppFlow policy.

Example

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

Top

unbind appflow global

Synopsis

unbind appflow global (<policyName> [-type <type>] [-priority <positive_integer>])

Description

Unbind entities from AppFlow global.

Parameters

policyName

Name of an AppFlow policy.

Example

unbind appflow global pol9

Top

show appflow global

Synopsis

show appflow global [-type <type>]

Description

Display the AppFlow global bindings.

Parameters

type

The bindpoint to which the policy is bound. Possible values: REQ_OVERRIDE, REQ_DEFAULT, OVERRIDE, DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE, MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT

Example

show appflow global

Top

Application Firewall Commands

This group of commands can be used to perform operations on the following entities:

- appfw
- appfw fieldType
- appfw profile
- appfw policy
- appfw policylabel
- appfw confidField
- appfw stats
- appfw xmlerrorpage
- appfw htmlerrorpage
- appfw settings
- appfw global
- appfw learningsettings
- appfw learningdata
- appfw wsdl
- appfw signatures
- appfw xmlschema
- appfw XMLContentType
- appfw archive

appfw

stat appfw

Synopsis

stat appfw [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display application firewall stats.

appfw fieldType

[add | rm | set | show]

add appfw fieldType

Synopsis

add appfw fieldType <name> <regex> <priority> [-comment <string>]

Description

Add an application firewall field type. Field types define the type of data that can appear in a web form field. The Learning engine uses the field types list to generate appropriate field type assignments for the field formats check.

Parameters

name

The name of this field type.

regex

The regular expression that describes this field type.

priority

The priority of this field type. Maximum value: 64000

comment

Comments associated with this field type.

Top

rm appfw fieldType

Synopsis

rm appfw fieldType <name>

Description

Remove an application firewall field type. Field types define the type of data that can appear in a web form field. The Learning engine uses the field types list to generate appropriate field type assignments for the field formats check.

Parameters

name

The name of this field type.

Top

set appfw fieldType

Synopsis

set appfw fieldType <name> <regex> <priority> [-comment <string>]

Description

Modify an application firewall field type. Field types define the type of data that can appear in a web form field. The Learning engine uses the field types list to generate appropriate field type assignments for the field formats check.

Parameters

name

The name of this field type.

regex

The regular expression that describes this field type.

Top

show appfw fieldType

Synopsis

show appfw fieldType [<name>]

Description

Display all configured application firewall form field types.

Parameters

name

The name of this field type.

Top

appfw profile

[add | rm | set | unset | bind | unbind | show | stat | archive | restore]

add appfw profile

Synopsis

add appfw profile <name> [-defaults (basic | advanced)] [-startURLAction <startURLAction> ...] [-startURLClosure (ON | OFF)] [-denyURLAction <denyURLAction> ...] [-RefererHeaderCheck <RefererHeaderCheck>] [-cookieConsistencyAction <cookieConsistencyAction> ...] [-cookieTransforms (ON | OFF)] [-cookieEncryption <cookieEncryption>] [-cookieProxying (none | sessionOnly)] [-addCookieFlags <addCookieFlags>] [-fieldConsistencyAction <fieldConsistencyAction> ...] [-CSRFtagAction <CSRFtagAction> ...] [-crossSiteScriptingAction <crossSiteScriptingAction> ...] [-crossSiteScriptingTransformUnsafeHTML (ON | OFF)] [-crossSiteScriptingCheckCompleteURLs (ON | OFF)] [-SQLInjectionAction <SQLInjectionAction> ...] [-SQLInjectionTransformSpecialChars (ON | OFF)] [-SQLInjectionOnlyCheckFieldsWithSQLChars (ON | OFF)] [-fieldFormatAction <fieldFormatAction> ...] [-defaultFieldFormatType <string>] [-defaultFieldFormatMinLength <positive_integer>] [-defaultFieldFormatMaxLength <positive_integer>] [-bufferOverflowAction <bufferOverflowAction> ...] [-bufferOverflowMaxURLLength <positive_integer>] [-bufferOverflowMaxHeaderLength <positive_integer>] [-bufferOverflowMaxCookieLength <positive_integer>] [-creditCardAction <creditCardAction> ...] [-creditCard <creditCard> ...] [-creditCardMaxAllowed <positive_integer>] [-creditCardXOut (ON | OFF)] [-requestContentType <string>] [-responseContentType <string>] [-XMLDoSAction <XMLDoSAction> ...] [-XMLFormatAction <XMLFormatAction> ...] [-XMLSQLInjectionAction <XMLSQLInjectionAction> ...] [-XMLSQLInjectionOnlyCheckFieldsWithSQLChars (ON | OFF)] [-XMLSQLInjectionParseComments <XMLSQLInjectionParseComments>] [-XMLXSSAction <XMLXSSAction> ...] [-XMLWSIAction <XMLWSIAction> ...] [-XMLAttachmentAction <XMLAttachmentAction> ...] [-XMLValidationAction <XMLValidationAction> ...] [-XMLErrorObject <string>] [-signatures <string>] [-XMLSOAPFaultAction <XMLSOAPFaultAction> ...] [-useHTMLErrorObject (ON | OFF)] [-errorURL <expression>] [-HTMLErrorObject <string>] [-logEveryPolicyHit (ON | OFF)] [-stripHtmlComments <stripHtmlComments>] [-stripXmlComments (none | all)] [-exemptClosureURLsFromSecurityChecks (ON | OFF)] [-defaultCharSet <string>] [-postBodyLimit <positive_integer>] [-fileUploadMaxNum <positive_integer>] [-canonicalizeHTMLResponse (ON | OFF)] [-enableFormTagging (ON | OFF)] [-sessionlessFieldConsistency <sessionlessFieldConsistency>] [-sessionlessURLClosure (ON | OFF)] [-semicolonFieldSeparator (ON | OFF)] [-excludeFileUploadFromChecks (ON | OFF)] [-SQLInjectionParseComments <SQLInjectionParseComments>] [-invalidPercentHandling <invalidPercentHandling>] [-type (HTML | XML) ...] [-checkRequestHeaders (ON | OFF)] [-comment <string>]

Description

Add an application firewall profile. A profile tells the application firewall how it should protect a given class of web content. Different types of content often require different protection strategies. You define these strategies in a profile. You can create profiles with basic or advanced defaults. The defaults, or predefined settings, provide solid initial protection for web content - a starting point from which you can configure additional protection for special content. Each profile is associated with a policy that tells the application firewall the content type of a request or response. When a request or response matches the policy, that profile is applied.

Parameters

name

Application firewall profile name.

defaults

Default Start URLs and Deny URLs. Possible values: basic, advanced

builtin

Indicates that a profile is a built-in entity.

builtinType

Type of built-in Profile. Possible values: APPFW_NOT_BUILTIN, APPFW_BYPASS, APPFW_BLOCK, APPFW_RESET, APPFW_DROP

startURLAction

Start URL action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. Default value: AS_DEFAULT_DISPOSITION

startURLClosure

Start URL closure. This check is applicable to Profile Type: HTML, XML. Possible values: ON, OFF Default value: OFF

denyURLAction

Deny URL action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. LEARN is not supported. Default value: AS_DEFAULT_DISPOSITION

RefererHeaderCheck

Referer header check This check is applicable to Profile Type: HTML. Possible values: OFF, if_present, always Default value: AS_HEADER_CHECK_OFF

cookieConsistencyAction

Cookie consistency action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. Default value: AS_NONE

cookieTransforms

Enable cookie transforms: encryption, proxying, and adding cookie flags. Make sure this is turned ON if you want the transforms to happen. This check is applicable to Profile Type: HTML. XML Possible values: ON, OFF Default value: OFF

cookieEncryption

Encrypts server cookies Possible values: none, decryptOnly, encryptSessionOnly, encryptAll Default value: AS_CKI_ENCRYPT_NONE

cookieProxying

Proxy server cookies using an application firewall session Possible values: none, sessionOnly Default value: AS_CKI_PROXY_NONE

addCookieFlags

Add HttpOnly and/or Secure flags to cookies Possible values: none, httpOnly, secure, all Default value: AS_ADD_CKI_FLAGS_NONE

fieldConsistencyAction

Form Field Consistency action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML. Default value: AS_NONE

CSRFtagAction

Cross-site request forgery tag action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML. LEARN is not supported. Default value: AS_NONE

crossSiteScriptingAction

Cross-site scripting action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML. Default value: AS_DEFAULT_DISPOSITION

crossSiteScriptingTransformUnsafeHTML

Transform HTML characters. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

crossSiteScriptingCheckCompleteURLs

Check complete URLs. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

SQLInjectionAction

SQL injection action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML. Default value: AS_DEFAULT_DISPOSITION

SQLInjectionTransformSpecialChars

Transform HTML characters. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

SQLInjectionOnlyCheckFieldsWithSQLChars

Check SQL characters. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: ON

fieldFormatAction

Field format action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML. Default value: AS_DEFAULT_DISPOSITION

defaultFieldFormatType

Default field type. This check is applicable to Profile Type: HTML.

defaultFieldFormatMinLength

Default field type minimum length. This check is applicable to Profile Type: HTML. Default value: AS_DEFAULTFIELDFORMAT_DEFAULT_MIN_LEN Maximum value: 65535

defaultFieldFormatMaxLength

Default field type maximum length. This check is applicable to Profile Type: HTML. Default value: AS_DEFAULTFIELDFORMAT_DEFAULT_MAX_LEN Minimum value: 1 Maximum value: 65535

bufferOverflowAction

Buffer overflow action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. LEARN is not supported. Default value: AS_DEFAULT_DISPOSITION

bufferOverflowMaxURLLength

Maximum URL length. This check is applicable to Profile Type: HTML, XML. Default value: AS_BUFFEROVERFLOW_DEFAULT_MAX_URL_LEN Maximum value: 65535

bufferOverflowMaxHeaderLength

Maximum header length. This check is applicable to Profile Type: HTML, XML. Default value: AS_BUFFEROVERFLOW_DEFAULT_MAX_HDR_LEN Maximum value: 65535

bufferOverflowMaxCookieLength

Maximum cookie length. This check is applicable to Profile Type: HTML, XML. Default value: AS_BUFFEROVERFLOW_DEFAULT_MAX_COOKIE_LEN Maximum value: 65535

creditCardAction

Credit Card action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. LEARN is not supported. Default value: AS_NONE

creditCard

Credit card. This check is applicable to Profile Type: HTML, XML. Default value: AS_CCARD_DEFAULT_CARD_TYPE

creditCardMaxAllowed

Maximum number of times a credit card number may be seen before action is taken. This check is applicable to Profile Type: HTML, XML. Maximum value: 255

creditCardXOut

X-out the credit card numbers. This check is applicable to Profile Type: HTML, XML. Possible values: ON, OFF Default value: OFF

requestContentType

Default content-type for request messages. This binding is applicable to Profile Type: HTML, XML. Default value: NS_S_AS_DEFAULT_REQUEST_CONTENT_TYPE

responseContentType

Default content-type for response messages. This binding is applicable to Profile Type: HTML, XML. Default value: NS_S_AS_DEFAULT_RESPONSE_CONTENT_TYPE

XMLDoSAction

XML DOS action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: XML. Default value: AS_DEFAULT_DISPOSITION

XMLFormatAction

XML well-formed request action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. LEARN is not supported. Default value: AS_DEFAULT_DISPOSITION

XMLSQLInjectionAction

XML SQL injection action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. LEARN is not supported. Default value: AS_DEFAULT_DISPOSITION

XMLSQLInjectionOnlyCheckFieldsWithSQLChars

Check SQL characters. This check is applicable to Profile Type: XML. Possible values: ON, OFF Default value: ON

XMLSQLInjectionParseComments

Canonicalize SQL Comments in XML Data. This check is applicable to Profile Type: XML. Possible values: checkall, ansi, nested, ansinested Default value: AS_CHECKALL

XMLXSSAction

XML cross-site scripting action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. LEARN is not supported. Default value: AS_DEFAULT_DISPOSITION

XMLWSIAction

XML WS-I action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: XML. Default value: AS_DEFAULT_DISPOSITION

XMLAttachmentAction

XML attachment action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: XML. Default value: AS_DEFAULT_DISPOSITION

XMLValidationAction

XML validation action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. LEARN is not supported. Default value: AS_DEFAULT_DISPOSITION

XMLErrorObject

Object name for the xml error page. This check is applicable to Profile Type: XML. Default value: NS_S_AS_ERROROBJECT_DEFAULT

customSettings

Object name for custom settings. This check is applicable to Profile Type: HTML, XML. Default value: NS_S_AS_ERROROBJECT_DEFAULT

signatures

Object name for signatures. This check is applicable to Profile Type: HTML, XML. Default value: NS_S_AS_ERROROBJECT_DEFAULT

XMLSOAPFaultAction

XML SOAP fault filtering action types. (BLOCK | LOG | STATS | REMOVE | NONE) This check is applicable to Profile Type: XML. LEARN is not supported. Default value: AS_DEFAULT_DISPOSITION

useHTMLErrorObject

Use HTML Error object for response instead of Redirect Error URL. Possible values: ON, OFF Default value: OFF

errorURL

Error page. This check is applicable to Profile Type: HTML. Default value: NS_S_AS_ERROR_URL_DEFAULT

HTMLErrorObject

Object name for the html error page. This check is applicable to Profile Type: HTML. Default value: NS_S_AS_ERROROBJECT_DEFAULT

logEveryPolicyHit

Log every profile match regardless of security checks results. Possible values: ON, OFF Default value: OFF

stripComments

Strip HTML comments. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

stripHtmlComments

Strip HTML comments. This check is applicable to Profile Type: HTML. Possible values: none, all, exclude_script_tag Default value: AS_STRIP_COMMENT_NONE

stripXmlComments

Strip XML comments. This check is applicable to Profile Type: XML. Possible values: none, all Default value: AS_STRIP_COMMENT_NONE

exemptClosureURLsFromSecurityChecks

Tells the application firewall to exempt closure URLs from security checks. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: ON

defaultCharSet

Default character set. Possible values are iso-8859-1 (English US), big5 (Chinese Traditional), gb2312 (Chinese Simplified), sjis (Japanese), euc-jp (Japanese EUC-JP), utf-8 (Unicode), and euc-kr (Korean). This check is applicable to Profile Type: HTML. Default value: NS_S_AS_CHARSET_DEFAULT Maximum value: 31

postBodyLimit

Maximum allowed post body size. This check is applicable to Profile Type: HTML, XML. Default value: AS_DEFAULT_POSTBODYLIMIT Maximum value: 1000000000

fileUploadMaxNum

Maximum allowed number of file uploads per form submission request. Setting this parameter to the maximum value of 65535 will allow an unlimited number of uploads. Default value: AS_DEFAULT_MAX_FILE_UPLOADS Maximum value: 65535

canonicalizeHTMLResponse

Entity encoding for html special characters for attributes in the response. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: ON

enableFormTagging

Enable Tagging of Forms for Field Consistency Checks. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: ON

sessionlessFieldConsistency

Enable session less Field Consistency Checks. This check is applicable to Profile Type: HTML. Possible values: OFF, ON, postOnly Default value: AS_OFF

sessionlessURLClosure

Enable session less URL Closure Checks. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

semicolonFieldSeparator

Allow ';' as a form field separator in URL queries and POST form bodies. Possible values: ON, OFF Default value: OFF

excludeFileUploadFromChecks

Exclude Uploaded Files from Form checks. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

SQLInjectionParseComments

Canonicalize SQL Comments in form fields. This check is applicable to Profile Type: HTML. Possible values: checkall, ansi, nested, ansinested Default value: AS_DEFAULT_SQLINJECTIONPARSECOMMENTS

invalidPercentHandling

Options for handling percent-encoded names and values. Possible values: apache_mode, asp_mode, secure_mode Default value: AS_PERCENT_DECODE_SECURE_MODE

type

Defines the type of the Application Firewall Profile. If the profile is of type XML, then you can only set security checks that are relevent to XML. Similary, if the profile type is HTML then you can set only security checks that are relevant to HTML. Composite profile types can have HTML and XML checks. Default value: AF_PROFILE_TYPE_HTML

checkRequestHeaders

Check for XSS and SQL injections in request headers. Possible values: ON, OFF Default value: OFF

comment

Comments associated with this profile.

Top

rm appfw profile

Synopsis

rm appfw profile <name>

Description

Remove an application firewall profile.

Parameters

name

Application firewall profile name.

Top

set appfw profile

Synopsis

set appfw profile <name> [-startURLAction <startURLAction> ...] [-startURLClosure (ON | OFF)] [-denyURLAction <denyURLAction> ...] [-RefererHeaderCheck <RefererHeaderCheck>] [-cookieConsistencyAction <cookieConsistencyAction> ...] [-cookieTransforms (ON | OFF)] [-cookieEncryption <cookieEncryption>] [-cookieProxying (none | sessionOnly)] [-addCookieFlags <addCookieFlags>] [-fieldConsistencyAction <fieldConsistencyAction> ...] [-CSRFtagAction <CSRFtagAction> ...] [-crossSiteScriptingAction <crossSiteScriptingAction> ...] [-crossSiteScriptingTransformUnsafeHTML (ON | OFF)] [-crossSiteScriptingCheckCompleteURLs (ON | OFF)] [-SQLInjectionAction <SQLInjectionAction> ...] [-SQLInjectionTransformSpecialChars (ON | OFF)] [-SQLInjectionOnlyCheckFieldsWithSQLChars (ON | OFF)] [-fieldFormatAction <fieldFormatAction> ...] [-defaultFieldFormatType <string>] [-defaultFieldFormatMinLength <positive_integer>] [-defaultFieldFormatMaxLength <positive_integer>] [-bufferOverflowAction <bufferOverflowAction> ...] [-bufferOverflowMaxURLLength <positive_integer>] [-bufferOverflowMaxHeaderLength <positive_integer>] [-bufferOverflowMaxCookieLength <positive_integer>] [-creditCardAction <creditCardAction> ...] [-creditCard <creditCard> ...] [-creditCardMaxAllowed <positive_integer>] [-creditCardXOut (ON | OFF)] [-requestContentType <string>] [-responseContentType <string>] [-XMLDoSAction <XMLDoSAction> ...] [-XMLFormatAction <XMLFormatAction> ...] [-XMLSQLInjectionAction <XMLSQLInjectionAction> ...] [-XMLSQLInjectionOnlyCheckFieldsWithSQLChars (ON | OFF)] [-XMLSQLInjectionParseComments <XMLSQLInjectionParseComments>] [-XMLXSSAction <XMLXSSAction> ...] [-XMLWSIAction <XMLWSIAction> ...] [-XMLAttachmentAction <XMLAttachmentAction> ...] [-XMLValidationAction <XMLValidationAction> ...] [-XMLErrorObject <string>] [-signatures <string>] [-XMLSOAPFaultAction <XMLSOAPFaultAction> ...] [-useHTMLErrorObject (ON | OFF)] [-errorURL <expression>] [-HTMLErrorObject <string>] [-logEveryPolicyHit (ON | OFF)] [-stripHtmlComments <stripHtmlComments>] [-stripXmlComments (none | all)] [-exemptClosureURLsFromSecurityChecks (ON | OFF)] [-defaultCharSet <string>] [-postBodyLimit <positive_integer>] [-fileUploadMaxNum <positive_integer>] [-canonicalizeHTMLResponse (ON | OFF)] [-enableFormTagging (ON | OFF)] [-sessionlessFieldConsistency <sessionlessFieldConsistency>] [-sessionlessURLClosure (ON | OFF)] [-semicolonFieldSeparator (ON | OFF)] [-excludeFileUploadFromChecks (ON | OFF)] [-SQLInjectionParseComments <SQLInjectionParseComments>] [-invalidPercentHandling <invalidPercentHandling>] [-type (HTML | XML) ...] [-checkRequestHeaders (ON | OFF)] [-comment <string>]

Description

Modify the settings for a given application firewall profile.

Parameters

name

Application firewall profile name.

startURLAction

Start URL action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. Default value: AS_DEFAULT_DISPOSITION

startURLClosure

Start URL closure. This check is applicable to Profile Type: HTML, XML. Possible values: ON, OFF Default value: OFF

denyURLAction

Deny URL action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. LEARN is not supported. Default value: AS_DEFAULT_DISPOSITION

RefererHeaderCheck

Referer header check This check is applicable to Profile Type: HTML. Possible values: OFF, if_present, always Default value: AS_HEADER_CHECK_OFF

cookieConsistencyAction

Cookie consistency action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. Default value: AS_NONE

cookieTransforms

Enable cookie transforms: encryption, proxying, and adding cookie flags. Make sure this is turned ON if you want the transforms to happen. This check is applicable to Profile Type: HTML. XML Possible values: ON, OFF

cookieEncryption

Encrypts server cookies Possible values: none, decryptOnly, encryptSessionOnly, encryptAll Default value: AS_CKI_ENCRYPT_NONE

cookieProxying

Proxy server cookies using an application firewall session Possible values: none, sessionOnly Default value: AS_CKI_PROXY_NONE

addCookieFlags

Add HttpOnly and Secure flags to cookies Possible values: none, httpOnly, secure, all Default value: AS_ADD_CKI_FLAGS_NONE

fieldConsistencyAction

Form Field Consistency action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML. Default value: AS_NONE

CSRFtagAction

Cross-site request forgery tag action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML. LEARN is not supported. Default value: AS_NONE

crossSiteScriptingAction

Cross-site scripting action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML. Default value: AS_DEFAULT_DISPOSITION

crossSiteScriptingTransformUnsafeHTML

Transform HTML characters. This check is applicable to Profile Type: HTML. Possible values: ON, OFF

crossSiteScriptingCheckCompleteURLs

Check complete URLs. This check is applicable to Profile Type: HTML. Possible values: ON, OFF

SQLInjectionAction

SQL injection action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML. Default value: AS_DEFAULT_DISPOSITION

SQLInjectionTransformSpecialChars

Transform HTML characters. This check is applicable to Profile Type: HTML. Possible values: ON, OFF

SQLInjectionOnlyCheckFieldsWithSQLChars

Check SQL characters. This check is applicable to Profile Type: HTML. Possible values: ON, OFF

fieldFormatAction

Field format action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML. Default value: AS_DEFAULT_DISPOSITION

defaultFieldFormatType

Default field type. This check is applicable to Profile Type: HTML.

defaultFieldFormatMinLength

Default field type minimum length. This check is applicable to Profile Type: HTML. Default value: AS_DEFAULTFIELDFORMAT_DEFAULT_MIN_LEN Maximum value: 65535

defaultFieldFormatMaxLength

Default field type maximum length. This check is applicable to Profile Type: HTML. Default value: AS_DEFAULTFIELDFORMAT_DEFAULT_MAX_LEN Minimum value: 1 Maximum value: 65535

bufferOverflowAction

Buffer overflow action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. LEARN is not supported. Default value: AS_DEFAULT_DISPOSITION

bufferOverflowMaxURLLength

Maximum URL length. This check is applicable to Profile Type: HTML, XML. Default value: AS_BUFFEROVERFLOW_DEFAULT_MAX_URL_LEN Maximum value: 65535

bufferOverflowMaxHeaderLength

Maximum header length. This check is applicable to Profile Type: HTML, XML. Default value: AS_BUFFEROVERFLOW_DEFAULT_MAX_HDR_LEN Maximum value: 65535

bufferOverflowMaxCookieLength

Maximum cookie length. This check is applicable to Profile Type: HTML, XML. Default value: AS_BUFFEROVERFLOW_DEFAULT_MAX_COOKIE_LEN Maximum value: 65535

creditCardAction

Credit Card action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. LEARN is not supported. Default value: AS_NONE

creditCard

Credit card. This check is applicable to Profile Type: HTML, XML. Default value: AS_CCARD_DEFAULT_CARD_TYPE

creditCardMaxAllowed

Maximum number of times a credit card number may be seen before action is taken. This check is applicable to Profile Type: HTML, XML. Maximum value: 255

creditCardXOut

X-out the credit card numbers. This check is applicable to Profile Type: HTML, XML. Possible values: ON, OFF

requestContentType

Default content-type for request messages. This binding is applicable to Profile Type: HTML, XML. Default value: NS_S_AS_DEFAULT_REQUEST_CONTENT_TYPE

responseContentType

Default content-type for response messages. This binding is applicable to Profile Type: HTML, XML. Default value: NS_S_AS_DEFAULT_RESPONSE_CONTENT_TYPE

XMLDoSAction

XML DOS action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: XML. Default value: AS_DEFAULT_DISPOSITION

XMLFormatAction

XML well-formed request action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. LEARN is not supported. Default value: AS_DEFAULT_DISPOSITION

XMLSQLInjectionAction

XML SQL injection action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. LEARN is not supported. Default value: AS_DEFAULT_DISPOSITION

XMLSQLInjectionOnlyCheckFieldsWithSQLChars

Check SQL characters. This check is applicable to Profile Type: XML. Possible values: ON, OFF

XMLSQLInjectionParseComments

Canonicalize SQL Comments in XML Data. This check is applicable to Profile Type: XML. Possible values: checkall, ansi, nested, ansinested Default value: AS_CHECKALL

XMLXSSAction

XML cross-site scripting action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. LEARN is not supported. Default value: AS_DEFAULT_DISPOSITION

XMLWSIAction

XML WS-I action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: XML. Default value: AS_DEFAULT_DISPOSITION

XMLAttachmentAction

XML attachment action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: XML. Default value: AS_DEFAULT_DISPOSITION

XMLValidationAction

XML validation action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. LEARN is not supported. Default value: AS_DEFAULT_DISPOSITION

XMLErrorObject

Object name for the xml error page. This check is applicable to Profile Type: XML. Default value: NS_S_AS_ERROROBJECT_DEFAULT

customSettings

Object name for custom settings. This check is applicable to Profile Type: HTML, XML. Default value: NS_S_AS_ERROROBJECT_DEFAULT

signatures

Object name for signatures. This check is applicable to Profile Type: HTML, XML. Default value: NS_S_AS_ERROROBJECT_DEFAULT

XMLSOAPFaultAction

XML SOAP fault filtering action types. (BLOCK | LOG | STATS | REMOVE | NONE) This check is applicable to Profile Type: XML. LEARN is not supported. Default value: AS_DEFAULT_DISPOSITION

useHTMLErrorObject

Use HTML Error object for response instead of Redirect Error URL. Possible values: ON, OFF

errorURL

Error page. This check is applicable to Profile Type: HTML. Default value: NS_S_AS_ERROR_URL_DEFAULT

HTMLErrorObject

Object name for the html error page. This check is applicable to Profile Type: HTML. Default value: NS_S_AS_ERROROBJECT_DEFAULT

logEveryPolicyHit

Log every profile match regardless of security checks results. Possible values: ON, OFF

stripComments

Strip HTML comments. This check is applicable to Profile Type: HTML. Possible values: ON, OFF

stripHtmlComments

Strip HTML comments. This check is applicable to Profile Type: HTML. Possible values: none, all, exclude_script_tag

stripXmlComments

Strip XML comments. This check is applicable to Profile Type: XML. Possible values: none, all

exemptClosureURLsFromSecurityChecks

Tells the application firewall to exempt closure URLs from security checks. This check is applicable to Profile Type: HTML. Possible values: ON, OFF

defaultCharSet

Default character set. Possible values are iso-8859-1 (English US), big5 (Chinese Traditional), gb2312 (Chinese Simplified), sjis (Japanese), euc-jp (Japanese EUC-JP), utf-8 (Unicode), and euc-kr (Korean). This check is applicable to Profile Type: HTML. Default value: NS_S_AS_CHARSET_DEFAULT Maximum value: 31

postBodyLimit

Maximum allowed post body size. This check is applicable to Profile Type: HTML, XML. Default value: AS_DEFAULT_POSTBODYLIMIT Maximum value: 1000000000

fileUploadMaxNum

Maximum allowed number of file uploads per form submission request. Setting this parameter to the maximum value of 65535 will allow an unlimited number of uploads. Default value: AS_DEFAULT_MAX_FILE_UPLOADS Maximum value: 65535

canonicalizeHTMLResponse

Entity encoding for html special characters for attributes in the response. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: ON

enableFormTagging

Enable Tagging of Forms for Field Consistency Checks. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: ON

sessionlessFieldConsistency

Enable session less Field Consistency Checks. This check is applicable to Profile Type: HTML. Possible values: OFF, ON, postOnly Default value: AS_OFF

sessionlessURLClosure

Enable session less URL Closure Checks. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

semicolonFieldSeparator

Allow ';' as a form field separator in URL queries and POST form bodies. Possible values: ON, OFF Default value: OFF

excludeFileUploadFromChecks

Exclude Uploaded Files from Form checks. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

SQLInjectionParseComments

Canonicalize SQL Comments in form fields. This check is applicable to Profile Type: HTML. Possible values: checkall, ansi, nested, ansinested Default value: AS_DEFAULT_SQLINJECTIONPARSECOMMENTS

invalidPercentHandling

Options for handling percent-encoded names and values. Possible values: apache_mode, asp_mode, secure_mode Default value: AS_PERCENT_DECODE_SECURE_MODE

type

Defines the type of the application firewall Profile. If the profile is of type XML, then you can only set security checks that are relevent to XML. Similary, if the profile type is HTML then you can set only security checks that are relevant to HTML. Composite profile types can have HTML and XML checks. Default value: AF_PROFILE_TYPE_HTML

checkRequestHeaders

Check for XSS and SQL injections in request headers. Possible values: ON, OFF Default value: OFF

comment

Comments associated with this profile.

Top

unset appfw profile

Synopsis

unset appfw profile <name> [-startURLAction] [-startURLClosure] [-denyURLAction] [-RefererHeaderCheck] [-cookieConsistencyAction] [-cookieTransforms] [-cookieEncryption] [-cookieProxying] [-addCookieFlags] [-fieldConsistencyAction] [-CSRFtagAction] [-crossSiteScriptingAction] [-crossSiteScriptingTransformUnsafeHTML] [-crossSiteScriptingCheckCompleteURLs] [-SQLInjectionAction] [-SQLInjectionTransformSpecialChars] [-SQLInjectionOnlyCheckFieldsWithSQLChars] [-fieldFormatAction] [-defaultFieldFormatType] [-defaultFieldFormatMinLength] [-defaultFieldFormatMaxLength] [-bufferOverflowAction] [-bufferOverflowMaxURLLength] [-bufferOverflowMaxHeaderLength] [-bufferOverflowMaxCookieLength] [-creditCardAction] [-creditCard] [-creditCardMaxAllowed] [-creditCardXOut] [-requestContentType] [-responseContentType] [-XMLDoSAction] [-XMLFormatAction] [-XMLSQLInjectionAction] [-XMLSQLInjectionOnlyCheckFieldsWithSQLChars] [-XMLSQLInjectionParseComments] [-XMLXSSAction] [-XMLWSIAction] [-XMLAttachmentAction] [-XMLValidationAction] [-XMLErrorObject] [-signatures] [-XMLSOAPFaultAction] [-useHTMLErrorObject] [-errorURL] [-HTMLErrorObject] [-logEveryPolicyHit] [-stripHtmlComments] [-stripXmlComments] [-exemptClosureURLsFromSecurityChecks] [-defaultCharSet] [-postBodyLimit] [-fileUploadMaxNum] [-canonicalizeHTMLResponse] [-enableFormTagging] [-sessionlessFieldConsistency] [-sessionlessURLClosure] [-semicolonFieldSeparator] [-excludeFileUploadFromChecks] [-SQLInjectionParseComments] [-invalidPercentHandling] [-type] [-checkRequestHeaders] [-comment]

Description

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

Top

bind appfw profile

Synopsis

bind appfw profile <name> (-startURL <expression> | -denyURL <expression> | (-fieldConsistency <string> <formActionURL> [-isRegex (REGEX | NOTREGEX)]) | (-cookieConsistency <string> [-isRegex (REGEX | NOTREGEX)]) | (-SQLInjection <string> <formActionURL> [-isRegex (REGEX | NOTREGEX)] [-location <location>]) | (-CSRFTag <expression> <CSRFFormActionURL>) | (-crossSiteScripting <string> <formActionURL> [-isRegex (REGEX | NOTREGEX)] [-location <location>]) | (-fieldFormat <string> <formActionURL> <fieldType> [-fieldFormatMinLength <positive_integer>] [-fieldFormatMaxLength <positive_integer>] [-isRegex (REGEX | NOTREGEX)]) | (-safeObject <string> <expression> <maxMatchLength> [-action <action> ...]) | -trustedLearningClients <ip_addr[/prefix]|ipv6_addr[/prefix]|*> | (-XMLDoSURL <expression> [-XMLMaxElementDepthCheck (ON | OFF) [-XMLMaxElementDepth <positive_integer>]] [-XMLMaxElementNameLengthCheck (ON | OFF) [-XMLMaxElementNameLength <positive_integer>]] [-XMLMaxElementsCheck (ON | OFF) [-XMLMaxElements <positive_integer>]] [-XMLMaxElementChildrenCheck (ON | OFF) [-XMLMaxElementChildren <positive_integer>]] [-XMLMaxAttributesCheck (ON | OFF) [-XMLMaxAttributes <positive_integer>]] [-XMLMaxAttributeNameLengthCheck (ON | OFF) [-XMLMaxAttributeNameLength <positive_integer>]] [-XMLMaxAttributeValueLengthCheck (ON | OFF) [-XMLMaxAttributeValueLength <positive_integer>]] [-XMLMaxCharDATALengthCheck (ON | OFF) [-XMLMaxCharDATALength <positive_integer>]] [-XMLMaxFileSizeCheck (ON | OFF) [-XMLMaxFileSize <positive_integer>]] [-XMLMinFileSizeCheck (ON | OFF) [-XMLMinFileSize <positive_integer>]] [-XMLBlockPI (ON | OFF)] [-XMLBlockDTD (ON | OFF)] [-XMLBlockExternalEntities (ON | OFF)] [-XMLMaxEntityExpansionsCheck (ON | OFF) [-XMLMaxEntityExpansions <positive_integer>]] [-XMLMaxEntityExpansionDepthCheck (ON | OFF) [-XMLMaxEntityExpansionDepth <positive_integer>]] [-XMLMaxNamespacesCheck (ON | OFF) [-XMLMaxNamespaces <positive_integer>]] [-XMLMaxNamespaceUriLengthCheck (ON | OFF) [-XMLMaxNamespaceUriLength <positive_integer>]] [-XMLSOAPArrayCheck (ON | OFF) [-XMLMaxSOAPArraySize <positive_integer>] [-XMLMaxSOAPArrayRank <positive_integer>]]) | (-XMLWSIURL <expression> [-XMLWSIChecks <string>]) | (-XMLValidationURL <expression> (-XMLRequestSchema <string> | (-XMLWSDL <string> [-XMLAdditionalSOAPHeaders (ON | OFF)] [-XMLEndPointCheck (ABSOLUTE | RELATIVE)]) | -XMLValidateSOAPEnvelope (ON | OFF)) [-XMLResponseSchema <string>] [-XMLValidateResponse (ON | OFF)]) | (-XMLAttachmentURL <expression> [-XMLMaxAttachmentSizeCheck (ON | OFF) [-XMLMaxAttachmentSize <positive_integer>]] [-XMLAttachmentContentTypeCheck (ON | OFF) [-XMLAttachmentContentType <expression>]]) | (-XMLSQLInjection <string> [-isRegex (REGEX | NOTREGEX)] [-location (ELEMENT | ATTRIBUTE)]) | (-XMLXSS <string> [-isRegex (REGEX | NOTREGEX)] [-location (ELEMENT | ATTRIBUTE)])) [-comment <string>] [-state (ENABLED | DISABLED)]

Description

Bind a security check to the application firewall profile. You can bind any number of security checks to the profile. When the profile is activated (see the add appfw global command), each security check tests the data stream for the specified condition. When a test fails, the appropriate action is determined by the action configured in the profile.

Parameters

name

Application firewall profile name.

startURL

Start URL regular expression. This binding is applicable to Profile Type: HTML, XML.

denyURL

Deny URL regular expression. This binding is applicable to Profile Type: HTML, XML.

fieldConsistency

Form field name. This binding is applicable to Profile Type: HTML.

cookieConsistency

Cookie name. This binding is applicable to Profile Type: HTML, XML.

SQLInjection

Form field, header or cookie name. This binding is applicable to Profile Type: HTML.

CSRFTag

CSRF Form Origin URL. This binding is applicable to Profile Type: HTML.

crossSiteScripting

Form field, header or cookie name. This binding is applicable to Profile Type: HTML.

fieldFormat

Field format name. This binding is applicable to Profile Type: HTML.

safeObject

Safe Object name. This binding is applicable to Profile Type: HTML, XML.

trustedLearningClients

Trusted host/network learning IP. This binding is appilicable to profile Type: HTML, XML.

comment

Comments associated with this profile.

state

Enabled. Possible values: ENABLED, DISABLED Default value: ENABLED

XMLDoSURL

XML DoS URL regular expression. This binding is applicable to Profile Type: XML.

XMLWSIURL

XML WS-I URL regular expression. This binding is applicable to Profile Type: XML.

XMLValidationURL

XML Validation URL regular expression. This binding is applicable to Profile Type: XML.

XMLAttachmentURL

XML Attachment URL regular expression. This binding is applicable to Profile Type: XML.

XMLSQLInjection

XML SQL Injection exemption field, this can be an element or an attribute name.

XMLXSS

XML XSS Injection exemption field, this can be an element or an attribute name.

Top

unbind appfw profile

Synopsis

unbind appfw profile <name> (-startURL <expression> | -denyURL <expression> | (-fieldConsistency <string> <formActionURL>) | -cookieConsistency <string> | (-SQLInjection <string> <formActionURL> [-location <location>]) | (-crossSiteScripting <string> <formActionURL> [-location <location>]) | (-fieldFormat <string> <formActionURL>) | -safeObject <string> | -trustedLearningClients <ip_addr[/prefix]|ipv6_addr[/prefix]|*> | -XMLDoSURL <expression> | -XMLWSIURL <expression> | -XMLValidationURL <expression> | -XMLAttachmentURL <expression> | (-XMLSQLInjection <string> [-location (ELEMENT | ATTRIBUTE)]) | (-XMLXSS <string> [-location (ELEMENT | ATTRIBUTE)])) [-CSRFTag <string> <CSRFFormActionURL>]

Description

Unbind a security check from the given application firewall profile.

Parameters

name

Application firewall profile name.

startURL

Start URL regular expression.

denyURL

Deny URL regular expression.

fieldConsistency

Form field name.

cookieConsistency

Cookie name.

SQLInjection

Form field, header or cookie name.

CSRFTag

CSRF Form origin URL. This binding is applicable to Profile Type: HTML.

crossSiteScripting

Form field, header or cookie name.

fieldFormat

Field format name.

safeObject

Safe Object name.

trustedLearningClients

Trusted learning Clients IP

XMLDoSURL

XML DoS URL regular expression.

XMLWSIURL

XML WS-I URL regular expression.

XMLValidationURL

XML Message URL regular expression.

XMLAttachmentURL

XML Attachment URL regular expression.

XMLSQLInjection

XML SQL Injection exemption field, this can be an element or an attribute name.

XMLXSS

XML XSS Injection exemption field, this can be an element or an attribute name.

Top

show appfw profile

Synopsis

show appfw profile [<name>]

Description

Display all application firewall profiles that currently exist.

Parameters

name

The name of the application firewall profile.

Top

stat appfw profile

Synopsis

stat appfw profile [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display appfw profile statistics.

Parameters

name

Application firewall profile name.

Example

stat appfw profile

Top

archive appfw profile

Synopsis

archive appfw profile <name> <archivename> [-comment <string>]

Description

Create archive for the profile.

Parameters

name

Application firewall profile name.

archivename

Source for tar archive.

comment

Comments associated with this profile.

Top

restore appfw profile

Synopsis

restore appfw profile <archivename>

Description

Restore configuration from archive file

Parameters

archivename

Source for tar archive.

Top

appfw policy

[add | rm | set | unset | show | stat | rename]

add appfw policy

Synopsis

add appfw policy <name> <rule> <profileName> [-comment <string>] [-logAction <string>]

Description

Create an application firewall policy.

Parameters

name

Application firewall policy name.

rule

The rule associated with the policy.

profileName

Application firewall profile name.

comment

Comments associated with this application firewall policy.

logAction

The log action associated with the application firewall policy

Top

rm appfw policy

Synopsis

rm appfw policy <name>

Description

Remove an application firewall policy.

Parameters

name

Application firewall policy name.

Top

set appfw policy

Synopsis

set appfw policy <name> [-rule <expression>] [-profileName <string>] [-comment <string>] [-logAction <string>]

Description

Modify an application firewall policy. Set a new rule/profile/comment for existing application firewall policy.

Parameters

name

Application firewall policy name.

rule

The rule associated with the policy.

profileName

Application firewall profile name.

comment

Comments associated with this application firewall policy.

logAction

The log action associated with the application firewall policy

Example

set transform policy pol9 -rule "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

Top

unset appfw policy

Synopsis

unset appfw policy <name> [-comment] [-logAction]

Description

Unset comment/logaction for existing transform policy..Refer to the set appfw policy command for meanings of the arguments.

Example

unset transform policy pol9 -undefAction

Top

show appfw policy

Synopsis

show appfw policy [<name>]

Description

Display the application firewall policies.

Parameters

name

Application firewall policy name.

Top

stat appfw policy

Synopsis

stat appfw policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display advance application firewall policy statistics.

Parameters

name

The name of the advance application firewall policy for which statistics will be displayed. If not given statistics are shown for all advance application firewall policies.

Example

stat appfw policy

Top

rename appfw policy

Synopsis

rename appfw policy <name>@ <newName>@

Description

Rename a application firewall policy.

Parameters

name

The name of the application firewall policy.

newName

The new name of the application firewall policy.

Example

rename appfw policy oldname newname

Top

appfw policylabel

[add | rm | bind | unbind | show | stat | rename]

add appfw policylabel

Synopsis

add appfw policylabel <labelName> <policylabeltype>

Description

Add a application firewall policy label.

Parameters

labelName

Name of the application firewall policy label.

policylabeltype

The type of transformations allowed by the policies bound to the label. Possible values: http_req

Example

add appfw policylabel appfw_label http_req

Top

rm appfw policylabel

Synopsis

rm appfw policylabel <labelName>

Description

Remove a application firewall policy label.

Parameters

labelName

Name of the application firewall policy label.

Example

rm appfw policylabel appfw_label

Top

bind appfw policylabel

Synopsis

bind appfw policylabel <labelName> <policyName> <priority> [<gotoPriorityExpression>] [-invoke (<labelType> <labelName>)]

Description

Bind the application firewall policy to one of the labels.

Parameters

labelName

Name of the application firewall policy label.

policyName

The transform policy name.

Example

i) bind appfw policylabel trans_http_url pol_1 1 2 -invoke reqvserver CURRENT
ii) bind appfw policylabel trans_http_url pol_2 2

Top

unbind appfw policylabel

Synopsis

unbind appfw policylabel <labelName> <policyName> [-priority <positive_integer>]

Description

Unbind entities from application firewall label.

Parameters

labelName

Name of the application firewall policy label.

policyName

The transform policy name.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind appfw policylabel appfw_label

Top

show appfw policylabel

Synopsis

show appfw policylabel [<labelName>]

Description

Display policy label or policies bound to application firewall policylabel.

Parameters

labelName

Name of the application firewall policy label.

Example

i) show appfw policylabel appfw_label
ii) show appfw policylabel

Top

stat appfw policylabel

Synopsis

stat appfw policylabel [<labelName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of application firewall policylabel(s).

Parameters

labelName

The name of the application firewall label for which statistics will be displayed. If not given statistics are shown for all application firewall policylabels.

Top

rename appfw policylabel

Synopsis

rename appfw policylabel <labelName>@ <newName>@

Description

Rename a application firewall policy label.

Parameters

labelName

The name of the application firewall policy label.

newName

The new name of the application firewall policylabel.

Example

rename appfw policylabel oldname newname

Top

appfw confidField

[add | rm | set | unset | show]

add appfw confidField

Synopsis

add appfw confidField <fieldName> <url> [-isRegex (REGEX | NOTREGEX)] [-comment <string>] [-state (ENABLED | DISABLED)]

Description

Define a form field (identified by the action URL and the field name) as confidential. These fields will have their values X'ed out in the audit logs.

Parameters

fieldName

Form field name.

url

Form action URL.

isRegex

Is field name a regular expression? Possible values: REGEX, NOTREGEX Default value: NS_NOTREGEX

comment

Comments associated with this confidential form field.

state

Enabled. Possible values: ENABLED, DISABLED Default value: ENABLED

Top

rm appfw confidField

Synopsis

rm appfw confidField <fieldName> <url>

Description

Remove a confidential field. The field values will be logged as-is in the audit logs.

Parameters

fieldName

Form field name.

url

Form action URL.

Top

set appfw confidField

Synopsis

set appfw confidField <fieldName> <url> [-comment <string>] [-state (ENABLED | DISABLED)]

Description

Modify a confidential field setting. Confidential fields have their values X'ed out in the audit logs

Parameters

fieldName

Form field name.

url

Form action URL.

comment

Comments associated with this confidential form field.

state

Enabled. Possible values: ENABLED, DISABLED Default value: ENABLED

Top

unset appfw confidField

Synopsis

unset appfw confidField <fieldName> <url> [-comment] [-state]

Description

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

Top

show appfw confidField

Synopsis

show appfw confidField [<fieldName> <url>]

Description

Display all configured confidential form fields.

Parameters

fieldName

Form field name.

url

Form action URL.

Top

appfw stats

show appfw stats

Synopsis

show appfw stats - alias for 'stat appfw'

Description

show appfw stats is an alias for stat appfw

appfw xmlerrorpage

[rm | show | import | update]

rm appfw xmlerrorpage

Synopsis

rm appfw xmlerrorpage <name>

Description

Removes the object imported by import xmlerrorpage.

Parameters

name

Indicates name of the imported xml error page to be removed.

Example

rm xmlerrorpage <name>

Top

show appfw xmlerrorpage

Synopsis

show appfw xmlerrorpage [<name>]

Description

Displays the object imported by import xmlerrorpage.

Example

show appfw xmlerrorpage

Top

import appfw xmlerrorpage

Synopsis

import appfw xmlerrorpage <src> <name> [-comment <string>] [-overwrite]

Description

Downloads the input XML Error Page to NetScaler Box with the given object name

Parameters

src

Indicates the source of the XML error page as a URL of the form <protocol>://<host>[:<port>][/<path>] <protocol> is http or https. <host> is the DNS name or IP address of the http or https server. <port> is the port number of the server. If omitted, the default port for http or https will be used. <path> is the path of the file on the server. Import will fail if an https server requires client certificate authentication.

name

Indicates name of the xml error page to import.

comment

Comments.

overwrite

Overwrites the existing file

Example

import xmlerrorpage http://www.example.com/errorpage.xml my-xml-error-page

Top

update appfw xmlerrorpage

Synopsis

update appfw xmlerrorpage <name>

Description

Reloads the XML error page of the given object name in appfw profiles

Parameters

name

Indicates name of the xml error page to update.

Example

update xmlerrorpage my-xml-error-page

Top

appfw htmlerrorpage

[rm | show | import | update]

rm appfw htmlerrorpage

Synopsis

rm appfw htmlerrorpage <name>

Description

Removes the object imported by import htmlerrorpage.

Parameters

name

Indicates name of the imported html error page to be removed.

Example

rm htmlerrorpage <name>

Top

show appfw htmlerrorpage

Synopsis

show appfw htmlerrorpage [<name>]

Description

Displays the object imported by import htmlerrorpage.

Example

show appfw htmlerrorpage

Top

import appfw htmlerrorpage

Synopsis

import appfw htmlerrorpage <src> <name> [-comment <string>] [-overwrite]

Description

Downloads the input HTML Error Page to NetScaler Box with the given object name

Parameters

src

Indicates the source of the HTML error page as a URL of the form <protocol>://<host>[:<port>][/<path>] <protocol> is http or https. <host> is the DNS name or IP address of the http or https server. <port> is the port number of the server. If omitted, the default port for http or https will be used. <path> is the path of the file on the server. Import will fail if an https server requires client certificate authentication.

name

Indicates name of the html error page to import.

comment

Comments.

overwrite

Overwrites the existing file

Example

import htmlerrorpage http://www.example.com/errorpage.html my-html-error-page

Top

update appfw htmlerrorpage

Synopsis

update appfw htmlerrorpage <name>

Description

Reloads the HTML error page of the given object name in appfw profiles

Parameters

name

Indicates name of the html error page to update.

Example

update htmlerrorpage my-html-error-page

Top

appfw settings

[set | unset | show]

set appfw settings

Synopsis

set appfw settings [-defaultProfile <string>] [-undefAction <string>] [-sessionTimeout <positive_integer>] [-learnRateLimit <positive_integer>] [-sessionLifetime <positive_integer>] [-sessionCookieName <string>] [-clientIPLoggingHeader <string>] [-importSizeLimit <positive_integer>] [-cookiePostEncryptPrefix <string>] [-logMalformedReq (ON | OFF)] [-CEFLogging (ON | OFF)] [-entityDecoding (ON | OFF)] [-useConfigurableSecretKey (ON | OFF)]

Description

Set the global settings for the application firewall module. Changes in these settings are applied to all application firewall profiles.

Parameters

defaultProfile

Application firewall global default profile. Default value: AS_ENGINESETTINGS_DEFAULT_PROF_DEFAULT

undefAction

Application firewall global undefined profile. Default value: AS_ENGINESETTINGS_UNDEF_PROF_DEFAULT

sessionTimeout

The user session timeout (in seconds). After this many seconds of no user activity, the session is terminated and the user must establish a new session before continuing to use the protected web site. Default value: AS_ENGINESETTINGS_SESSIONTIMEOUT_DEFAULT Minimum value: 1 Maximum value: 65535

learnRateLimit

The AppFw learn messages rate limit value (in messages per second). The extra learn messages are dropped when the rate goes above this value. Default value: AS_ENGINESETTINGS_LEARN_RATE_LIMIT_DEFAULT Minimum value: 1 Maximum value: 1000

sessionLifetime

The user session lifetime (in seconds). If a session has existed more than the specified number of seconds, the session can be terminated and the user must establish a new session before continuing to use the protected web site. Default value: AS_ENGINESETTINGS_SESSIONLIFETIME_DEFAULT Maximum value: 2147483647

sessionCookieName

The name of the session cookie set by the application firewall to track the user session. Default value: NS_S_AS_DEFAULT_COOKIE_NAME

clientIPLoggingHeader

The name of the header that holds downstream IP address for logging purposes.

importSizeLimit

Total import size limit. Default value: AS_ENGINESETTINGS_IMPORTSIZELIMIT_DEFAULT Minimum value: 1 Maximum value: 134217728

cookiePostEncryptPrefix

String which is prepended to all encrypted cookie values Default value: NS_S_AS_DEFAULT_CKI_POST_ENCRYPT_PREFIX

logMalformedReq

Log requests that are so malformed that AppFw parsing doesn't happen Possible values: ON, OFF Default value: ON

CEFLogging

Enable CEF formatted logging. Possible values: ON, OFF Default value: OFF

entityDecoding

Decode Entity-Encoded characters before doing AppFw checks. Possible values: ON, OFF Default value: OFF

useConfigurableSecretKey

Use configurable secret key in AppFw operations Possible values: ON, OFF Default value: OFF

Top

unset appfw settings

Synopsis

unset appfw settings [-defaultProfile] [-undefAction] [-sessionTimeout] [-learnRateLimit] [-sessionLifetime] [-sessionCookieName] [-clientIPLoggingHeader] [-importSizeLimit] [-cookiePostEncryptPrefix] [-logMalformedReq] [-CEFLogging] [-entityDecoding] [-useConfigurableSecretKey]

Description

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

Top

show appfw settings

Synopsis

show appfw settings

Description

Display the global settings for the application firewall module.

Top

appfw global

[bind | unbind | show]

bind appfw global

Synopsis

bind appfw global <policyName> <priority> [-state (ENABLED | DISABLED)] [<gotoPriorityExpression>] [-type <type>] [-invoke (<labelType> <labelName>)]

Description

Activate an application firewall policy.

Parameters

policyName

Application firewall policy name.

Top

unbind appfw global

Synopsis

unbind appfw global <policyName> [-type <type>] [-priority <positive_integer>]

Description

Deactivate an application firewall policy.

Parameters

policyName

Application firewall policy name.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Top

show appfw global

Synopsis

show appfw global [-type <type>]

Description

Display the active application firewall policies.

Parameters

type

The bindpoint to which to policy is bound. This can be used with advance application firewall policy only. Possible values: REQ_OVERRIDE, REQ_DEFAULT, NONE

Top

appfw learningsettings

[set | unset | show]

set appfw learningsettings

Synopsis

set appfw learningsettings <profileName> [-startURLMinThreshold <positive_integer>] [-startURLPercentThreshold <positive_integer>] [-cookieConsistencyMinThreshold <positive_integer>] [-cookieConsistencyPercentThreshold <positive_integer>] [-CSRFtagMinThreshold <positive_integer>] [-CSRFtagPercentThreshold <positive_integer>] [-fieldConsistencyMinThreshold <positive_integer>] [-fieldConsistencyPercentThreshold <positive_integer>] [-crossSiteScriptingMinThreshold <positive_integer>] [-crossSiteScriptingPercentThreshold <positive_integer>] [-SQLInjectionMinThreshold <positive_integer>] [-SQLInjectionPercentThreshold <positive_integer>] [-fieldFormatMinThreshold <positive_integer>] [-fieldFormatPercentThreshold <positive_integer>] [-XMLWSIMinThreshold <positive_integer>] [-XMLWSIPercentThreshold <positive_integer>] [-XMLAttachmentMinThreshold <positive_integer>] [-XMLAttachmentPercentThreshold <positive_integer>]

Description

Set the application firewall learning settings.

Parameters

profileName

Application firewall profile name.

startURLMinThreshold

Minimum threshold to learn Start URLs. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

startURLPercentThreshold

Minimum threshold (in percent) to learn Start URLs. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

cookieConsistencyMinThreshold

Minimum threshold to learn cookie consistency information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

cookieConsistencyPercentThreshold

Minimum threshold (in percent) to learn cookie consistency information. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

CSRFtagMinThreshold

Minimum threshold to learn CSRF tag information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

CSRFtagPercentThreshold

Minimum threshold (in percent) to learn CSRF tag information. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

fieldConsistencyMinThreshold

Minimum threshold to learn field consistency information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

fieldConsistencyPercentThreshold

Minimum threshold (in percent) to learn field consistency information. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

crossSiteScriptingMinThreshold

Minimum threshold to learn cross-site scripting information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

crossSiteScriptingPercentThreshold

Minimum threshold (in percent) to learn cross-site scripting information. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

SQLInjectionMinThreshold

Minimum threshold to learn SQL injection information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

SQLInjectionPercentThreshold

Minimum threshold (in percent) to learn SQL injection information. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

fieldFormatMinThreshold

Minimum threshold to learn field format information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

fieldFormatPercentThreshold

Minimum threshold (in percent) to learn field format information. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

XMLWSIMinThreshold

Minimum threshold to learn XML Web Services Interoperability information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

XMLWSIPercentThreshold

Minimum threshold (in percent) to learn XML Web Services Interoperability information. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

XMLAttachmentMinThreshold

Minimum threshold to learn XML Attachment information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

XMLAttachmentPercentThreshold

Minimum threshold (in percent) to learn XML Attachment information. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

Top

unset appfw learningsettings

Synopsis

unset appfw learningsettings <profileName> [-startURLMinThreshold] [-startURLPercentThreshold] [-cookieConsistencyMinThreshold] [-cookieConsistencyPercentThreshold] [-CSRFtagMinThreshold] [-CSRFtagPercentThreshold] [-fieldConsistencyMinThreshold] [-fieldConsistencyPercentThreshold] [-crossSiteScriptingMinThreshold] [-crossSiteScriptingPercentThreshold] [-SQLInjectionMinThreshold] [-SQLInjectionPercentThreshold] [-fieldFormatMinThreshold] [-fieldFormatPercentThreshold] [-XMLWSIMinThreshold] [-XMLWSIPercentThreshold] [-XMLAttachmentMinThreshold] [-XMLAttachmentPercentThreshold]

Description

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

Top

show appfw learningsettings

Synopsis

show appfw learningsettings [<profileName>]

Description

Display the application firewall learning settings.

Parameters

profileName

Application firewall profile name.

Top

appfw learningdata

[rm | show | reset | export]

rm appfw learningdata

Synopsis

rm appfw learningdata <profileName> (-startURL <expression> | -cookieConsistency <string> | (-fieldConsistency <string> <formActionURL>) | (-crossSiteScripting <string> <formActionURL>) | (-SQLInjection <string> <formActionURL>) | (-fieldFormat <string> <formActionURL>) | (-CSRFTag <expression> <CSRFFormOriginURL>) | -XMLDoSCheck <expression> | -XMLWSICheck <expression> | -XMLAttachmentCheck <expression>) [-TotalXMLRequests]

Description

Remove some raw application firewall learning data.

Parameters

profileName

Application firewall profile name.

startURL

Start URL configuration.

cookieConsistency

Cookie Name.

fieldConsistency

Form field name.

crossSiteScripting

Cross-site scripting.

SQLInjection

Form field name.

fieldFormat

Field format name.

CSRFTag

CSRF Form Action URL

XMLDoSCheck

XML Denial of Service check, one of MaxAttributes MaxAttributeNameLength MaxAttributeValueLength MaxElementNameLength MaxFileSize MinFileSize MaxCDATALength MaxElements MaxElementDepth MaxElementChildren NumDTDs NumProcessingInstructions NumExternalEntities MaxEntityExpansions MaxEntityExpansionDepth MaxNamespaces MaxNamespaceUriLength MaxSOAPArraySize MaxSOAPArrayRank

XMLWSICheck

Web Services Interoperability Rule ID.

XMLAttachmentCheck

XML Attachment Content-Type.

TotalXMLRequests

Total XML requests.

Top

show appfw learningdata

Synopsis

show appfw learningdata <profileName> <securityCheck>

Description

Display the raw application firewall learning data.

Parameters

profileName

Application firewall profile name.

securityCheck

Security check. Possible values: startURL, cookieConsistency, fieldConsistency, crossSiteScripting, SQLInjection, fieldFormat, CSRFtag, XMLDoSCheck, XMLWSICheck, XMLAttachmentCheck, TotalXMLRequests

Top

reset appfw learningdata

Synopsis

reset appfw learningdata

Description

Remove all databases. Make transaction count zero

Top

export appfw learningdata

Synopsis

export appfw learningdata <profileName> <securityCheck> [-target <string>]

Description

Export appfw learnt data in csv format to the location /var/learnt_data/

Parameters

profileName

Application firewall profile name.

securityCheck

Security check. Possible values: startURL, cookieConsistency, fieldConsistency, crossSiteScripting, SQLInjection, fieldFormat, CSRFtag, XMLDoSCheck, XMLWSICheck, XMLAttachmentCheck, TotalXMLRequests

target

Target filename for data to be exported.

Top

appfw wsdl

[rm | show | import]

rm appfw wsdl

Synopsis

rm appfw wsdl <name>

Description

Removes the object imported by import wsdl.

Parameters

name

Indicates name of the imported wsdl to be removed.

Example

rm wsdl <name>

Top

show appfw wsdl

Synopsis

show appfw wsdl [<name>]

Description

Displays the object imported by import wsdl.

Parameters

name

Indicates name of the importd wsdl to be displayed.

Example

show appfw wsdl

Top

import appfw wsdl

Synopsis

import appfw wsdl <src> <name> [-comment <string>] [-overwrite]

Description

Compiles the input WSDL file into NetScaler native format.

Parameters

src

Indicates the source of the WSDL file as a URL of the form <protocol>://<host>[:<port>][/<path>] <protocol> is http or https. <host> is the DNS name or IP address of the http or https server. <port> is the port number of the server. If omitted, the default port for http or https will be used. <path> is the path of the file on the server. Import will fail if an https server requires client certificate authentication. If the path contains a '?', escape the '?' with a backslash

name

Indicates name of the wsdl to import.

comment

Comments.

overwrite

Overwrites the existing file

Example

import appfw wsdl http://www.webservicex.net/stockquote.asmx?wsdl stockquote

Top

appfw signatures

[rm | show | import | update]

rm appfw signatures

Synopsis

rm appfw signatures <name>

Description

Removes the object imported by import signatures.

Parameters

name

Indicates name of signature object.

Example

rm signatures <name>

Top

show appfw signatures

Synopsis

show appfw signatures [<name>]

Description

Displays the object imported by import signatures.

Parameters

name

Indicates name of signature object.

Example

show appfw signatures

Top

import appfw signatures

Synopsis

import appfw signatures <src> <name> [-xslt <string>] [-comment <string>] [-overwrite]

Description

Downloads the application firewall signatures XML configuration to the NetScaler Box with the given object name

Parameters

src

Indicates the source of the signature file as a URL of the form <protocol>://<host>[:<port>][/<path>] <protocol> is http or https. <host> is the DNS name or IP address of the http or https server. <port> is the port number of the server. If omitted, the default port for http or https will be used. <path> is the path of the file on the server. Import will fail if an https server requires client certificate authentication.

name

Indicates name of signature object.

xslt

XSLT file source.

comment

Comments.

overwrite

Overwrites the existing file

Example

import signatures http://www.example.com/ns/signatures.xml my-signature

Top

update appfw signatures

Synopsis

update appfw signatures <name>

Description

Updates the application firewall signatures XML configuration to the NetScaler Box with the given object name

Parameters

name

Indicates name of the signature object to update.

Example

update signatures my-signatures

Top

appfw xmlschema

[rm | show | import]

rm appfw xmlschema

Synopsis

rm appfw xmlschema <name>

Description

Removes the object imported by import xmlschema.

Parameters

name

Indicates name of the imported xmlschema to be removed.

Example

rm xmlschema <name>

Top

show appfw xmlschema

Synopsis

show appfw xmlschema [<name>]

Description

Displays the object imported by import xmlschema.

Parameters

name

Indicates name of the imported xmlschema to be displayed.

Example

show appfw xmlschema

Top

import appfw xmlschema

Synopsis

import appfw xmlschema <src> <name> [-comment <string>] [-overwrite]

Description

Compiles the input XML Schema file into NetScaler native format.

Parameters

src

Indicates the source of the XML schema file as a URL of the form <protocol>://<host>[:<port>][/<path>] <protocol> is http or https. <host> is the DNS name or IP address of the http or https server. <port> is the port number of the server. If omitted, the default port for http or https will be used. <path> is the path of the file on the server. Import will fail if an https server requires client certificate authentication.

name

Indicates name of the xmlschema to import.

comment

Comments.

overwrite

Overwrites the existing file

Example

import xmlschema http://schemas.xmlsoap.org/soap/envelope/ soap

Top

appfw XMLContentType

[add | rm | show]

add appfw XMLContentType

Synopsis

add appfw XMLContentType <XMLContenttypevalue> [-isRegex (REGEX | NOTREGEX)]

Description

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

Parameters

XMLContenttypevalue

Content type to be classified as XML

isRegex

Is field name a regular expression? Possible values: REGEX, NOTREGEX Default value: NS_NOTREGEX

Top

rm appfw XMLContentType

Synopsis

rm appfw XMLContentType <XMLContenttypevalue>

Description

Remove XML contenti type.

Parameters

XMLContenttypevalue

Content type to be classified as XML

Top

show appfw XMLContentType

Synopsis

show appfw XMLContentType [<XMLContenttypevalue>]

Description

Display all xml content types.

Parameters

XMLContenttypevalue

Content type to be classified as XML

Top

appfw archive

[show | export | import | rm]

show appfw archive

Synopsis

show appfw archive

Example

show appfw archive

Top

export appfw archive

Synopsis

export appfw archive <name> <target>

Description

Exports the archive file to the specified location

Parameters

name

Name of tar archive

target

Path to the file to be exported

Top

import appfw archive

Synopsis

import appfw archive <src> <name> [-comment <string>]

Description

Imports the archive file from specified location

Parameters

src

Indicates the source of the tar archive file as a URL of the form <protocol>://<host>[:<port>][/<path>] <protocol> is http or https. <host> is the DNS name or IP address of the http or https server. <port> is the port number of the server. If omitted, the default port for http or https will be used. <path> is the path of the file on the server. Import will fail if an https server requires client certificate authentication.

name

Indicates name of archive

comment

Comments associated with this archive.

Top

rm appfw archive

Synopsis

rm appfw archive <name>

Description

Removes the archive created by archive command.

Parameters

name

Indicates name of the archive to be removed.

Example

rm appfw archive <name>

Top

Audit Commands

This group of commands can be used to perform operations on the following entities:

- audit
- audit syslogAction
- audit syslogPolicy
- audit nslogAction
- audit nslogPolicy
- audit messageaction
- audit stats
- audit messages
- audit syslogParams
- audit nslogParams

audit

stat audit

Synopsis

stat audit [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display the audit statistics

audit syslogAction

[add | rm | set | unset | show]

add audit syslogAction

Synopsis

add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> ... [-dateFormat (MMDDYYYY | DDMMYYYY)] [-logFacility <logFacility>] [-tcp (NONE | ALL)] [-acl (ENABLED | DISABLED)] [-timeZone (GMT_TIME | LOCAL_TIME)] [-userDefinedAuditlog (YES | NO)] [-appflowExport (ENABLED | DISABLED)]

Description

Add an syslog action

Parameters

name

The name of the syslog action.

serverIP

The IP address of the syslog server.

serverPort

The port on which the syslog server is running. Minimum value: 1

logLevel

The audit log level.

dateFormat

The date format. Possible values: MMDDYYYY, DDMMYYYY

logFacility

The log facility (RFC 3164). Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp

Log the tcp messages Possible values: NONE, ALL

acl

Log the acl messages Possible values: ENABLED, DISABLED

timeZone

Specifies the timezone in which the timestmps in the log messages will be generated Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog

Specifies whether the user configurable log messages should be done or not Possible values: YES, NO

appflowExport

Control export of log messages to AppFlow collectors. Possible values: ENABLED, DISABLED

Top

rm audit syslogAction

Synopsis

rm audit syslogAction <name>

Description

Remove a previously configured syslog action. Note that the syslog action cannot be removed if it is bound to a syslog policy.

Parameters

name

The name of the action .

Top

set audit syslogAction

Synopsis

set audit syslogAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-logLevel <logLevel> ...] [-dateFormat (MMDDYYYY | DDMMYYYY)] [-logFacility <logFacility>] [-tcp (NONE | ALL)] [-acl (ENABLED | DISABLED)] [-timeZone (GMT_TIME | LOCAL_TIME)] [-userDefinedAuditlog (YES | NO)] [-appflowExport (ENABLED | DISABLED)]

Description

Modify an existing syslog action.

Parameters

name

The name for the syslog action.

serverIP

The IP address of the syslog server.

serverPort

The port on which the syslog server is running. Minimum value: 1

logLevel

The audit log level.

dateFormat

The date format. Possible values: MMDDYYYY, DDMMYYYY

logFacility

The log facility (RFC 3164). Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp

Log the tcp messages Possible values: NONE, ALL

acl

Log the acl messages Possible values: ENABLED, DISABLED

timeZone

Specifies the timezone in which the timestmps in the log messages will be generated Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog

Specifies whether the user configurable log messages should be done or not Possible values: YES, NO

appflowExport

Control export of log messages to AppFlow collectors. Possible values: ENABLED, DISABLED

Top

unset audit syslogAction

Synopsis

unset audit syslogAction <name> [-serverPort] [-logLevel] [-dateFormat] [-logFacility] [-tcp] [-acl] [-timeZone] [-userDefinedAuditlog] [-appflowExport] [-serverIP]

Description

Reset an existing syslog action..Refer to the set audit syslogAction command for meanings of the arguments.

Top

show audit syslogAction

Synopsis

show audit syslogAction [<name>]

Description

Display details of the configured syslog action(s).

Parameters

name

The name of the syslog action. If no syslog action name is provided, all the configured syslog actions will be displayed.

Top

audit syslogPolicy

[add | rm | set | show]

add audit syslogPolicy

Synopsis

add audit syslogPolicy <name> <rule> <action>

Description

Add a syslog policy. The policy defines the conditions under which the specified syslog server will be used for logging.

Parameters

name

The name of syslog policy.

rule

The name of the rule or expression that the policy will use. Currently supports only the rule "ns_true".

action

The name of the syslog action to be bound to the the policy.

Top

rm audit syslogPolicy

Synopsis

rm audit syslogPolicy <name>

Description

Remove an audit syslog policy.

Parameters

name

The name of the syslog policy.

Top

set audit syslogPolicy

Synopsis

set audit syslogPolicy <name> [-rule <expression>] [-action <string>]

Description

Modify the properties of a syslog policy.

Parameters

name

The name of syslog policy.

rule

The name of the rule or expression that the policy will use. Currently supports only the rule "ns_true".

action

The name of the syslog action to be bound to the the policy.

Top

show audit syslogPolicy

Synopsis

show audit syslogPolicy [<name>]

Description

Display the configured syslog policies.

Parameters

name

The name of the policy to be displayed. If the policy name is not provided, all the configured syslog policies will be displayed.

Top

audit nslogAction

[add | rm | set | unset | show]

add audit nslogAction

Synopsis

add audit nslogAction <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> ...
[-dateFormat (MMDDYYYY | DDMMYYYY)] [-logFacility <logFacility>] [-tcp (NONE | ALL)]
[-acl (ENABLED | DISABLED)] [-timeZone (GMT_TIME | LOCAL_TIME)]
[-userDefinedAuditlog (YES | NO)] [-appflowExport (ENABLED | DISABLED)]

Description

Add an nslog action

Parameters

name

The name of the nslog action.

serverIP

The IP address of the nslog server.

serverPort

The port on which the nslog server is running. Minimum value: 1

logLevel

The audit log level.

dateFormat

The date format. Possible values: MMDDYYYY, DDMMYYYY

logFacility

The log facility (RFC 3164). Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp

Log the tcp messages Possible values: NONE, ALL

acl

Log the acl messages Possible values: ENABLED, DISABLED

timeZone

Specifies the timezone in which the timestmps in the log messages will be generated Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog

Specifies whether the user configurable log messages should be done or not Possible values: YES, NO

appflowExport

Control export of log messages to AppFlow collectors. Possible values: ENABLED, DISABLED

Top

rm audit nslogAction

Synopsis

rm audit nslogAction <name>

Description

Remove a previously configured nslog action. Note that the nslog action cannot be removed if it is bound to an nslog policy.

Parameters

name

The name of the nslog action.

Top

set audit nslogAction

Synopsis

set audit nslogAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-logLevel <logLevel> ...] [-dateFormat (MMDDYYYY | DDMMYYYY)] [-logFacility <logFacility>] [-tcp (NONE | ALL)] [-acl (ENABLED | DISABLED)] [-timeZone (GMT_TIME | LOCAL_TIME)] [-userDefinedAuditlog (YES | NO)] [-appflowExport (ENABLED | DISABLED)]

Description

Modify an existing nslog action.

Parameters

name

The name for the nslog action.

serverIP

The IP address of the nslog server.

serverPort

The port on which the nslog server is running. Minimum value: 1

logLevel

The audit log level.

dateFormat

The date format. Possible values: MMDDYYYY, DDMMYYYY

logFacility

The log facility (RFC 3164). Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp

Log the tcp messages Possible values: NONE, ALL

acl

Log the acl messages Possible values: ENABLED, DISABLED

timeZone

Specifies the timezone in which the timestmps in the log messages will be generated Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog

Specifies whether the user configurable log messages should be done or not Possible values: YES, NO

appflowExport

Control export of log messages to AppFlow collectors. Possible values: ENABLED, DISABLED

Top

unset audit nslogAction

Synopsis

unset audit nslogAction <name> [-serverPort] [-logLevel] [-dateFormat] [-logFacility] [-tcp] [-acl] [-timeZone] [-userDefinedAuditlog] [-appflowExport]

Description

Unsets an existing nslog action..Refer to the set audit nslogAction command for meanings of the arguments.

Top

show audit nslogAction

Synopsis

show audit nslogAction [<name>]

Description

Display details of the configured nslog action(s).

Parameters

name

The name of the nslog action. If the nslog action name is not provided, all of the configured nslog actions will be displayed.

Top

audit nslogPolicy

[add | rm | set | show]

add audit nslogPolicy

Synopsis

add audit nslogPolicy <name> <rule> <action>

Description

Add an nslog policy. The policy defines the conditions under which the specified nslog server will be used for logging.

Parameters

name

The name of nslog policy.

rule

The name of the rule or expression that the policy will use. Currently supports only the rule "ns_true".

action

The name of the nslog action to be bound to the nslog policy.

Top

rm audit nslogPolicy

Synopsis

rm audit nslogPolicy <name>

Description

Remove an nslog policy.

Parameters

name

The name of the nslog policy.

Top

set audit nslogPolicy

Synopsis

set audit nslogPolicy <name> [-rule <expression>] [-action <string>]

Description

Modify properties of a nslog policy.

Parameters

name

The name of the nslog policy to be modified.

rule

The new rule to be associated with the policy.

action

The new nslog action to be associated with the policy.

Top

show audit nslogPolicy

Synopsis

show audit nslogPolicy [<name>]

Description

Display configured nslog policies.

Parameters

name

The name of the nslog policy. If an nslog policy name is not provided, all of the configured nslog policies will be displayed.

Top

audit messageaction

[add | rm | set | unset | show]

add audit messageaction

Synopsis

add audit messageaction <name> <logLevel> <stringBuilderExpr> [-logtoNewnslog (YES | NO)] [-bypassSafetyCheck (YES | NO)]

Description

Add a audit message action

Parameters

name

The name of the audit message action.

logLevel

The audit logLevel, which specifies the severity level of the log message being generated. Possible values: EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG

stringBuilderExpr

String builder expression which is a regular expression which will be used to build the log message

logtoNewnslog

The flag to control whether the message should go to the newnslog or not Possible values: YES, NO

bypassSafetyCheck

Bypass the safety check and allow unsafe expressions. Possible values: YES, NO Default value: NO

Top

rm audit messageaction

Synopsis

rm audit messageaction <name>

Description

Remove a previously configured audit message action

Parameters

name

The name of the action .

Top

set audit messageaction

Synopsis

set audit messageaction <name> [-logLevel <logLevel>] [-stringBuilderExpr <string>] [-logtoNewnslog (YES | NO)] [-bypassSafetyCheck (YES | NO)]

Description

Set a audit message action

Parameters

name

The name of the audit message action

logLevel

Set the audit logLevel, which specifies the severity level of the log message being generated. Possible values: EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG

stringBuilderExpr

Set the string builder expression which is a regular expression which will be used to build the log message

logtoNewnslog

Set the flag to control whether the message should go to the newnslog or not Possible values: YES, NO

bypassSafetyCheck

Bypass the safety check and allow unsafe expressions. Possible values: YES, NO Default value: NO

Top

unset audit messageaction

Synopsis

unset audit messageaction <name> [-logtoNewnslog] [-bypassSafetyCheck]

Description

Use this command to remove audit messageaction settings.Refer to the set audit messageaction command for meanings of the arguments.

Top

show audit messageaction

Synopsis

show audit messageaction [<name>]

Description

Display details of the configured syslog action(s).

Parameters

name

The name of the syslog action. If no syslog action name is provided, all the configured syslog actions will be displayed.

Top

audit stats

show audit stats

Synopsis

show audit stats - alias for 'stat audit'

Description

show audit stats is an alias for stat audit

audit messages

show audit messages

Synopsis

show audit messages [-logLevel <logLevel> ...] [-numOfMesgs <positive_integer>]

Description

display the most recent audit log messages

Parameters

logLevel

The log level filter.

numOfMesgs

The number of log messages to be printed. Default value: 20 Minimum value: 1 Maximum value: 256

audit syslogParams

[set | unset | show]

set audit syslogParams

Synopsis

set audit syslogParams [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-dateFormat (MMDDYYYY | DDMMYYYY)] [-logLevel <logLevel> ...] [-logFacility <logFacility>] [-tcp (NONE | ALL)] [-acl (ENABLED | DISABLED)] [-timeZone (GMT_TIME | LOCAL_TIME)] [-userDefinedAuditlog (YES | NO)] [-appflowExport (ENABLED | DISABLED)]

Description

Modify the syslog parameters.

Parameters

serverIP

The IP address of the syslog server.

serverPort

The port on which the syslog server is running. Minimum value: 1

dateFormat

The date format. Possible values: MMDDYYYY, DDMMYYYY

logLevel

The audit log level for which messages should be logged.

logFacility

The log facility (RFC 3164). Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp

Log the tcp messages Possible values: NONE, ALL

acl

Log the acl messages Possible values: ENABLED, DISABLED

timeZone

Specifies the timezone in which the timestmps in the log messages will be generated Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog

Specifies whether the user configurable log messages should be done or not Possible values: YES, NO

appflowExport

Control export of log messages to AppFlow collectors. Possible values: ENABLED, DISABLED

Top

unset audit syslogParams

Synopsis

unset audit syslogParams [-serverIP] [-serverPort] [-logLevel] [-dateFormat] [-logFacility] [-tcp] [-acl] [-timeZone] [-userDefinedAuditlog] [-appflowExport]

Description

Unset syslog parameters.Refer to the set audit syslogParams command for meanings of the arguments.

Top

show audit syslogParams

Synopsis

show audit syslogParams

Description

Display configured syslog params.

Top

audit nslogParams

[set | unset | show]

set audit nslogParams

Synopsis

set audit nslogParams [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-dateFormat (MMDDYYYY | DDMMYYYY)] [-logLevel <logLevel> ...] [-logFacility <logFacility>] [-tcp (NONE | ALL)] [-acl (ENABLED | DISABLED)] [-timeZone (GMT_TIME | LOCAL_TIME)] [-userDefinedAuditlog (YES | NO)] [-appflowExport (ENABLED | DISABLED)]

Description

Modify the nslog parameters

Parameters

serverIP

The IP address of the nslog server.

serverPort

The port on which the nslog server is running. Minimum value: 1

dateFormat

The date format. Possible values: MMDDYYYY, DDMMYYYY

logLevel

The audit log level for which messages should be logged.

logFacility

The log facility (RFC 3164). Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp

Log the tcp messages Possible values: NONE, ALL

acl

Log the acl messages Possible values: ENABLED, DISABLED

timeZone

Specifies the timezone in which the timestamps in the log messages will be generated Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog

Specifies whether the user configurable log messages should be done or not Possible values: YES, NO

appflowExport

Control export of log messages to AppFlow collectors. Possible values: ENABLED, DISABLED

Top

unset audit nslogParams

Synopsis

unset audit nslogParams [-serverIP] [-serverPort] [-logLevel] [-dateFormat] [-logFacility] [-tcp] [-acl] [-timeZone] [-userDefinedAuditlog] [-appflowExport]

Description

Unset nslog parameters.Refer to the set audit nslogParams command for meanings of the arguments.

Top

show audit nslogParams

Synopsis

show audit nslogParams

Description

Display configured nslog params.

Top

Authentication Commands

This group of commands can be used to perform operations on the following entities:

- authentication radiusAction
- authentication ldapAction
- authentication tacacsAction
- authentication negotiateAction
- authentication samlAction
- authentication certAction
- authentication localPolicy
- authentication radiusPolicy
- authentication certPolicy
- authentication ldapPolicy
- authentication tacacsPolicy
- authentication negotiatePolicy
- authentication samlPolicy
- authentication vserver

authentication radiusAction

[add | rm | set | unset | show]

add authentication radiusAction

Synopsis

add authentication radiusAction <name> {-serverIP <ip_addr|ipv6_addr|*>} [-serverPort <port>] [-authTimeout <positive_integer>] {-radKey } [-radNASip (ENABLED | DISABLED)] [-radNASid <string>] [-radVendorID <positive_integer>] [-radAttributeType <positive_integer>] [-radGroupsPrefix <string>] [-radGroupSeparator <string>] [-passEncoding <passEncoding>] [-ipVendorID <positive_integer>] [-ipAttributeType <positive_integer>] [-accounting (ON | OFF)] [-pwdVendorID <positive_integer> [-pwdAttributeType <positive_integer>]]

Description

Add a profile for a RADIUS server. The profile contains all the configuration data necessary to communicate with a RADIUS server.

Parameters

name

The name of the RADIUS action.

serverIP

The IP address of the RADIUS server.

serverPort

The port on which the RADIUS Server is running. Default value: 1812 Minimum value: 1

authTimeout

The maximum number of seconds the system will wait for a response from the RADIUS server. Default value: 3 Minimum value: 1

radKey

The key shared between the client and the server. This information is required for the system to communicate with the RADIUS server.

radNASip

If enabled, the system's IP address (NSIP) is sent to the server as the "nasip" (Network Access Server IP) in accordance with the RADIUS protocol. Possible values: ENABLED, DISABLED

radNASid

If configured, this string is sent to the RADIUS server as the "nasid" (Network Access Server ID) in accordance with the RADIUS protocol.

radVendorID

The vendor ID for using RADIUS group extraction. Minimum value: 1

radAttributeType

The Attribute type for using RADIUS group extraction. Minimum value: 1

radGroupsPrefix

The groups prefix string that precedes the group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator

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

passEncoding

This option specifies how passwords should be encoded in the radius packets traveling from the system to the RADIUS server. Possible values: pap, chap, mschapv1, mschapv2 Default value: AAA_PAP

ipVendorID

The vendor ID of the attribute in the RADIUS response which denotes the intranet IP. The value of 0 denotes that the attribute is not vendor encoded.

ipAttributeType

The attribute type of the remote IP address attribute in a RADIUS response. Minimum value: 1

accounting

The state of the RADIUS server that will receive accounting messages. Possible values: ON, OFF

pwdVendorID

Vendor ID of the attribute in the RADIUS response which will be used to extract the user Password. Minimum value: 1

pwdAttributeType

Attribute type of the vendor specific Password-Attribute in a RADIUS response. Minimum value: 1

Top

rm authentication radiusAction

Synopsis

rm authentication radiusAction <name>

Description

Remove a previously created RADIUS action. Note that an action cannot be removed as long as it is configured in a policy.

Parameters

name

The name of the action to be removed.

Top

set authentication radiusAction

Synopsis

set authentication radiusAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-authTimeout <positive_integer>] {-radKey } [-radNASip (ENABLED | DISABLED)] [-radNASid <string>] [-radVendorID <positive_integer>] [-radAttributeType <positive_integer>] [-radGroupsPrefix <string>] [-radGroupSeparator <string>] [-passEncoding <passEncoding>] [-ipVendorID <positive_integer>] [-ipAttributeType <positive_integer>] [-accounting (ON | OFF)] [-pwdVendorID <positive_integer>] [-pwdAttributeType <positive_integer>]

Description

Change the profile for a RADIUS server. The profile contains all the configuration data needed to communicate with a RADIUS server.

Parameters

name

The name of the RADIUS action.

serverIP

The IP address of the RADIUS server.

serverPort

The port on which RADIUS Server is running. Default value: 1812 Minimum value: 1

authTimeout

The maximum number of seconds the system will wait for a response from the RADIUS server. Default value: 3 Minimum value: 1

radKey

The key shared between the client and the server. This information is required for the system to communicate with the RADIUS server.

radNASip

If enabled, the system's IP address (NSIP) is sent to the server as the "nasip" (Network Access Server IP) in accordance with the RADIUS protocol. Possible values: ENABLED, DISABLED

radNASid

If configured, this string is sent to the RADIUS server as the "nasid" (Network Access Server ID) in accordance with the RADIUS protocol.

radVendorID

The Vendor ID for using RADIUS group extraction. Minimum value: 1

radAttributeType

The Attribute type for using RADIUS group extraction. Minimum value: 1

radGroupsPrefix

The groups prefix string that precedes the group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator

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

passEncoding

This option specifies how passwords should be encoded in RADIUS packets traveling from the system to the RADIUS server. Possible values: pap, chap, mschapv1, mschapv2 Default value: AAA_PAP

ipVendorID

The vendor ID of the attribute in the RADIUS response which denotes the intranet IP. The value of 0 denotes that the attribute is not vendor encoded.

ipAttributeType

The attribute type of the remote IP address attribute in a RADIUS response. Minimum value: 1

accounting

The state of the RADIUS server that will receive accounting messages. Possible values: ON, OFF

pwdVendorID

Vendor ID of the attribute in the RADIUS response which will be used to extract the user Password. Minimum value: 1

Top

unset authentication radiusAction

Synopsis

unset authentication radiusAction <name> [-serverIP] [-serverPort] [-authTimeout] [-radNASip] [-radNASid] [-radVendorID] [-radAttributeType] [-radGroupsPrefix] [-radGroupSeparator] [-passEncoding] [-ipVendorID] [-ipAttributeType] [-accounting] [-pwdVendorID] [-pwdAttributeType]

Description

Use this command to remove authentication radiusAction settings.Refer to the set authentication radiusAction command for meanings of the arguments.

Top

show authentication radiusAction

Synopsis

show authentication radiusAction [<name>]

Description

Display details of the configured RADIUS action(s).

Parameters

name

The name of the RADIUS action.

Top

authentication ldapAction

[add | rm | set | unset | show]

add authentication ldapAction

Synopsis

add authentication ldapAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-authTimeout <positive_integer>] [-ldapBase <string>] [-ldapBindDn <string>] {-ldapBindDnPassword } [-ldapLoginName <string>] [-searchFilter <string>] [-groupAttrName <string>] [-subAttributeName <string>] [-secType <secType>] [-svrType (AD | NDS)] [-ssoNameAttribute <string>] [-authentication (ENABLED | DISABLED)] [-requireUser (YES | NO)] [-passwdChange (ENABLED | DISABLED)] [-nestedGroupExtraction (ON | OFF) [-maxNestingLevel <positive_integer>] [-groupSearchSubAttribute <string>] [-groupSearchFilter <string>]] [-groupNameIdentifier <string>] [-groupSearchAttribute <string>]

Description

Add a profile for an LDAP server. This profile contains all the configuration data needed to communicate with the LDAP server..

Parameters

name

The name for the new LDAP action.

serverIP

The IP address of the LDAP server.

serverPort

The port number on which the LDAP server is running. Default value: 389 Minimum value: 1

authTimeout

The maximum number of seconds the system will wait for a response from the LDAP server. Default value: 3 Minimum value: 1

ldapBase

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

ldapBindDn

The full distinguished name that is used to bind to the LDAP server. The default value of the bindDN is cn=Manager,dc=netscaler,dc=com.

ldapBindDnPassword

The password that is used to bind to the LDAP server.

ldapLoginName

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

searchFilter

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

groupAttrName

The Attribute name for group extraction from the LDAP server.

subAttributeName

The Sub-Attribute name for group extraction from the LDAP server.

secType

This option indicates whether communication between the system and the authentication server should be encrypted. The following values are allowed: PLAINTEXT: No encryption required. TLS: Communicate using TLS protocol. SSL: Communicate using SSL Protocol. Possible values: PLAINTEXT, TLS, SSL Default value: AAA_LDAP_PLAINTEXT

svrType

The type of LDAP server. Possible values: AD, NDS Default value: AAA_LDAP_SERVER_TYPE_DEFAULT

ssoNameAttribute

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

authentication

Disable authentication. If disabled this LDAP action will return authentication success if the user is found. This should only be used for authorization group extraction and in conjuction with other authentication methods. The other authentication methods should be bound to a primary list or flagged as secondary. Possible values: ENABLED, DISABLED Default value: ENABLED

requireUser

Setting this option to NO allows failed user searches to be considered authentication successes. If you set require user to NO, you may only configure it with authentication DISABLED Possible values: YES, NO Default value: YES

passwdChange

Enabling this option does not block password change request.Disabling would block password change request. Possible values: ENABLED, DISABLED Default value: DISABLED

nestedGroupExtraction

Setting this option to ON enables the nested group extraction feature where the system queries the external LDAP server to determine if a group belongs to another group Possible values: ON, OFF Default value: OFF

maxNestingLevel

If NESTED GROUP EXTRACTION is set to ON, this option specifies the level upto which ancestors of a group/subgroup will be determined Default value: 2 Minimum value: 2

groupNameIdentifier

The group-attribute used by the system to uniquely identify a group in LDAP/AD

groupSearchAttribute

This option specifies the attribute that will be used to determine group-membership of a 'group'

groupSearchSubAttribute

This option specifies the sub-attribute that will be used to determine group-membership of a 'group'

groupSearchFilter

The string to be combined with the default LDAP group search string to form the value. For example, vpnallowed=true with groupIdentifier "samaccount" and the groupname "g1" would yield the LDAP search string "(&(vpnallowed=true)(samaccount=g1)".

Top

rm authentication ldapAction

Synopsis

rm authentication ldapAction <name>

Description

Remove an LDAP action. Note that an action cannot be removed as long as it is configured in a policy.

Parameters

name

The name of the LDAP action to be removed.

Top

set authentication ldapAction

Synopsis

set authentication ldapAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-authTimeout <positive_integer>] [-ldapBase <string>] [-ldapBindDn <string>] {-ldapBindDnPassword } [-ldapLoginName <string>] [-searchFilter <string>] [-groupAttrName <string>] [-subAttributeName <string>] [-secType <secType>] [-svrType (AD | NDS)] [-ssoNameAttribute <string>] [-authentication (ENABLED | DISABLED)] [-requireUser (YES | NO)] [-passwdChange (ENABLED | DISABLED)] [-nestedGroupExtraction (ON | OFF)] [-maxNestingLevel <positive_integer>] [-groupNameIdentifier <string>] [-groupSearchAttribute <string> [-groupSearchSubAttribute <string>]] [-groupSearchFilter <string>]

Description

Changes the profile of an LDAP server. The profile contains all of the configuration data needed to communicate with the LDAP server.

Parameters

name

The name for the new LDAP action.

serverIP

The IP address of the LDAP server.

serverPort

The port number on which the LDAP server is running. Default value: 389 Minimum value: 1

authTimeout

The maximum number of seconds for the system will wait for a response from the LDAP server. Default value: 3 Minimum value: 1

ldapBase

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

ldapBindDn

The full distinguished name that is used to bind to the LDAP server. The default value of the bindDN is cn=Manager,dc=netscaler,dc=com.

ldapBindDnPassword

The password that is used to bind to the LDAP server.

ldapLoginName

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

searchFilter

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

groupAttrName

The Attribute name for group extraction from the LDAP server.

subAttributeName

The Sub-Attribute name for group extraction from the LDAP server.

secType

This option indicates whether communication between the system and the authentication server should be encrypted. The following values are allowed: PLAINTEXT: No encryption required. TLS: Communicate using TLS protocol. SSL: Communicate using SSL protocol. Possible values: PLAINTEXT, TLS, SSL Default value: AAA_LDAP_PLAINTEXT

svrType

LDAP server type. Possible values: AD, NDS Default value: AAA_LDAP_SERVER_TYPE_DEFAULT

ssoNameAttribute

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

authentication

Disable authentication. If disabled this LDAP action will return authentication success if the user is found. This should only be used for authorization group extraction and in conjuction with other authentication methods. The other authentication methods should be bound to a primary list or flagged as secondary. Possible values: ENABLED, DISABLED Default value: ENABLED

requireUser

This option allows failed searches to be considered authentication successes. If you set require user to NO, you may only configure it with authentication DISABLED Possible values: YES, NO Default value: YES

passwdChange

Enabling this option does not block password change request.Disabling would block password change request. Possible values: ENABLED, DISABLED Default value: DISABLED

nestedGroupExtraction

Setting this option to ON enables the nested group extraction feature where the system queries the external LDAP server to determine if a group belongs to another group Possible values: ON, OFF Default value: OFF

Top

unset authentication ldapAction

Synopsis

unset authentication ldapAction <name> [-serverIP] [-serverPort] [-authTimeout] [-ldapBase] [-ldapBindDn] [-ldapBindDnPassword] [-ldapLoginName] [-searchFilter] [-groupAttrName] [-subAttributeName] [-secType] [-svrType] [-ssoNameAttribute] [-authentication] [-requireUser] [-passwdChange] [-nestedGroupExtraction] [-maxNestingLevel] [-groupNameIdentifier] [-groupSearchAttribute] [-groupSearchSubAttribute] [-groupSearchFilter]

Description

Use this command to remove authentication ldapAction settings.Refer to the set authentication ldapAction command for meanings of the arguments.

Top

show authentication ldapAction

Synopsis

show authentication ldapAction [<name>]

Description

Display details of the configured LDAP action(s).

Parameters

name

The name of the LDAP action.

Top

authentication tacacsAction

[add | rm | set | unset | show]

add authentication tacacsAction

Synopsis

add authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-authTimeout <positive_integer>] {-tacacsSecret } [-authorization (ON | OFF)] [-accounting (ON | OFF)] [-auditFailedCmds (ON | OFF)]

Description

Add a profile for a TACACS+ server. The profile contains all of the configuration data needed to communicate with the TACACS+ server.

Parameters

name

The name for the new TACACS+ action.

serverIP

The IP address of the TACACS+ server.

serverPort

The port on which the TACACS+ server is running. Default value: 49 Minimum value: 1

authTimeout

The maximum number of seconds the system will wait for a response from the TACACS+ server. Default value: 3 Minimum value: 1

tacacsSecret

The key shared between the client and the server. This information is required for the system to communicate with the TACACS+ server.

authorization

The state of the TACACS+ server that will be used for streaming authorization. Possible values: ON, OFF

accounting

The state of the TACACS+ server that will receive accounting messages. Possible values: ON, OFF

auditFailedCmds

The state of the TACACS+ server that will receive accounting messages. Possible values: ON, OFF

Top

rm authentication tacacsAction

Synopsis

rm authentication tacacsAction <name>

Description

Remove a TACACS+ action. Note that an action cannot be removed if it is configured in a policy.

Parameters

name

The name of TACACS+ action to be removed.

Top

set authentication tacacsAction

Synopsis

set authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-authTimeout <positive_integer>] {-tacacsSecret } [-authorization (ON | OFF)] [-accounting (ON | OFF)] [-auditFailedCmds (ON | OFF)]

Description

Changes the profile for a TACACS+ server. The profile contains all the configuration data needed to communicate with the TACACS+ server.

Parameters

name

The name for the new TACACS+ action.

serverIP

The IP address of the TACACS+ server.

serverPort

The port on which the TACACS+ server is running. Default value: 49 Minimum value: 1

authTimeout

The maximum number of seconds the system will wait for a response from the TACACS+ server. Default value: 3 Minimum value: 1

tacacsSecret

The key shared between the client and the server. This information is required for the system to communicate with the TACACS+ server.

authorization

The state of the TACACS+ server to be used for streaming authorization. Possible values: ON, OFF

accounting

The state of the TACACS+ server that will receive accounting messages. Possible values: ON, OFF

auditFailedCmds

The state of the TACACS+ server that will receive accounting messages. Possible values: ON, OFF

Top

unset authentication tacacsAction

Synopsis

unset authentication tacacsAction <name> [-serverIP] [-serverPort] [-authTimeout] [-tacacsSecret] [-authorization] [-accounting] [-auditFailedCmds]

Description

Use this command to remove authentication tacacsAction settings.Refer to the set authentication tacacsAction command for meanings of the arguments.

Top

show authentication tacacsAction

Synopsis

show authentication tacacsAction [<name>]

Description

Display details of the configured TACACS+ action(s).

Parameters

name

The name of the TACACS+ action.

Top

authentication negotiateAction

[add | rm | set | unset | show]

add authentication negotiateAction

Synopsis

add authentication negotiateAction <name> {-domain <string>} {-domainUser <string>} {-domainUserPasswd } {-OU <string>}

Parameters

name

The name for the new Negotiate action.

OU

organizational unit

Top

rm authentication negotiateAction

Synopsis

rm authentication negotiateAction <name>

Description

Remove a Negotiate action. Note that an action cannot be removed if it is configured in a policy.

Parameters

name

The name of Negotiate action to be removed.

Top

set authentication negotiateAction

Synopsis

set authentication negotiateAction <name> [-domain <string>] [-domainUser <string>] [-domainUserPasswd] [-OU <string>]

Description

Changes the profile for a AD server. The profile contains all the configuration data needed to communicate with the AD server.

Parameters

name

The name for the Negotiate action.

OU

organizational unit

Top

unset authentication negotiateAction

Synopsis

unset authentication negotiateAction <name> [-domain] [-domainUser] [-domainUserPasswd] [-OU]

Description

Use this command to remove authentication negotiateAction settings.Refer to the set authentication negotiateAction command for meanings of the arguments.

Top

show authentication negotiateAction

Synopsis

show authentication negotiateAction [<name>]

Description

Display details of the configured Negotiate action(s).

Parameters

name

The name of the Negotiate action.

Top

authentication samlAction

[add | rm | set | unset | show]

add authentication samlAction

Synopsis

add authentication samlAction <name> {-samlIdPCertName <string>} {-samlSigningCertName <string>} {-samlRedirectUrl <string>} {-samlUserField <string>} {-samlRejectUnsignedAssertion (ON | OFF)} {-samlIssuerName <string>}

Parameters

name

The name for the new SAML action.

samlIdPCertName

The name of the certificate to be used to decrypt messages from IdP.

samlSigningCertName

The name of the certificate to be used to sign messages to IdP.

samlRedirectUrl

The URL at the IdP to which user must be redirected for authentication.

samlUserField

The field/tag from where username/id is to be extracted.

samlRejectUnsignedAssertion

The option to reject Assertions which come without Signature. Possible values: ON, OFF
Default value: ON

samlIssuerName

The name to be used in requests sent from Netscaler to IdP to uniquely identify Netscaler.

Top

rm authentication samlAction

Synopsis

rm authentication samlAction <name>

Description

removes saml action.

Parameters

name

The name of SAML action to be removed.

Top

set authentication samlAction

Synopsis

set authentication samlAction <name> [-samlIdPCertName <string>] [-samlSigningCertName <string>] [-samlRedirectUrl <string>] [-samlUserField <string>] [-samlRejectUnsignedAssertion (ON | OFF)] [-samlIssuerName <string>]

Description

Modifies the parameters associated with saml action.

Parameters

name

The name for the SAML action.

samlIdPCertName

The name of the certificate to be used to decrypt messages from IdP.

samlSigningCertName

The name of the certificate to be used to sign messages to IdP.

samlRedirectUrl

The URL at the IdP to which user must be redirected for authentication.

samlUserField

The field/tag from where username/id is to be extracted.

samlRejectUnsignedAssertion

The option to reject Assertions which come without Signature. Possible values: ON, OFF
Default value: ON

samlIssuerName

The name to be used in requests sent from Netscaler to IdP to uniquely identify Netscaler.

Top

unset authentication samlAction

Synopsis

unset authentication samlAction <name> [-samlIdPCertName] [-samlSigningCertName] [-samlRedirectUrl] [-samlUserField] [-samlRejectUnsignedAssertion] [-samlIssuerName]

Description

Use this command to remove authentication samlAction settings.Refer to the set authentication samlAction command for meanings of the arguments.

Top

show authentication samlAction

Synopsis

show authentication samlAction [<name>]

Description

Display details of the configured saml action(s).

Parameters

name

The name of the saml action.

Top

authentication certAction

[add | rm | set | unset | show]

add authentication certAction

Synopsis

add authentication certAction <name> [-twoFactor (ON | OFF)] [-userNameField <string>] [-groupNameField <string>]

Description

Add a certificate action.

Parameters

name

The name of the CERT action.

twoFactor

The state of two factor authentication. Two factor authentication means client certificate authentication followed by password authentication. Possible values: ON, OFF Default value: OFF

userNameField

The field in the client certificate from which the username will be extracted. Should be of the format <field:subfield>. Allowed values for the field are "Subject" and "Issuer".

groupNameField

The field in the certificate from which the group will be extracted. Should be of the format <field:subfield>. Allowed values for the field are "Subject" and "Issuer".

Example

add authentication certaction -twoFactor ON -userNameField "Subject:CN" -groupNameField "Subject:OU"

Top

rm authentication certAction

Synopsis

rm authentication certAction <name>

Description

Remove a cert action. Note that an action cannot be removed if it is configured in a policy.

Parameters

name

The name of the CERT action to be removed.

Top

set authentication certAction

Synopsis

set authentication certAction <name> [-twoFactor (ON | OFF)] [-userNameField <string>] [-groupNameField <string>]

Description

Modifies the certificate action.

Parameters

name

The name of the CERT action.

twoFactor

The state of two factor authentication. Two factor authentication means client certificate authentication followed by password authentication. Possible values: ON, OFF Default value: OFF

userNameField

The field in the client certificate from which the username will be extracted. Should be of the format <field:subfield>. Allowed values for the field are "Subject" and "Issuer".

groupNameField

The field in the certificate from which the group will be extracted. Should be of the format <field:subfield>. Allowed values for the field are "Subject" and "Issuer".

Example

set authentication certaction -twoFactor ON -userNameField "Subject:CN" -groupNameField "Subject:OU"

Top

unset authentication certAction

Synopsis

unset authentication certAction <name> [-twoFactor] [-userNameField] [-groupNameField]

Description

Use this command to remove authentication certAction settings.Refer to the set authentication certAction command for meanings of the arguments.

Top

show authentication certAction

Synopsis

show authentication certAction [<name>]

Description

Display the details of configured CERT action(s).

Parameters

name

The name of the CERT action.

Top

authentication localPolicy

[add | rm | set | unset | show]

add authentication localPolicy

Synopsis

add authentication localPolicy <name> <rule>

Description

Add an authentication LOCAL policy. The policy defines the conditions under which the kernel will authenticate the user.

Parameters

name

The name of the new authentication LOCAL policy.

rule

The name of the rule or expression the policy will use.

Top

rm authentication localPolicy

Synopsis

rm authentication localPolicy <name>

Description

Remove an authentication LOCAL policy.

Parameters

name

The name of the LOCAL policy to remove.

Top

set authentication localPolicy

Synopsis

set authentication localPolicy <name> -rule <expression>

Description

Change properties of a LOCAL policy.

Parameters

name

The name of the policy.

rule

The new rule to be associated with the policy.

Top

unset authentication localPolicy

Synopsis

unset authentication localPolicy <name> -rule

Description

Use this command to remove authentication localPolicy settings.Refer to the set authentication localPolicy command for meanings of the arguments.

Top

show authentication localPolicy

Synopsis

show authentication localPolicy [<name>]

Description

Display configured LOCAL policies.

Parameters

name

The name of the policy. If a name is not provided, all the configured LOCAL policies will be displayed.

Top

authentication radiusPolicy

[add | rm | set | unset | show]

add authentication radiusPolicy

Synopsis

add authentication radiusPolicy <name> <rule> [<reqAction>]

Description

Add an authentication RADIUS policy. The policy defines the conditions under which the specified RADIUS server will be used for authentication.

Parameters

name

The name of the new authentication RADIUS policy.

rule

The name of the rule or expression the policy will use.

reqAction

The name of the RADIUS action the policy will use.

Top

rm authentication radiusPolicy

Synopsis

rm authentication radiusPolicy <name>

Description

Remove an authentication RADIUS policy.

Parameters

name

The name of the RADIUS policy to remove.

Top

set authentication radiusPolicy

Synopsis

set authentication radiusPolicy <name> [-rule <expression>] [-reqAction <string>]

Description

Change properties of a RADIUS policy.

Parameters

name

The name of the policy.

rule

The new rule to be associated with the policy.

reqAction

The new RADIUS action to be associated with the policy.

Top

unset authentication radiusPolicy

Synopsis

unset authentication radiusPolicy <name> [-rule] [-reqAction]

Description

Use this command to remove authentication radiusPolicy settings.Refer to the set authentication radiusPolicy command for meanings of the arguments.

Top

show authentication radiusPolicy

Synopsis

show authentication radiusPolicy [<name>]

Description

Display configured RADIUS policies.

Parameters

name

The name of the policy. If no name is provided, all the configured RADIUS policies will be displayed.

Top

authentication certPolicy

[add | rm | set | unset | show]

add authentication certPolicy

Synopsis

add authentication certPolicy <name> <rule> [<reqAction>]

Description

Add an authentication cert policy. This policy defines the conditions under which the specified cert action will be used for authentication.

Parameters

name

The name for the new policy.

rule

The name of the rule or expression the policy will use.

reqAction

The cert action to associate with the policy.

Top

rm authentication certPolicy

Synopsis

rm authentication certPolicy <name>

Description

Remove a CERT authentication policy.

Parameters

name

The name of the CERT policy to be removed.

Top

set authentication certPolicy

Synopsis

set authentication certPolicy <name> [-rule <expression>] [-reqAction <string>]

Description

Change the properties of a CERT policy.

Parameters

name

The name of the policy.

rule

The new rule to associate with the policy.

reqAction

The new cert action to associate to the policy.

Top

unset authentication certPolicy

Synopsis

unset authentication certPolicy <name> [-rule] [-reqAction]

Description

Use this command to remove authentication certPolicy settings.Refer to the set authentication certPolicy command for meanings of the arguments.

Top

show authentication certPolicy

Synopsis

show authentication certPolicy [<name>]

Description

Display configured CERT policies.

Parameters

name

The name of the policy. If a name is not provided, all of the configured policies are displayed.

Top

authentication ldapPolicy

[add | rm | set | unset | show]

add authentication ldapPolicy

Synopsis

add authentication ldapPolicy <name> <rule> [<reqAction>]

Description

Add an authentication LDAP policy. This policy defines the conditions under which the specified LDAP server will be used for authentication.

Parameters

name

The name for the new policy.

rule

The name of the rule or expression the policy will use.

reqAction

The LDAP action to associate with the policy.

Top

rm authentication ldapPolicy

Synopsis

rm authentication ldapPolicy <name>

Description

Remove an LDAP authentication policy.

Parameters

name

The name of the LDAP policy to be removed.

Top

set authentication ldapPolicy

Synopsis

set authentication ldapPolicy <name> [-rule <expression>] [-reqAction <string>]

Description

Change properties of an LDAP policy.

Parameters

name

The name of the policy.

rule

The new rule to associate with the policy.

reqAction

The new LDAP action to associate with the policy.

Top

unset authentication ldapPolicy

Synopsis

unset authentication ldapPolicy <name> [-rule] [-reqAction]

Description

Use this command to remove authentication ldapPolicy settings.Refer to the set authentication ldapPolicy command for meanings of the arguments.

Top

show authentication ldapPolicy

Synopsis

show authentication ldapPolicy [<name>]

Description

Display configured LDAP policies.

Parameters

name

The name of the policy. If a name is not provided, all of the configured policies are displayed.

Top

authentication tacacsPolicy

[add | rm | set | unset | show]

add authentication tacacsPolicy

Synopsis

add authentication tacacsPolicy <name> <rule> [<reqAction>]

Description

Add an authentication TACACS+ policy. This policy defines the conditions under which the specified TACACS+ server will be used for authentication.

Parameters

name

The name of the new TACACS+ policy.

rule

The name of the rule or expression the policy will use.

reqAction

The name of the TACACS+ action to be associated with the policy.

Top

rm authentication tacacsPolicy

Synopsis

rm authentication tacacsPolicy <name>

Description

Remove a TACACS+ policy.

Parameters

name

The name of the TACACS+ policy to be removed.

Top

set authentication tacacsPolicy

Synopsis

set authentication tacacsPolicy <name> [-rule <expression>] [-reqAction <string>]

Description

Change the properties of a TACACS+ policy.

Parameters

name

The name of the policy.

rule

The new rule to associate with the policy.

reqAction

The new TACACS+ action to associate to the policy.

Top

unset authentication tacacsPolicy

Synopsis

unset authentication tacacsPolicy <name> [-rule] [-reqAction]

Description

Use this command to remove authentication tacacsPolicy settings.Refer to the set authentication tacacsPolicy command for meanings of the arguments.

Top

show authentication tacacsPolicy

Synopsis

show authentication tacacsPolicy [<name>]

Description

Display the configured TACACS+ policies.

Parameters

name

The name of the TACACS+ policy. If no name is given, all of the configured TACACS+ policies are displayed.

Top

authentication negotiatePolicy

[add | rm | set | unset | show]

add authentication negotiatePolicy

Synopsis

add authentication negotiatePolicy <name> <rule> <reqAction>

Description

Add a negotiate authentication policy. The policy defines the conditions under which the specified AD server will be used for authentication.

Parameters

name

The name for the new Negotiate policy.

rule

The name of the rule or expression the policy will use.

reqAction

The Negotiate action the policy will use.

Top

rm authentication negotiatePolicy

Synopsis

rm authentication negotiatePolicy <name>

Description

Remove a Negotiate policy.

Parameters

name

The name of the Negotiate policy to remove.

Top

set authentication negotiatePolicy

Synopsis

set authentication negotiatePolicy <name> [-rule <expression>] [-reqAction <string>]

Description

Change the properties of a Negotiate policy.

Parameters

name

The name of the Negotiate policy.

rule

The name of the new rule to be associated with the policy.

reqAction

The name of the Negotiate action to be associated with the policy.

Top

unset authentication negotiatePolicy

Synopsis

unset authentication negotiatePolicy <name> [-rule] [-reqAction]

Description

Use this command to remove authentication negotiatePolicy settings.Refer to the set authentication negotiatePolicy command for meanings of the arguments.

Top

show authentication negotiatePolicy

Synopsis

show authentication negotiatePolicy [<name>]

Description

Display Negotiate policies.

Parameters

name

The name of the Negotiate policy. If no name is given, all the configured Negotiate policies will be displayed.

Top

authentication samlPolicy

[add | rm | set | unset | show]

add authentication samlPolicy

Synopsis

add authentication samlPolicy <name> <rule> <reqAction>

Description

Add a saml authentication policy. The policy defines the conditions under which saml authentication is used.

Parameters

name

The name for the new SAML policy.

rule

The name of the rule or expression the policy will use.

reqAction

The SAML action the policy will use.

Top

rm authentication samlPolicy

Synopsis

rm authentication samlPolicy <name>

Description

Remove a SAML policy.

Parameters

name

The name of the SAML policy to remove.

Top

set authentication samlPolicy

Synopsis

set authentication samlPolicy <name> [-rule <expression>] [-reqAction <string>]

Description

Change the properties of a SAML policy.

Parameters

name

The name of the SAML policy.

rule

The name of the new rule to be associated with the policy.

reqAction

The name of the SAML action to be associated with the policy.

Top

unset authentication samlPolicy

Synopsis

unset authentication samlPolicy <name> [-rule] [-reqAction]

Description

Use this command to remove authentication samlPolicy settings.Refer to the set authentication samlPolicy command for meanings of the arguments.

Top

show authentication samlPolicy

Synopsis

show authentication samlPolicy [<name>]

Description

Display SAML policies.

Parameters

name

The name of the SAML policy. If no name is given, all the configured SAML policies will be displayed.

Top

authentication vserver

[add | rm | set | unset | bind | unbind | enable | disable | show | stat | rename]

add authentication vserver

Synopsis

add authentication vserver <name> <serviceType> (<IPAddress> [-range <positive_integer>]) <port> [-state (ENABLED | DISABLED)] [-authentication (ON | OFF)] [-AuthenticationDomain <string>] [-comment <string>] [-appflowLog (ENABLED | DISABLED)]

Description

Add an authentication virtual server.

Parameters

name

The name for the new authentication vserver.

serviceType

The authentication vserver's protocol type, e.g. SSL Possible values: SSL Default value: NSSVC_SSL

IPAddress

The IP address for the authentication vserver.

port

The TCP port on which the vserver listens. Minimum value: 1

state

The intital vserver server state, e.g. ENABLED or DISABLED Possible values: ENABLED, DISABLED Default value: ENABLED

authentication

Indicates whether or not authentication is being applied to incoming users to the vserver. Possible values: ON, OFF Default value: ON

AuthenticationDomain

Domain of authentication vserver FQDN

comment

Comments associated with this vserver.

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

Example

The following example creates an authentication vserver named myauthenticationvip which supports SSL por
vserver myauthenticationvip SSL 65.219.17.34 443 -aaa ON

Top

rm authentication vserver

Synopsis

rm authentication vserver <name>@ ...

Description

Remove a virtual server.

Parameters

name

The name of the virtual server to be removed.

Example

rm vserver authn_vip

Top

set authentication vserver

Synopsis

set authentication vserver <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-authentication (ON | OFF)] [-AuthenticationDomain <string>] [-comment <string>] [-appflowLog (ENABLED | DISABLED)]

Description

Change the parameters of a authentication virtual server.

Parameters

name

The name of the vserver to be modified.

IPAddress

The new IP address of the virtual server.

authentication

Indicates whether authentication is ON/OFF on this vserver. Possible values: ON, OFF Default value: ON

AuthenticationDomain

Domain of authentication vserver FQDN

comment

Comments associated with this vserver.

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

Top

unset authentication vserver

Synopsis

unset authentication vserver <name> [-AuthenticationDomain] [-authentication] [-comment] [-appflowLog]

Description

Unset the parameters of an authentication virtual server..Refer to the set authentication vserver command for meanings of the arguments.

Top

bind authentication vserver

Synopsis

bind authentication vserver <name> [-policy <string> [-priority <positive_integer>] [-secondary]]

Description

Bind policies to a authentication vserver.

Parameters

name

The vserver to which this command shall bind parameters.

policy

The name of the policy to be bound to the vserver.

Top

unbind authentication vserver

Synopsis

unbind authentication vserver <name> [-policy <string> [-secondary]]

Description

Unbind policies from a authentication vserver.

Parameters

name

The name of the vserver from which an attribute is to be unbound.

policy

The name of the policy to be unbound.

Top

enable authentication vserver

Synopsis

enable authentication vserver <name>@

Description

Enable a virtual authentication server. Note: Virtual servers, when added, are enabled by default.

Parameters

name

The name of the virtual server to be enabled.

Example

enable vserver authentication1

Top

disable authentication vserver

Synopsis

disable authentication vserver <name>@

Description

Disable (take out of service) a virtual server.

Parameters

name

The name of the virtual server to be disabled. Notes: 1. The system still responds to ARP and/or ping requests for the IP address of this virtual server. 2. As the virtual server is still configured in the system, you can enable the virtual server using ###enable vserver### command.

Example

disable vserver authn_vip

Top

show authentication vserver

Synopsis

show authentication vserver [<name>] show authentication vserver stats - alias for 'stat authentication vserver'

Description

Display all of the configured Authentication virtual servers.

Parameters

name

The name of the authentication vserver.

Example

show authentication vserver

Top

stat authentication vserver

Synopsis

stat authentication vserver [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display authentication vserver statistics.

Parameters

name

The name of the vserver for which statistics will be displayed. If not given statistics are shown for all authentication vservers.

Top

rename authentication vserver

Synopsis

rename authentication vserver <name>@ <newName>@

Description

Rename an authnetication virtual server.

Parameters

name

The name of the authentication virtual server.

newName

The new name of the authentication virtual server.

Example

rename authentication vserver av1 av_new

Top

Authorization Commands

This group of commands can be used to perform operations on the following entities:

- authorization policy
- authorization policylabel

authorization policy

[add | rm | set | show]

add authorization policy

Synopsis

add authorization policy <name> <rule> <action>

Description

Add an authorization policy. Authorization policies allow AAA users and AAA groups to access resources through the SSL VPN/AAA enabled vservers. By default, the SSLVPN is configured to deny access to all resources. You can alter this default action by configuring authorization policies. (You can modify the default for a SSLVPN session with a vpn session policy. See "add vpn sessionpolicy"). You can selectively alter access to some resources to DENY by binding one or more authorization policies to the AAA user or AAA group. Once bound, an authorization policy acts on all incoming AAA user resource requests. If an authorization policy rule evaluates to TRUE, the specified action (ALLOW/DENY) is applied. If the rule evaluates to FALSE, the action is not applied. You can also bind multiple authorization policies to AAA users/groups and give them different priorities. (See "bind aaa user/group".) Policies with different priorities are sorted in descending order. The following principles are applied when policies are evaluated: 1. DENY has the highest priority and takes effect immediately. 2. ALLOW has the next-highest priority. It waits for any other DENY policy in an authorization policy that has the same priority. 3. Implicit DENY has the third-highest priority. It waits for an explicit ALLOW/DENY of *any* priority. 4. Implicit ALLOW has the lowest priority. It waits for an explicit ALLOW/DENY with any priority and an Implict DENY with the same priority.

Parameters

name

The name for the new authorization policy.

rule

The rule or expression for conditional evaluation of the policy. This rule can be an expression specified by "add policy expression." or it may be an inline expression.

action

The action to be taken when the expression is satisfied. The allowed actions are ALLOW or DENY.

Example

Example: Consider the following authorization policy, "author-policy",

```
add authorization policy author-policy "URL == /*.gif" DENY
bind aaa user foo -policy author-policy
```

If the user "foo" now logs in through the SSL VPN and makes any other request except "gif", the rule will be e

Top

rm authorization policy

Synopsis

rm authorization policy <name>

Description

Remove a configured authorization policy.

Parameters

name

The name of the authorization policy to be removed.

Top

set authorization policy

Synopsis

set authorization policy <name> [-rule <expression>] [-action <string>]

Description

Modify the rule or action value of a configured authorization policy.

Parameters

name

The name of the authorization policy to be modified.

rule

The new rule to be associated with the authorization policy.

action

The new action to be associated with the authorization policy.

Top

show authorization policy

Synopsis

show authorization policy [<name>]

Description

Display all configured authorization policies.

Parameters

name

The name of the authorization policy.

Top

authorization policylabel

[add | rm | bind | unbind | show | stat]

add authorization policylabel

Synopsis

add authorization policylabel <labelName>

Description

Add a authorization policy label.

Parameters

labelName

Name of the authorization policy label.

Example

add authorization policylabel trans_http_url

Top

rm authorization policylabel

Synopsis

rm authorization policylabel <labelName>

Description

Remove a authorization policy label.

Parameters

labelName

Name of the authorization policy label.

Example

rm authorization policylabel trans_http_url

Top

bind authorization policylabel

Synopsis

bind authorization policylabel <labelName> <policyName> <priority> [<gotoPriorityExpression>] [-invoke (<labelType> <labelName>)]

Description

Bind the authorization policy to one of the labels.

Parameters

labelName

Name of the authorization policy label.

policyName

The authorization policy name.

Example

i) bind authorization policylabel trans_http_url pol_1 1 2 -invoke reqvserver CURRENT
ii) bind authorization policylabel trans_http_url pol_2 2

Top

unbind authorization policylabel

Synopsis

unbind authorization policylabel <labelName> <policyName> [-priority <positive_integer>]

Description

Unbind entities from authorization label.

Parameters

labelName

Name of the authorization policy label.

policyName

The authorization policy name.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind authorization policylabel trans_http_url pol_1

Top

show authorization policylabel

Synopsis

show authorization policylabel [<labelName>]

Description

Display policy label or policies bound to authorization policylabel.

Parameters

labelName

Name of the authorization policy label.

Example

i) show authorization policylabel trans_http_url
ii) show authorization policylabel

Top

stat authorization policylabel

Synopsis

stat authorization policylabel [<labelName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of authorization policylabel(s).

Parameters

labelName

The name of the authorization policy label for which statistics will be displayed. If not given statistics are shown for all authorization policylabels.

Top

Basic Commands

This group of commands can be used to perform operations on the following entities:

- location
- locationFile
- server
- service
- serviceGroup
- dbsMonitors
- locationData
- svcbindings
- servicegroupbindings
- serviceGroupMember
- configstatus
- locationParameter
- vserver
- uiinternal
- reporting
- nstrace

location

[add | rm | show]

add location

Synopsis

add location <IPfrom> <IPto> <preferredLocation> [-longitude <integer> [-latitude <integer>]]

Description

Add Custom Location entries in the system.

Parameters

IPfrom

The start of the IP address range in dotted notation.

IPto

The end of the IP address range in dotted notation.

preferredLocation

The qualifiers in dotted notation for the ipaddress range mentioned.

longitude

Numerical value, in degrees, specifying the longitude of the geographical location of the IP address-range. Note: Longitude and latitude parameters are used for selecting a service with the static proximity GSLB method. If they are not specified, selection is based on the qualifiers specified for the location. Minimum value: -180 Maximum value: 180

latitude

Numerical value, in degrees, specifying the latitude of the geographical location of the IP address-range. Note: Longitude and latitude parameters are used for selecting a service with the static proximity GSLB method. If they are not specified, selection is based on the qualifiers specified for the location. Minimum value: -90 Maximum value: 90

Example

Add location 192.168.100.1 192.168.100.100 *.us.ca.san jose

Top

rm location

Synopsis

rm location <IPfrom> <IPto>

Description

Remove a custom location entry configured in system

Parameters

IPfrom

The start of the IP address range in dotted notation.

IPto

The end of the IP address range in dotted notation.

Example

rm location 192.168.100.1 192.168.100.100

Top

show location

Synopsis

show location [<IPfrom>]

Description

Display custom location entries configured in the system.

Parameters

IPfrom

The qualifiers in dotted notation for the ipaddress. If this value is not specified, all custom entries are displayed.

Example

show location

Top

locationFile

[add | rm | show]

add locationFile

Synopsis

add locationFile <locationFile> [-format <format>]

Description

load static database from the specified file into the system.

Parameters

locationFile

The name of the location file. The file name must include the full path. If the full path is not given, the default path /var/netscaler/locdb will be assumed. In high-availability mode, the static database should be stored in the same location on both systems.

format

The format of the location file. This optional argument is used to tell the system how to understand the file. The allowable values are: format = netscaler, ip-country, ip-country-isp, ip-country-region-city, ip-country-region-city-isp, geoip-country, geoip-region, geoip-city, geoip-country-org, geoip-country-isp, geoip-city-isp-org . Possible values: netscaler, ip-country, ip-country-isp, ip-country-region-city, ip-country-region-city-isp, geoip-country, geoip-region, geoip-city, geoip-country-org, geoip-country-isp, geoip-city-isp-org Default value: NSMAP_FORMAT_NETSCALER

Example

add locationfile /var/nsmap/locationdb -format netscaler

Top

rm locationFile

Synopsis

rm locationFile

Description

Remove the location file loaded into the system.

Example

rm locationfile

Top

show locationFile

Synopsis

show locationFile

Description

Display the location file loaded in the system.

Example

show locationfile

Top

server

[add | rm | set | unset | enable | disable | show | rename]

add server

Synopsis

add server <name>@ (<IPAddress>@ | (<domain>@ [-domainResolveRetry <integer>] [-IPv6Address (YES | NO)]) | (-translationIp <ip_addr> -translationMask <netmask>)) [-state (ENABLED | DISABLED)] [-comment <string>]

Description

Add a physical server to the system.

Parameters

name

The server's name.

IPAddress

The IP address of the server.

domain

The domain name of the server for which a service needs to be added. If an IP Address has been specified, the domain name does not need to be specified.

translationIp

The IP address used for translating dns obtained ip.

domainResolveRetry

The duration in seconds for which NetScaler system waits to send the next dns query to resolve the domain name, in case the last query failed. If last query succeeds, the netscaler system waits for TTL time in the response. Default value: 5 Minimum value: 5 Maximum value: 20939

state

The initial state of the service. Possible values: ENABLED, DISABLED Default value: ENABLED

IPv6Address

Defines whether server is of type ipv6 or not for DBS services Possible values: YES, NO
Default value: NO

comment

Comments associated with this server.

Example

add server web_serv 10.102.27.150
To add multiple servers you can use the following command:
add server serv[1-3] 10.102.27.[151-153]
The above command adds three servers: serv1 with IP 10.102.27.151, serv2 with IP 10.102.27.152 and serv

Top

rm server

Synopsis

rm server <name>@ ...

Description

Remove a server entry from the system.

Parameters

name

The name of the server.

Example

rm server web_svr
To remove the servers named serv1, serv2 and serv3 at once you can use the following command:
rm server serv[1-3]

Top

set server

Synopsis

set server <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@ | -domainResolveRetry <integer> | -translationIp <ip_addr> | -translationMask <netmask> | -domainResolveNow] [-comment <string>]

Description

Set server attributes.

Parameters

name

The name of the server.

IPAddress

The new IP address of the server.

domainResolveRetry

The duration in seconds for which NetScaler system waits to send the next dns query to resolve the domain name, in case the last query failed. If last query succeeds, the netscaler system waits for TTL time in the response. Default value: 5 Minimum value: 5 Maximum value: 20939

translationIp

The IP address used for translating dns obtained ip.

translationMask

The netmask of the translation ip

domainResolveNow

Restart the probe for this domain based server, immediately

comment

Comments associated with this server.

Example

set server http_svr -IPAddress 10.102.1.112
To set multiple servers IP addresses at onece you can use the following command:
setserver serv[1-3] -IPAddress 10.102.27.[1-3]
The above command sets the IP address of serv1 to 10.102.27.1, serv2 to 10.102.27.2 and serv3 to 10.102

Top

unset server

Synopsis

unset server <name>@ -comment

Description

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

Top

enable server

Synopsis

enable server <name>@

Description

Enable all the services under the specified server. Note: A server is enabled by default when it is added to the system. When a server is disabled, all services under the server are disabled.

Parameters

name

The server name.

Example

enable server web_serv
To enable all the services configured on servers named serv1, serv2 and serv3 at once, use the following c
enable server serv[1-3]

Top

disable server

Synopsis

disable server <name>@ [<delay>] [-graceFul (YES | NO)]

Description

Disable all services (that have been configured in the system) for the specified server.

Parameters

name

The name of the server (created with the add server command) for which services will be disabled.

delay

The time in seconds after which all services in this server are brought down.

graceFul

Indicates graceful shutdown of the service. System will wait for all outstanding connections to this service to be closed before disabling the service. Possible values: YES, NO Default value: NO

Example

disable server web_svr 30

To disable all the services configured on servers named serv1, serv2 and serv3 at once, use the following c
disable server serv[1-3]

Top

show server

Synopsis

show server [<name> | -internal]

Description

View the attributes of a particular physical server.

Parameters

name

The name of the server. When a servername is specifed, all services under the server are displayed.

internal

Display internally created named servers.

Example

```
> show server web_svr1
   Name:          web_svr1     State:ENABLED
   IPAddress:   10.102.27.154

> show server web_svr1
   Name:          web_svr2     State:ENABLED
   Domain: www.abc.com     Resolve Retry: 30 Secs
   Translation IP:   10.102.27.153  Translation Mask:   255.255.255.0
```

Top

rename server

Synopsis

rename server <name>@ <newName>@

Description

Rename a server.

Parameters

name

The name of the server.

newName

The new name of the server.

Example

```
rename server s1 s1-new
```

Top

service

[add | rm | set | unset | bind | unbind | enable | disable | show | rename | stat]

add service

Synopsis

add service <name>@ (<IP>@ | <serverName>@) <serviceType> <port> [-clearTextPort <port>] [-cacheType <cacheType>] [-maxClient <positive_integer>] [-healthMonitor (YES | NO)] [-maxReq <positive_integer>] [-cacheable (YES | NO)] [-cip (ENABLED | DISABLED) [<cipHeader>]] [-usip (YES | NO)] [-pathMonitor (YES | NO)] [-pathMonitorIndv (YES | NO)] [-useproxyport (YES | NO)] [-sc (ON | OFF)] [-sp (ON | OFF)] [-rtspSessionidRemap (ON | OFF)] [-cltTimeout <secs>] [-svrTimeout <secs>] [-CustomServerID <string>] [-CKA (YES | NO)] [-TCPB (YES | NO)] [-CMP (YES | NO)] [-maxBandwidth <positive_integer>] [-accessDown (YES | NO)] [-monThreshold <positive_integer>] [-state (ENABLED | DISABLED)] [-downStateFlush (ENABLED | DISABLED)] [-tcpProfileName <string>] [-httpProfileName <string>] [-hashId <positive_integer>] [-comment <string>] [-appflowLog (ENABLED | DISABLED)] [-netProfile <string>]

Description

Add a service to the system. Each server can have multiple services. Note: Each time you add a service for the same server, you must specify a unique port number for the service.

Parameters

name

The name of the service.

IP

The IP address of the server for which a service will be added.

serverName

The name of the server for which a service will be added.

serviceType

The type of service. The supported protocols are: HTTP - To load balance web servers and provide connection multiplexing, latency improvement, and other content and TCP protection benefits for HTTP traffic. FTP - To load balance FTP servers. In FTP mode, the system provides TCP protection benefits, protection against SYN attacks, and surge protection. TCP - To host any other TCP protocols that are not HTTP, FTP, NNTP, or SSL. In TCP mode, the system provides TCP protection benefits, protection against SYN

attack, and surge protection. UDP - To load balance servers with UDP-based services (other than DNS). SSL - To provide end-to-end encryption and SSL acceleration. SSL_BRIDGE - To load balance SSL servers. SSL_TCP - To offload SSL traffic for TCP applications. NNTP - To load balance NNTP servers. DNS - To load balance DNS servers. ADNS: To create an authoritative DNS service. ANY - To load balance a service type not listed above (for example, for IP traffic when load balancing firewalls). Note: The NNTP service is for cache redirection. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, RADIUS, RDP, DIAMETER, SSL_DIAMETER

port

The port number to be used for the service.

clearTextPort

The clear text port number where clear text data is sent. Used with SSL offload service. Minimum value: 1

cacheType

The cache type option supported by the cache server. Possible values: TRANSPARENT, REVERSE, FORWARD

maxClient

The maximum number of open connections to the service. Maximum value: 4294967294

healthMonitor

Health monitoring state of the service. Possible values: YES, NO Default value: YES

maxReq

The maximum number of requests that can be sent on a persistent connection to the service. Maximum value: 65535

cacheable

The virtual server (used in load balancing or content switching) routes a request to the virtual server (used in transparent cache redirection) on the same system before sending it to the configured servers. The virtual server used for transparent cache redirection determines if the request is directed to the cache servers or configured servers. Note: This argument is disabled by default. Do not specify this argument if a -cacheType cacheType is specified. Possible values: YES, NO Default value: NO

cip

The Client IP header insertion option for the service. Possible values: ENABLED, DISABLED

cipHeader

The client IP header. If client IP insertion is enabled and the client IP header is not specified, then the value set by the ###set ns param### command will be used as the Client IP header.

usip

The use of client's IP Address option to the source IP Address while connecting to this server. By default, the system uses a mapped IP address for its server connection; however, you can use this option to tell the system to use the client's IP address when it communicates with the server. Possible values: YES, NO

pathMonitor

Path monitoring for clustering Possible values: YES, NO

pathMonitorIndv

Individual Path monitoring decisions Possible values: YES, NO

useproxyport

When USIP is enabled, based on the setting of this variable proxy port or the client port will be used as the source port for the backend connection. Possible values: YES, NO

sc

The state of SureConnect for the service. Note: This parameter is supported for legacy purposes only. It has no effect on this system, and its only valid value is OFF. Possible values: ON, OFF Default value: OFF

sp

The state of Surge protection for the the service. Possible values: ON, OFF

rtspSessionidRemap

Use this parameter to enable mapping of RTSP sessionid. Possible values: ON, OFF Default value: OFF

cltTimeout

The idle time (in seconds) after which the client connection is terminated. Maximum value: 31536000

svrTimeout

The idle time (in seconds) after which the server connection is terminated. Maximum value: 31536000

CustomServerID

The identifier for the service. This is used when the persistency type is set to Custom Server ID. Default value: "None"

serverID

The identifier for the service. This is used when the persistency type is set to Custom Server ID.

CKA

The state of the Client Keep-Alive feature for the service. Possible values: YES, NO

TCPB

The state of the TCP Buffering feature for the service. Possible values: YES, NO

CMP

The state of the HTTP Compression feature for the service. Possible values: YES, NO

maxBandwidth

The maximum bandwidth in kbps allowed for the service. Maximum value: 4294967287

accessDown

The option to allow access to disabled or down services. If enabled, all packets to this service are bridged. If disabled, they are dropped. Possible values: YES, NO Default value: NO

monThreshold

The monitoring threshold. Maximum value: 65535

state

The state of the service after it is added. Possible values: ENABLED, DISABLED Default value: ENABLED

downStateFlush

Perform delayed clean up of connections on this service. Possible values: ENABLED, DISABLED Default value: ENABLED

tcpProfileName

The name of the TCP profile.

httpProfileName

Name of the HTTP profile.

hashId

The hash identifier for the service. This must be unique for each service. This parameter is used by hash based load balancing methods. Minimum value: 1

comment

Comments associated with this server.

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

The name of the network profile.

Example

add service http_svc 10.102.1.112 http 80
The below command adds the service web_svc1 for the server web_serv1, web_svc2 for web_serv2 and we
add service web_svc[1-3] web_serv[1-3] http 80

Top

rm service

Synopsis

rm service <name>@

Description

Remove a service from the system.

Parameters

name

The name of the service.

Example

rm service http_svc
To remove services svc1, svc2 and svc3 in one go use the following command:
rm service svc[1-3]

Top

set service

Synopsis

set service <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@] [-maxClient <positive_integer>] [-maxReq <positive_integer>] [-cacheable (YES | NO)] [-cip (ENABLED | DISABLED) [<cipHeader>]] [-usip (YES | NO)] [-pathMonitor (YES | NO)] [-pathMonitorIndv (YES | NO)] [-useproxyport (YES | NO)] [-sc (ON | OFF)] [-sp (ON | OFF)] [-rtspSessionidRemap (ON | OFF)] [-healthMonitor (YES | NO)] [-cltTimeout <secs>] [-svrTimeout <secs>] [-CustomServerID <string>] [-CKA (YES | NO)] [-TCPB (YES | NO)] [-CMP (YES | NO)] [-maxBandwidth <positive_integer>] [-accessDown (YES | NO)] [-monThreshold <positive_integer>] [-weight <positive_integer> <monitorName>] [-downStateFlush (ENABLED | DISABLED)] [-tcpProfileName <string>] [-httpProfileName <string>] [-hashId <positive_integer>] [-comment <string>] [-appflowLog (ENABLED | DISABLED)] [-netProfile <string>]

Description

Use this command to modify the attributes of an existing service.

Parameters

name

The name of the service.

IPAddress

The new IP address of the service.

maxClient

The maximum number of open connections to the service. Maximum value: 4294967294

maxReq

The maximum number of requests that can be sent on a persistent connection to the service. Maximum value: 65535

cacheable

The state of cache on the service. Possible values: YES, NO Default value: NO

cip

The Client IP header insertion option for the service. Possible values: ENABLED, DISABLED

usip

The usage of Client IP Address. Possible values: YES, NO

pathMonitor

Path monitoring for clustering Possible values: YES, NO

pathMonitorIndv

Individual Path monitoring decisions Possible values: YES, NO

useproxyport

The usage of Client Port. Possible values: YES, NO

sc

The state of SureConnect for the service. Possible values: ON, OFF Default value: OFF

sp

The state of surge protection for the service. Possible values: ON, OFF

rtspSessionidRemap

Use this parameter to enable mapping of RTSP sessionid. Possible values: ON, OFF Default value: OFF

healthMonitor

Health monitoring state of the service. Possible values: YES, NO Default value: YES

cltTimeout

The idle time in seconds after which the client connection is terminated. Maximum value: 31536000

svrTimeout

The idle time in seconds after which the server connection is terminated. Maximum value: 31536000

CustomServerID

The identifier for the service. Used when the persistency type is set to Custom Server ID. Default value: "None"

serverID

The identifier for the service. This is used when the persistency type is set to Custom Server ID.

CKA

The state of the Client Keep-Alive feature for the service. Possible values: YES, NO

TCPB

The state of the TCP Buffering feature for this service. Possible values: YES, NO

CMP

The state of the HTTP Compression feature for this service. Possible values: YES, NO

maxBandwidth

The maximum bandwidth in kbps allowed for this service. Maximum value: 4294967287

accessDown

The option to allow access to disabled or down services. Possible values: YES, NO Default value: NO

monThreshold

The monitoring threshold. Maximum value: 65535

weight

The weight for the specified monitor. Minimum value: 1 Maximum value: 100

downStateFlush

Perform delayed clean up of connections on this service. Possible values: ENABLED, DISABLED Default value: ENABLED

tcpProfileName

The name of the TCP profile.

httpProfileName

Name of the HTTP profile.

hashId

The hash identifier for the service. This must be unique for each service. This parameter is used by hash based load balancing methods. Minimum value: 1

comment

Comments associated with this service.

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

The name of the network profile.

Example

set service http_svc -maxClient 100

The following command sets IP address 10.102.27.53 for service svc1, 10.102.27.54 for svc2 and 10.102.27
set service svc[1-3] -IPAddress 10.102.27.[53-55]

Top

unset service

Synopsis

unset service <name>@ [-maxClient] [-maxReq] [-cacheable] [-cip] [-usip] [-pathMonitor] [-pathMonitorIndv] [-useproxyport] [-sc] [-sp] [-rtspSessionidRemap] [-CustomServerID] [-CKA] [-TCPB] [-CMP] [-maxBandwidth] [-accessDown] [-monThreshold] [-cltTimeout] [-svrTimeout] [-tcpProfileName] [-httpProfileName] [-hashId] [-appflowLog] [-netProfile] [-cipHeader] [-healthMonitor] [-monitorName] [-downStateFlush] [-comment]

Description

Use this command to unset the attributes of an existing service..Refer to the set service command for meanings of the arguments.

Example

unset service http_svc -maxClient
To unset maxclients for services svc1, svc2 and svc3, the following command can be used:
unset service svc[1-3] -maxClient

Top

bind service

Synopsis

bind service <name>@ (-policyName <string> | (-monitorName <string>@ [-monState (ENABLED | DISABLED)] [-weight <positive_integer>]))

Description

Use this command to bind a policy to a service. Notes: 1. This command does not support SureConnect policies. 2. This command only works for services that are not bound to virtual servers. If you attempt to bind a policy to a service that is already bound to a virtual server, the error message "Binding invalid policy" is displayed.

Parameters

name

The name of the service to which the policy will be bound.

policyName

The DoS protection policy name must be bound to the service. Also, for DoS protection to work on a service, an appropriate policy must be bound to the service.

monitorName

The name of the service or a service group to which the monitor is to be bound.

Example

bind service svc1 -policyName pol1
To bind svc1, svc2 and svc3 to the policy pol1 you can use the following command:
bind service svc[1-3] -policyName pol1

Top

unbind service

Synopsis

unbind service <name>@ (-policyName <string> | -monitorName <string>@)

Description

Unbind a policy from a service.

Parameters

name

The name of the service.

policyName

Name of the policy to be unbound.

monitorName

The monitor Names.

Example

unbind service http_svc -policyName pol1
To unbind a policy called pol1 on services svc1, svc2 and svc3, use the following command:
unbind service svc[1-3] -policyName pol1

Top

enable service

Synopsis

enable service <name>@

Description

Enable a service.

Parameters

name

The name of the service.

Example

enable service http_svc
To enable svc1, svc2 and svc3 in one go use the following command:
enable service svc[1-3]

Top

disable service

Synopsis

disable service <name>@ [<delay>] [-graceFul (YES | NO)]

Description

Disable a service.

Parameters

name

The name of the service that needs to be disabled.

delay

The time allowed (in seconds) for a graceful shutdown. During this period, new connections and requests continue to be sent to the service for clients who already have persistent sessions on the system. Connections or requests from fresh or new clients who do not yet have a persistence sessions on the NetScaler system are not sent to the service. Instead, they are load balanced among other available services. After the delay

time has passed, no new requests or connections are sent to the service.

graceFul

Indicates graceful shutdown of the service. System will wait for all outstanding connections to this service to be closed before disabling the service. Possible values: YES, NO Default value: NO

Example

disable service http_svc 10
To disable svc1, svc2 and svc3 in one go use the following command:
disable service svc[1-3] 10

Top

show service

Synopsis

show service [<name> | -all | -internal] show service bindings - alias for 'show svcbindings'

Description

Display the services configured on the system. This command either lists all services or displays complete information about a particular service.

Parameters

name

The name of the service.

all

Display both configured and dynamically learned services. If you do not use this option, only the configured services are displayed.

internal

Display internally created named services.

Example

The following is sample output of the show service -all command:

```
4 configured services:
1)      svc1 (10.124.99.12:80) - HTTP        State: UP
     Max Conn: 0     Max Req: 0      Use Source IP: NO
     Client Keepalive(CKA): NO
    TCP Buffering(TCPB): NO
```

```
   HTTP Compression(CMP): NO
   Idle timeout: Client: 180 sec   Server: 360 sec
   Client IP: DISABLED
2) svc_3 (10.100.100.3:53) - DNS   State: UP
   Max Conn: 0     Max Req: 0      Use Source IP: NO
   Client Keepalive(CKA): NO
   TCP Buffering(TCPB): NO
   HTTP Compression(CMP): NO
   Idle timeout: Client: 180 sec   Server: 360 sec
   Client IP: DISABLED
3) tsvc1 (77.45.32.45:80) - HTTP   State: UP
   Max Conn: 0     Max Req: 0      Use Source IP: NO
   Client Keepalive(CKA): NO
   TCP Buffering(TCPB): NO
   HTTP Compression(CMP): NO
   Idle timeout: Client: 180 sec   Server: 360 sec
   Client IP: DISABLED
4) foosvc (10.124.99.13:7979) - HTTP  State: UP
   Max Conn: 0     Max Req: 0      Use Source IP: NO
   Client Keepalive(CKA): NO
   TCP Buffering(TCPB): NO
   HTTP Compression(CMP): NO
   Idle timeout: Client: 180 sec   Server: 360 sec
   Client IP: DISABLED
```

Top

rename service

Synopsis

rename service <name>@ <newName>@

Description

Rename a service.

Parameters

name

The name of the service.

newName

The new name of the service.

Example

rename service svc1 svcnew

Top

stat service

Synopsis

stat service [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of a service.

Parameters

name

Name of the service

Top

serviceGroup

[add | rm | set | unset | bind | unbind | enable | disable | show | stat | rename]

add serviceGroup

Synopsis

add serviceGroup <serviceGroupName>@ <serviceType> [-cacheType <cacheType>] [-maxClient <positive_integer>] [-maxReq <positive_integer>] [-cacheable (YES | NO)] [-cip (ENABLED | DISABLED) [<cipHeader>]] [-usip (YES | NO)] [-pathMonitor (YES | NO)] [-pathMonitorIndv (YES | NO)] [-useproxyport (YES | NO)] [-healthMonitor (YES | NO)] [-sc (ON | OFF)] [-sp (ON | OFF)] [-rtspSessionidRemap (ON | OFF)] [-cltTimeout <secs>] [-svrTimeout <secs>] [-CKA (YES | NO)] [-TCPB (YES | NO)] [-CMP (YES | NO)] [-maxBandwidth <positive_integer>] [-monThreshold <positive_integer>] [-state (ENABLED | DISABLED)] [-downStateFlush (ENABLED | DISABLED)] [-tcpProfileName <string>] [-httpProfileName <string>] [-comment <string>] [-appflowLog (ENABLED | DISABLED)] [-netProfile <string>] [-autoScale (DISABLED | DNS)]

Description

Add a service group to the system.

Parameters

serviceGroupName

The name of the service group.

serviceType

The type of service group that is being added. Supported protocols are: HTTP - To load balance web servers and provide connection multiplexing, latency improvement, and other content and TCP protection benefits for HTTP traffic. FTP - To load balance FTP servers. In FTP mode, the NetScaler 9000 system provides TCP protection benefits, protection against SYN attacks, and surge protection. TCP - To host any other TCP protocols that are not HTTP, FTP, NNTP, or SSL. In TCP mode, the NetScaler 9000 system provides TCP protection benefits, protection against SYN attack, and surge protection UDP - To load balance servers with UDP-based service groups (other than DNS) SSL - To provide end-to-end encryption and SSL acceleration. SSL_BRIDGE - To load balance SSL servers. SSL_TCP - To offload SSL traffic for TCP applications. NNTP - To load balance NNTP servers. DNS - To load balance DNS servers. ANY - To load balance a service group type not listed above (for example, for IP traffic when load balancing firewalls). Note: The NNTP service group is for cache redirection. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, RADIUS, RDP, DIAMETER, SSL_DIAMETER

cacheType

The cache type option supported by the cache server. The options are: TRANSPARENT, REVERSE, and FORWARD. Possible values: TRANSPARENT, REVERSE, FORWARD

maxClient

The maximum number of open connections to each service in the service group. Maximum value: 4294967294

maxReq

The maximum number of requests that can be sent over a persistent connection to a service in the service group. Maximum value: 65535

cacheable

Whether a virtual server (used in the NetScaler 9000 system's load balancing or content switching feature) routes a request to the virtual server (used in transparent cache redirection) on the same NetScaler 9000 system before sending it to the configured servers. The virtual server used for transparent cache redirection determines if the request is directed to the cache servers or configured servers. Note: Do not specify this argument if a cache type is specified. This argument is disabled by default. Possible values: YES, NO Default value: NO

cip

Enables or disables insertion of the Client IP header for services in the service group. Possible values: ENABLED, DISABLED

cipHeader

The client IP header. If client IP insertion is enabled and the client IP header is not specified, then the value set by the ###set ns param### command will be used as the Client IP header.

usip

Enables or disables use of client's IP Address as the source IP Address while connecting to the server. By default, the system uses a mapped IP address for its server connection. However, with this option, you can tell the NetScaler 9000 system to use the client's IP address when it communicates with the server. Possible values: YES, NO

pathMonitor

Path monitoring for clustering Possible values: YES, NO

pathMonitorIndv

Individual Path monitoring decisions. Possible values: YES, NO

useproxyport

When USIP is enabled, based on the setting of this variable proxy port or the client port will be used as the source port for the backend connection. Possible values: YES, NO

healthMonitor

Health monitoring state of the all service group members. Possible values: YES, NO Default value: YES

sc

The state of SureConnect on this service group. Note: This parameter is supported for legacy purposes only; it has no effect, and the only valid value is OFF. Possible values: ON, OFF Default value: OFF

sp

Whether surge protection needs to be enabled on this service group. Possible values: ON, OFF Default value: OFF

rtspSessionidRemap

Use this parameter to enable mapping of RTSP sessionid. Possible values: ON, OFF Default value: OFF

cltTimeout

The idle time in seconds after which the client connection is terminated. Maximum value: 31536000

svrTimeout

The idle time in seconds after which the server connection is terminated. Maximum value: 31536000

CKA

The state of the Client Keep-Alive feature for the services in the service group. Possible values: YES, NO

TCPB

The state of the TCP Buffering feature for the services in the service group. Possible values: YES, NO

CMP

The state of the HTTP Compression feature for the services in the service group. Possible values: YES, NO

maxBandwidth

A positive integer that identifies the maximum bandwidth in kbps allowed for the services in the service group. Maximum value: 4294967287

monThreshold

The monitoring threshold. Maximum value: 65535

state

The state of the service group after it is added. Possible values: ENABLED, DISABLED Default value: ENABLED

downStateFlush

Perform delayed clean up of connections on this service group. Possible values: ENABLED, DISABLED Default value: ENABLED

tcpProfileName

The name of the TCP profile.

httpProfileName

Name of the HTTP profile.

comment

Comments associated with this servicegroup.

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

The name of the network profile.

autoScale

Auto scale option for a domain based server when bound to a servicegroup Possible values: DISABLED, DNS Default value: DISABLED

Example

add servicegroup http_svc_group http
To add service groups sgrp1, sgrp2 and sgrp3 at one go use the following command: add servicegroup sgrp[1-3] http

Top

rm serviceGroup

Synopsis

rm serviceGroup <serviceGroupName>@

Description

Remove a service group.

Parameters

serviceGroupName

The name of the service group that will be removed.

Example

rm servicegroup http_svc_group
To remove multiple servicegroups at once, the following command can be used:
rm servicegroup http_svc_group[1-3]

Top

set serviceGroup

Synopsis

set serviceGroup <serviceGroupName>@ [(<serverName>@ <port> [-weight <positive_integer>] [-CustomServerID <string>] [-hashId <positive_integer>]) | -maxClient <positive_integer> | -maxReq <positive_integer> | -cacheable (YES | NO) | -cip (ENABLED | DISABLED) | <cipHeader> | -usip (YES | NO) | -useproxyport (YES | NO) | -sc (ON | OFF) | -sp (ON | OFF) | -rtspSessionidRemap (ON | OFF) | -cltTimeout <secs> | -svrTimeout <secs> | -CKA (YES | NO) | -TCPB (YES | NO) | -CMP (YES | NO) | -maxBandwidth <positive_integer> | -monThreshold <positive_integer> | -downStateFlush (ENABLED | DISABLED)] [-monitorName <string> -weight <positive_integer>] [-healthMonitor (YES | NO)] [-pathMonitor (YES | NO)] [-pathMonitorIndv (YES | NO)] [-tcpProfileName <string>] [-httpProfileName <string>] [-comment <string>] [-appflowLog (ENABLED | DISABLED)] [-netProfile <string>]

Description

Modify the attributes of an existing service group.

Parameters

serviceGroupName

The name of the service group whose attributes will be changed.

serverName

The name of the server to be changed.

monitorName

Name of monitor bound to servicegroup, it is used in setting weight bound to monitor.

maxClient

The maximum number of open connections to each service in the service group. Maximum value: 4294967294

maxReq

The maximum number of requests that can be sent on a persistent connection to a service. Maximum value: 65535

healthMonitor

Health monitoring state of the all service group members. Possible values: YES, NO Default value: YES

cacheable

The state of cache on the service group. Possible values: YES, NO Default value: NO

cip

The state of insertion of the Client IP header for a service. Possible values: ENABLED, DISABLED

usip

The usage of client's IP Address Possible values: YES, NO

pathMonitor

Path monitoring for clustering Possible values: YES, NO

pathMonitorIndv

Individual Path monitoring decisions. Possible values: YES, NO

useproxyport

When USIP is enabled, based on the setting of this variable proxy port or the client port will be used as the source port for the backend connection. Possible values: YES, NO

sc

Whether SureConnect will be enabled on this service. Possible values: ON, OFF Default value: OFF

sp

The state of surge protection on this service group. Possible values: ON, OFF Default value: OFF

rtspSessionidRemap

Use this parameter to enable mapping of RTSP sessionid. Possible values: ON, OFF Default value: OFF

cltTimeout

The idle time (in seconds) after which the client connection is terminated. Maximum value: 31536000

svrTimeout

The idle time in seconds after which the server connection is terminated. Maximum value: 31536000

CKA

The state of the Client Keep-Alive feature for the service. Possible values: YES, NO

TCPB

The state of the TCP Buffering feature for this service. Possible values: YES, NO

CMP

The state of the HTTP Compression feature for this service. Possible values: YES, NO

maxBandwidth

A positive integer that identifies the maximum bandwidth in kbps allowed for this service. Maximum value: 4294967287

monThreshold

The monitoring threshold. Maximum value: 65535

downStateFlush

Perform delayed cleanup of connections on this service group. Possible values: ENABLED, DISABLED Default value: ENABLED

tcpProfileName

The name of the TCP profile.

httpProfileName

Name of the HTTP profile.

comment

Comments associated with this servicegroup.

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

The name of the network profile.

Example

set servicegroup http_svc_group -maxClient 100
To set the attribute maxclient for multiple servicegroups at once, use the following command:
set servicegroup http_svc_group[1-3] -maxClient 100

Top

unset serviceGroup

Synopsis

unset serviceGroup <serviceGroupName>@ [<serverName>@ <port> [-weight] [-CustomServerID] [-hashId]] [-maxClient] [-maxReq] [-cacheable] [-cip] [-usip] [-useproxyport] [-sc] [-sp] [-rtspSessionidRemap] [-cltTimeout] [-svrTimeout] [-CKA] [-TCPB] [-CMP] [-maxBandwidth] [-monThreshold] [-tcpProfileName] [-httpProfileName] [-appflowLog] [-netProfile] [-monitorName] [-weight] [-healthMonitor] [-cipHeader] [-pathMonitor] [-pathMonitorIndv] [-downStateFlush] [-comment]

Description

Use this command to unset the attributes of an existing service group..Refer to the set serviceGroup command for meanings of the arguments.

Example

unset servicegroup http_svc_group -maxClient

Top

bind serviceGroup

Synopsis

bind serviceGroup <serviceGroupName> ((<IP>@ <port>) | <serverName>@ | ((-monitorName <string>@ [-monState (ENABLED | DISABLED)]) | -CustomServerID <string> | -state (ENABLED | DISABLED) | -hashId <positive_integer> |)) [-weight <positive_integer>]

Description

Bind a service to a service group.

Parameters

serviceGroupName

The name of the service group to which the service will be bound.

IP

The IP address of a member to be added.

serverName

The name of the server that hosts the member.

port

The port number of a service to be added.

monitorName

The name of the service or a service group to which the monitor is to be bound.

weight

Weight for this service. This weight is used when the system performs load balancing. It is useful to specify weights when services bound to the service group have different capacities. Default value: 1 Minimum value: 1 Maximum value: 100

CustomServerID

A positive integer that will identify the service. Used when the persistency type is set to Custom Server ID. Default value: "None"

serverID

The identifier for the service. This is used when the persistency type is set to Custom Server ID.

state

The state of the IP/Port after binding. Possible values: ENABLED, DISABLED Default value: ENABLED

hashId

The hash identifier for the service. This must be unique for each service. This parameter is used by hash based load balancing methods. Minimum value: 1

Example

bind servicegroup http_svc_group 10.102.27.153 80
To bind multiple servers to a servicegroup, following command can be used:
bind servicegroup http_svc_group 10.102.27.[153-155] 80

Top

unbind serviceGroup

Synopsis

unbind serviceGroup <serviceGroupName> ((<IP>@ <port>) | <serverName>@ | -monitorName <string>@)

Description

Unbind a service from a service group.

Parameters

serviceGroupName

The name of the service group.

IP

The IP address of a member to be removed.

serverName

The name of the server that hosts the member to be unbound from the service group.

port

The port number of a service to be unbound from the service group.

monitorName

Monitor name.

Example

unbind servicegroup http_svc_group 10.102.27.153 80
To unbind multiple servers following command can be used:
unbind servicegroup http_svc_group 10.102.27.[153-155] 80

Top

enable serviceGroup

Synopsis

enable serviceGroup <serviceGroupName>@ [<serverName>@ <port>]

Description

Use this command to enable a service group.

Parameters

serviceGroupName

The name of the service group to be enabled.

serverName

The name of the server that hosts the member to be enabled from the service group.

port

The port number of the service to be enabled.

Example

enable servicegroup http_svc_group
To enable multiple service groups at one go use the following command:
enable servicegroup http_svc_group[1-3]

Top

disable serviceGroup

Synopsis

disable serviceGroup <serviceGroupName>@ [<serverName>@ <port>] [-delay <secs>] [-graceFul (YES | NO)]

Description

Use this command to disable a service group.

Parameters

serviceGroupName

The name of the service group that needs to be disabled.

serverName

The name of the server that hosts the member to be disabled from the service group.

port

The port number of the service to be disabled.

delay

The time allowed (in seconds) for a graceful shutdown. During this period, new connections or requests will continue to be sent to this service for clients who already have a persistent session on the system. Connections or requests from fresh or new clients who do not yet have a persistence sessions on the system will not be sent to the service. Instead, they will be load balanced among other available services. After the delay time expires, no new requests or connections will be sent to the service.

graceFul

Indicates graceful shutdown of the service. System will wait for all outstanding connections to this service to be closed before disabling the service. Possible values: YES, NO Default value: NO

Example

disable servicegroup http_svc_group 10.102.27.153 80 -delay 10
To disable multiple servicegroups use the following command:
disable servicegroup http_svc_group[1-3] 10.102.27.[153-155] 80 -delay 30

Top

show serviceGroup

Synopsis

show serviceGroup [<serviceGroupName> | -includeMembers]

Description

Display the configured service groups. This command either lists all service groups or displays complete information about a particular service group.

Parameters

serviceGroupName

The name of the service group.

includeMembers

Include a summary of the members in a group too.

Top

stat serviceGroup

Synopsis

stat serviceGroup [<serviceGroupName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of service group(s).

Parameters

serviceGroupName

The name of a service group

Top

rename serviceGroup

Synopsis

rename serviceGroup <serviceGroupName>@ <newName>@

Description

Rename a service group.

Parameters

serviceGroupName

The name of the service group.

newName

The new name of the service group.

Example

rename service svcgrp1 svcgrp-new1

Top

dbsMonitors

restart dbsMonitors

Synopsis

restart dbsMonitors

Description

Use this command to clear/flush all learnt ip addresses for domain based servers

Example

restart dbsMonitors

locationData

clear locationData

Synopsis

clear locationData

Description

Clear all location information, including custom entries and static database entries.

Example

clear locationdata

svcbindings

show svcbindings

Synopsis

show svcbindings <serviceName>

Description

Displays service information followed by vservers bound to it.

Parameters

serviceName

The name of the service.

servicegroupbindings

show servicegroupbindings

Synopsis

show servicegroupbindings <serviceGroupName>

Description

Displays servicegroup information followed by vservers bound to it.

Parameters

serviceGroupName

The name of the service.

serviceGroupMember

stat serviceGroupMember

Synopsis

stat serviceGroupMember <serviceGroupName> (<IP> | <serverName>) <port> [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of a service group member.

Parameters

serviceGroupName

The name of a service group

IP

The IP address of the member

serverName

The name of the Domain based server for which stats are required

port

The port number of the member

configstatus

show configstatus

Synopsis

show configstatus

Description

Display status of packet engines.

Example

show configstatus

locationParameter

[set | unset | show]

set locationParameter

Synopsis

set locationParameter [-context (geographic | custom)] [-q1label <string>] [-q2label <string>] [-q3label <string>] [-q4label <string>] [-q5label <string>] [-q6label <string>]

Description

This command specifies the location parameters used for static proximity based load balancing.

Parameters

context

The context in which a static proximity decision has to be made. Possible values: geographic, custom

q1label

The label for the 1st qualifier. These qualifier labels specify the locations mapped with the IP addresses used to make static proximity decisions.

q2label

The label for the 2nd qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

q3label

The label for the 3rd qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

q4label

The label for the 4th qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

q5label

The label for the 5th qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

q6label

The label for the 6th qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

Example

set locationparameter -context custom

Top

unset locationParameter

Synopsis

unset locationParameter [-context] [-q1label] [-q2label] [-q3label] [-q4label] [-q5label] [-q6label]

Description

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

Top

show locationParameter

Synopsis

show locationParameter

Description

Display information about the context and qualifier labels used for static proximity based load balancing.

Example

show locationparameter

Top

vserver

show vserver

Synopsis

show vserver

Description

Use this command to display all virtual servers configured on the NetScaler system. The information displayed includes the virtual server name, IP address, port number, service type, virtual server state and virtual server type.

Example

show vserver lb_vip

uiinternal

[set | unset | show]

set uiinternal

Synopsis

set uiinternal <entityType> <name> [-template <string>] [-comment <string>] [-rule <string>]

Description

set uiinternal data for the entities

Parameters

entityType

The entitiy type of UI internal data Possible values: LBVSERVER, GSLBVSERVER, CRVSERVER, VPNVSERVER, CSVSERVER, AUTHENTICATIONVSERVER, SERVER, SERVICE, SERVICEGROUP, GSLBSERVICE, EXPRESSION, VPNURL

name

The entity name

template

The application template associated with entity

comment

The application template associated with entity

rule

rules associated with entity

Example

set uiinternal lbvserver v1 -template app1

Top

unset uiinternal

Synopsis

unset uiinternal <entityType> <name> [-template] [-comment] [-rule] [-all]

Description

unset uiinternal for the entities.Refer to the set uiinternal command for meanings of the arguments.

Example

unset uiinternal lbvserver v1 -template app1

Top

show uiinternal

Synopsis

show uiinternal [<entityType>] [<name>]

Description

display all UI internal data information for the entities

Parameters

entityType

The entitiy type of UI internal data Possible values: LBVSERVER, GSLBVSERVER, CRVSERVER, VPNVSERVER, CSVSERVER, AUTHENTICATIONVSERVER, SERVER, SERVICE, SERVICEGROUP, GSLBSERVICE, EXPRESSION, VPNURL

name

The entity name

Example

show uiinternal LBVSERVER v1

Top

reporting

[enable | disable | show]

enable reporting

Synopsis

enable reporting

Description

Enable the data collection for reporting module.

Example

enable reporting

Top

disable reporting

Synopsis

disable reporting

Description

Disable the data collection for reporting module.

Example

disable reporting

Top

show reporting

Synopsis

show reporting

Description

show the state of data collection for reporting module.

Example

show reporting

Top

nstrace

[start | stop | show]

start nstrace

Synopsis

start nstrace [-nf <positive_integer>] [-time <positive_integer>] [-size <positive_integer>] [-mode <mode> ...] [-tcpdump (ENABLED | DISABLED)] [-perNIC (ENABLED | DISABLED)] [-fileName <string>] [-fileId <string>] [-filter <expression>] [-link (ENABLED | DISABLED)] [-nodes <positive_integer> ...]

Description

Start NetScaler packet capture tool.

Parameters

nf

Number of files to be generated in cycle. Default value: 24 Minimum value: 1 Maximum value: 100

time

Time per file (sec). Default value: 3600 Minimum value: 1

size

Size of the captured data. Set 0 for full packet trace. Default value: 164 Maximum value: 1514

mode

Capturing mode for trace. Mode can be any of the following values or combination of these values: RX Received packets before NIC pipelining NEW_RX Received packets after NIC pipelining TX Transmitted packets TXB Packets buffered for transmission IPV6 Translated IPv6 packets C2C Capture C2C message NS_FR_TX TX/TXB packets are not captured in flow receiver. Default mode: NEW_RX TXB Default value: DEFAULT_MODE

tcpdump

Trace is captured in TCPDUMP(.pcap) format. Default capture format is NSTRACE(.cap). Possible values: ENABLED, DISABLED Default value: DISABLED

perNIC

Use separate trace files for each interface. Works only with tcpdump format. Possible values: ENABLED, DISABLED Default value: DISABLED

fileName

Name of the trace file.

fileId

ID for the trace file name for uniqueness. Should be used only with -name option.

filter

Filter expression for nstrace. Maximum length of filter is 255 and it can be of following format: <expression> [<relop> <expression>] <relop> = (&& | ||) nstrace supports two types of filter expressions: Classic Expressions: <expression> = the expression string in the format: <qualifier> <operator> <qualifier-value> <qualifier> = SOURCEIP. <qualifier-value> = A valid IP address <qualifier> = SOURCEPORT. <qualifier-value> = A valid port number. <qualifier> = DESTIP. <qualifier-value> = A valid IP address. <qualifier> = DESTPORT. <qualifier-value> = A valid port number. <qualifier> = IP. <qualifier-value> = A valid IP address. <qualifier> = PORT. <qualifier-value> = A valid port number. <qualifier> = SVCNAME. <qualifier-value> = The name of a service. <qualifier> = VSVRNAME. <qualifier-value> = The name of a vserver. <qualifier> = CONNID <qualifier-value> = A valid PCB dev number. <qualifier> = VLAN <qualifier-value> = A valid VLAN ID. <qualifier> = INTF <qualifier-value> = A valid interface id in the form of x/y (n/x/y in case of cluster interface). <operator> = (== | eq | != | neq | > | gt | < | lt | >= | ge | <= | le | BETWEEN) eg: start nstrace -filter "SOURCEIP == 10.102.34.201 || (SVCNAME != s1 && SOURCEPORT > 80)" The filter expression should be given in double quotes. Default Expressions: <expression> = CONNECTION.<qualifier>.<qualifier-method>.(<qualifier-value>) <qualifier> = SRCIP <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address. example = CONNECTION.SRCIP.EQ(127.0.0.1) <qualifier> = DSTIP <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address. example = CONNECTION.DSTIP.EQ(127.0.0.1) <qualifier> = IP <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address. example = CONNECTION.IP.EQ(127.0.0.1) <qualifier> = SRCIPv6 <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv6 address. example = CONNECTION.SRCIPv6.EQ(2001:db8:0:0:1::1) <qualifier> = DSTIPv6 <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv6 address. example = CONNECTION.DSTIPv6.EQ(2001:db8:0:0:1::1) <qualifier> = IPv6 <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv6 address. example = CONNECTION.IPv6.EQ(2001:db8:0:0:1::1) <qualifier> = SRCPORT <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A valid port number. example = CONNECTION.SRCPORT.EQ(80) <qualifier> = DSTPORT <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A valid port number. example = CONNECTION.DSTPORT.EQ(80) <qualifier> = PORT <qualifier-method> = [EQ | NE] <qualifier-value> = A valid port number. example = CONNECTION.PORT.EQ(80) <qualifier> = VLANID <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A valid vlan ID. example = CONNECTION.VLANID.EQ(0) <qualifier> = CONNID <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A valid PCB dev number. example = CONNECTION.CONNID.EQ(0) <qualifier> = PPEID <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A valid core ID. example = CONNECTION.PPEID.EQ(0) <qualifier> = SVCNAME <qualifier-method> = [EQ | NE | CONTAINS | STARTSWITH | ENDSWITH] <qualifier-value> = A valid text string. example = CONNECTION.SVCNAME.EQ("name") <qualifier> = INTF <qualifier-method> = [EQ | NE] <qualifier-value> = A valid interface id in the form of x/y. example = CONNECTION.INTF.EQ("x/y") eg: start nstrace -filter "CONNECTION.SRCIP.EQ(127.0.0.1)

|| (CONNECTION.SVCNAME.NE("s1") && CONNECTION.SRCPORT.EQ(80))" The filter expression should be given in double quotes. common use cases: Trace capturing full sized traffic from/to ip 10.102.44.111, excluding loopback traffic start nstrace -size 0 -filter "CONNECTION.IP.NE(127.0.0.1) && CONNECTION.IP.EQ(10.102.44.111)" Trace capturing all traffic to (terminating at) port 80 or 443 start nstrace -size 0 -filter "CONNECTION.DSTPORT.EQ(443) || CONNECTION.DSTPORT.EQ(80)" Trace capturing all backend traffic specific to service service1 along with corresponding client side traffic start nstrace -size 0 -filter "CONNECTION.SVCNAME.EQ("service1")" -link ENABLED Trace capturing all traffic through NS interface 1/1 start nstrace -filter "CONNECTION.INTF.EQ("1/1")" Trace capturing all traffic specific through vlan 2 start nstrace -filter "CONNECTION.VLANID.EQ(2)" Trace capturing all frontend (client side) traffic specific to lb vserver vserver1 along with corresponding server side traffic start nstrace -size 0 -filter "CONNECTION.LB_VSERVER.NAME.EQ("vserver1")" -link ENABLED

link

Includes filtered connection's peer traffic. Possible values: ENABLED, DISABLED Default value: DISABLED

nodes

Nodes on which tracing is started. Maximum value: 32

Example

start nstrace -time 10

Top

stop nstrace

Synopsis

stop nstrace

Description

Stop running NetScaler packet capture tool.

Example

stop nstrace

Top

show nstrace

Synopsis

show nstrace

Description

Display nstrace parameters set through 'start nstrace' command.

Example

show nstrace

Top

Cache Commands

This group of commands can be used to perform operations on the following entities:

- cache
- cache policy
- cache policylabel
- cache contentGroup
- cache forwardProxy
- cache selector
- cache object
- cache stats
- cache global
- cache parameter

cache

stat cache

Synopsis

stat cache [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display the Integrated Cache statistics.

cache policy

[add | rm | set | unset | show | stat | rename]

add cache policy

Synopsis

add cache policy <policyName> -rule <expression> -action <action> [-storeInGroup <string>] [-invalGroups <string> ...] [-invalObjects <string> ...] [-undefAction (NOCACHE | RESET)]

Description

Create Integrated Cache policies. The newly created policy is in the inactive state. To activate the policy, use the ###bind cache global### command. The type of the policy depends on whether it is a request policy or a response policy, and the type of the specified action, as follows: CACHE or MAY_CACHE action: positive cachability policy NOCACHE or MAY_NOCACHE action: negative cachability policy INVAL action: Dynamic Invalidation Policy The order in which the policies are configured is significant. For a detailed discussion of the significance of the order, see the System Installation and Configuration Guide.

Parameters

policyName

The name of the new Integrated Cache policy.

rule

The request/response rule that will trigger the given action. The only actions you can specify with a request rule are: MAY_CACHE, MAY_NOCACHE, and INVAL. You specify a rule using a single expression or a logical combination of expressions (called a compound expression). You can combine xpressions using the && and || operators. For more information on creating expressions, refer to the add expression CLI command. Note: If a compound expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes. The following are examples of valid expressions: ns_ext_cgi||ns_ext_asp "ns_non_get && (ns_header_cookie||ns_header_pragma)"

action

The integrated cache action to be applied when the system finds content that matches the rules. Possible values: CACHE, NOCACHE, MAY_CACHE, MAY_NOCACHE, INVAL

storeInGroup

The content group where the object will be stored when the action directive is CACHE

invalGroups

The content group(s) to be invalidated when the action directive is INVAL

invalObjects

The content group(s) where the objects will be invalidated when the action directive is INVAL

undefAction

A CACHE action, which is used by the policy when the rule evaluation is undefined. The undef action can be NOCACHE or RESET. Possible values: NOCACHE, RESET

Top

rm cache policy

Synopsis

rm cache policy <policyName>

Description

Remove the specified Integrated Cache policy.

Parameters

policyName

The name of the cache policy to be removed.

Top

set cache policy

Synopsis

set cache policy <policyName> [-rule <expression>] [-action <action>] [-storeInGroup <string>] [-invalGroups <string> ...] [-invalObjects <string> ...] [-undefAction (NOCACHE | RESET)]

Description

Set a new rule/action/storeInGroup/invalGroups/invalObjects/undefAction for existing cache policy. The rule flow type can change only if action and undefAction(if present) are of NEUTRAL flow type

Parameters

policyName

The name of the new Integrated Cache policy.

rule

The request/response rule that will trigger the given action. The only actions you can specify with a request rule are: MAY_CACHE, MAY_NOCACHE, and INVAL. You specify a rule using a single expression or a logical combination of expressions (called a compound expression). You can combine xpressions using the && and || operators. For more information on creating expressions, refer to the add expression CLI command. Note: If a compound expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes. The following are examples of valid expressions: ns_ext_cgi||ns_ext_asp "ns_non_get && (ns_header_cookie||ns_header_pragma)"

action

The integrated cache action to be applied when the system finds content that matches the rules. Possible values: CACHE, NOCACHE, MAY_CACHE, MAY_NOCACHE, INVAL

storeInGroup

The content group where the object will be stored when the action directive is CACHE

invalGroups

The content group(s) to be invalidated when the action directive is INVAL

invalObjects

The content group(s) where the objects will be invalidated when the action directive is INVAL

undefAction

A CACHE action, to be used by the policy when the rule evaluation turns out to be undefined. The undef action can be NOREWRITE or RESET. Possible values: NOCACHE, RESET

Example

set cache policy pol9 -rule "http.req.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

Top

unset cache policy

Synopsis

unset cache policy <policyName> [-storeInGroup] [-invalGroups] [-invalObjects] [-undefAction]

Description

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

Top

show cache policy

Synopsis

show cache policy [<policyName>] show cache policy stats - alias for 'stat cache policy'

Description

Display all configured cache policies. To display a single cache policy, specify the name of the policy. When all Integrated Cache policies are displayed, the order of the displayed policies within each group is the same as the evaluation order of the policies. There are three groups: request policies, response policies, and dynamic invalidation policies.

Parameters

policyName

The name of the cache policy to be displayed.

Top

stat cache policy

Synopsis

stat cache policy [<policyName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display cache policy statistics.

Parameters

policyName

The name of the cache policy for which statistics will be displayed. If not given statistics are shown for all cache policies.

Example

stat cache policy

Top

rename cache policy

Synopsis

rename cache policy <policyName>@ <newName>@

Description

Rename a cache policy.

Parameters

policyName

The name of the cache policy.

newName

The new name of the cache policy.

Example

rename cache policy oldname newname

Top

cache policylabel

[add | rm | bind | unbind | show | stat | rename]

add cache policylabel

Synopsis

add cache policylabel <labelName> -evaluates <evaluates>

Description

Add a cache policy label.

Parameters

labelName

Name of the cache policy label.

evaluates

Gives when policies bound to this label get executed. Possible values: REQ, RES, MSSQL_REQ, MSSQL_RES, MYSQL_REQ, MYSQL_RES

Example

add cache policylabel cache_http_url -evaluates REQ

Top

rm cache policylabel

Synopsis

rm cache policylabel <labelName>

Description

Remove a cache policy label.

Parameters

labelName

Name of the cache policy label.

Example

rm cache policylabel cache_http_url

Top

bind cache policylabel

Synopsis

bind cache policylabel <labelName> -policyName <string> -priority <positive_integer> [-gotoPriorityExpression <expression>] [-invoke (<labelType> <labelName>)]

Description

Bind the cache policy to one of the labels.

Parameters

labelName

Name of the cache policy label.

policyName

The cache policy name.

Example

i) bind cache policylabel cache_http_url pol_1 1 2 -invoke reqvserver CURRENT
ii) bind cache policylabel cache_http_url pol_2 2

Top

unbind cache policylabel

Synopsis

unbind cache policylabel <labelName> -policyName <string> [-priority <positive_integer>]

Description

Unbind entities from cache label.

Parameters

labelName

Name of the cache policy label.

policyName

The cache policy name.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind cache policylabel cache_http_url pol_1

Top

show cache policylabel

Synopsis

show cache policylabel [<labelName>]

Description

Display policy label or policies bound to cache policylabel.

Parameters

labelName

Name of the cache policy label.

Example

i) show cache policylabel cache_http_url
ii) show cache policylabel

Top

stat cache policylabel

Synopsis

stat cache policylabel [<labelName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of cache policylabel(s).

Parameters

labelName

The name of the cache policy label for which statistics will be displayed. If not given statistics are shown for all cache policylabels.

Top

rename cache policylabel

Synopsis

rename cache policylabel <labelName>@ <newName>@

Description

Rename a cache policy label.

Parameters

labelName

The name of the cache policylabel.

newName

The new name of the cache policylabel.

Example

rename cache policylabel oldname newname

Top

cache contentGroup

[add | rm | set | unset | show | expire | flush]

add cache contentGroup

Synopsis

add cache contentGroup <name> [-weakPosRelExpiry <secs> | -relExpiry <secs> | -relExpiryMilliSec <msecs> | -absExpiry <HH:MM> ... | -absExpiryGMT <HH:MM> ...] [-heurExpiryParam <positive_integer>] [-weakNegRelExpiry <secs>] [(-hitParams <string> ... [-ignoreParamValueCase (YES | NO) | -hitSelector <string> | -invalSelector <string>] [-matchCookies (YES | NO)])] [-invalParams <string> ... [-invalRestrictedToHost (YES | NO)]] [-pollEveryTime (YES | NO)] [-ignoreReloadReq (YES | NO)] [-removeCookies (YES | NO)] [-prefetch (YES | NO) [-prefetchPeriod <secs> | -prefetchPeriodMilliSec <msecs>]] [-prefetchMaxPending <positive_integer>] [-flashCache (YES | NO)] [-expireAtLastByte (YES | NO)] [-insertVia (YES | NO)] [-insertAge (YES | NO)] [-insertETag (YES | NO)] [-cacheControl <string>] [-quickAbortSize <KBytes>] [-minResSize <KBytes>] [-maxResSize <KBytes>] [-memLimit <MBytes>] [-ignoreReqCachingHdrs (YES | NO)] [-minHits <integer>] [-alwaysEvalPolicies (YES | NO)] [-pinned (YES | NO)] [-lazyDnsResolve (YES | NO)] [-type <type>]

Description

Create a new content group.

Parameters

name

The name of the content group to be created

weakPosRelExpiry

Use this parameter for responses with response codes between 200 and 399. (Similar to -relExpiry but has lesser precedence.) Default value: VAL_NOT_SET Maximum value: 31536000

heurExpiryParam

The heuristic expiry time, in percent of the duration since the object was last modified Default value: VAL_NOT_SET Maximum value: 100

relExpiry

The relative expiry time in seconds Default value: VAL_NOT_SET Maximum value: 31536000

relExpiryMilliSec

The relative expiry time in milliseconds. Default value: VAL_NOT_SET Maximum value: 86400000

absExpiry

Up to 4 times a day (local time) when all objects in the content group must expire.

absExpiryGMT

Up to 4 times a day (GMT), when all objects in the content group must expire.

weakNegRelExpiry

Use this parameter for all negative responses. This value will be used only if the expiry time cannot be determiend from any other source. Default value: VAL_NOT_SET Maximum value: 31536000

hitParams

Use these parameters for parameterized hit evaluation of an object. Up to 128 parameters can be configured.

invalParams

Use these parameters for parameterized invalidation of an object. Up to 8 parameters can be configured.

ignoreParamValueCase

Use this parameter to specify whether to ignore case when comparing parameter values during parameterized hit evaluation. (Parameter value case is always ignored during parameterized invalidation.) Possible values: YES, NO Default value: VAL_NOT_SET

matchCookies

Use this parameter to specify whether to look for parameters also in the cookie header. Possible values: YES, NO Default value: VAL_NOT_SET

invalRestrictedToHost

Use this parameter to specify whether the host header should be taken into account during parameterized invalidation. Possible values: YES, NO Default value: VAL_NOT_SET

pollEveryTime

Use this parameter to specify whether to poll every time for the objects in this content group Possible values: YES, NO Default value: NO

ignoreReloadReq

Use this parameter to specify whether a request can force the system to reload a cached object from the origin. To guard against Denial of Service attacks, you should set this flag to YES. To get RFC-compliant behavior you should set it to NO. Possible values: YES, NO Default value: YES

removeCookies

Use this parameter to specify whether to remove cookies from a response. Possible values: YES, NO Default value: YES

prefetch

Use this parameter to specify whether Integrated Cache should attempt to refresh an object immediately before it is about to go stale. Possible values: YES, NO Default value: YES

prefetchPeriod

The duration in seconds of the period during which prefetch should be attempted, immediately before the object's calculated expiry time. Default value: VAL_NOT_SET Maximum value: 4294967294

prefetchPeriodMilliSec

The duration in milliseconds of the period during which prefetch should be attempted, immediately before the object's calculated expiry time. Default value: VAL_NOT_SET Maximum value: 4294967290

prefetchMaxPending

The maximum number of outstanding prefetches on the contentgroup Default value: VAL_NOT_SET

flashCache

Use this parameter to specify whether Integrated Cache should do flash cache. Possible values: YES, NO Default value: NO

expireAtLastByte

Use this parameter to specify whether Integrated Cache should expire the content immediately after receving the last body byte. Possible values: YES, NO Default value: NO

insertVia

Use this parameter to specify whether Integrated Cache should insert a Via header. Possible values: YES, NO Default value: YES

insertAge

Use this parameter to specify whether Integrated Cache should insert an Age header. Possible values: YES, NO Default value: YES

insertETag

Use this parameter to specify whether Integrated Cache should insert an ETag header. Possible values: YES, NO Default value: YES

cacheControl

Use this parameter to specify the Cache-Control header to be inserted.

quickAbortSize

If the client aborts when the downloaded response size is less than or equal to quick-abort-size, then Integrated Cache will stop downloading the response. Default value: 4194303 Maximum value: 4194303

minResSize

The minimum size of the response. Maximum value: 2097151

maxResSize

The maximum size of the response Default value: 80 Maximum value: 2097151

memLimit

The memory limit for the content group, in MB. The limit is not exact. At times, a group's memory utilization may overshoot the limit, only to stabilize later. Default value: 65536

ignoreReqCachingHdrs

Use this parameter to specify whether to ignore the Cache-control and Pragma headers in the incoming request. Possible values: YES, NO Default value: YES

minHits

Specify the minimum number of accesses for an object to be stored in Cache.

alwaysEvalPolicies

Forces policy evaluation for each response arriving from origin. Possible values: YES, NO Default value: NO

pinned

Setting pinned to YES prevents IC from flushing objects from this contentgroup under memory pressure. Possible values: YES, NO Default value: NO

lazyDnsResolve

Setting this parameter to NO causes DNS resolution for every response. Setting this parameter to YES causes DNS resolution only when the destination IP in the request does not match the destination IP of the stored object. Possible values: YES, NO Default value: YES

hitSelector

The selector used for hit selection.

invalSelector

The selector used for invalidation.

type

This parameter will specify the type of content group Possible values: HTTP, MYSQL, MSSQL Default value: NSSVC_HTTP

Top

rm cache contentGroup

Synopsis

rm cache contentGroup <name>

Description

Remove the specified content group.

Parameters

name

The name of the content group to be removed.

Top

set cache contentGroup

Synopsis

set cache contentGroup <name> [-weakPosRelExpiry <secs> | -relExpiry <secs> | -relExpiryMilliSec <msecs> | -absExpiry <HH:MM> ... | -absExpiryGMT <HH:MM> ...] [-heurExpiryParam <positive_integer>] [-weakNegRelExpiry <secs>] [-hitParams <string> ... | -hitSelector <string> | -invalSelector <string>] [-invalParams <string> ...] [-ignoreParamValueCase (YES | NO)] [-matchCookies (YES | NO)] [-invalRestrictedToHost (YES | NO)] [-pollEveryTime (YES | NO)] [-ignoreReloadReq (YES | NO)] [-removeCookies (YES | NO)] [-prefetch (YES | NO)] [-prefetchPeriod <secs> | -prefetchPeriodMilliSec <msecs>] [-prefetchMaxPending <positive_integer>] [-flashCache (YES | NO)] [-expireAtLastByte (YES | NO)] [-insertVia (YES | NO)] [-insertAge (YES | NO)] [-insertETag (YES | NO)] [-cacheControl <string>] [-quickAbortSize <KBytes>] [-minResSize <KBytes>] [-maxResSize <KBytes>] [-memLimit <MBytes>] [-ignoreReqCachingHdrs (YES | NO)] [-minHits <integer>] [-alwaysEvalPolicies (YES | NO)] [-pinned (YES | NO)] [-lazyDnsResolve (YES | NO)]

Description

Modify attributes of the content group.

Parameters

name

The name of the content group whose attibutes will be changed.

weakPosRelExpiry

Responses with response codes between 200 and 399. (Similar to -relExpiry, but has lesser precedence.) Maximum value: 31536000

heurExpiryParam

The heuristic expiry time, in percentage of the elapsed time since the object was last modified. Maximum value: 100

relExpiry

The relative expiry time in seconds. Default value: VAL_NOT_SET Maximum value: 31536000

relExpiryMilliSec

The relative expiry time in milliseconds. Default value: VAL_NOT_SET Maximum value: 86400000

absExpiry

Expiry time for all objects in the content group(up to 4 times a day [local time]).

absExpiryGMT

Expiry time for all objects in the content group(up to 4 times a day [GMT]).

weakNegRelExpiry

All negative responses. This value is used only if the expiry time cannot be determined from any other source. Maximum value: 31536000

hitParams

Parameterized hit evaluation of an object. Up to 128 parameters can be configured.

invalParams

Parameterized invalidation of an object. Up to 8 parameters can be configured.

ignoreParamValueCase

The option to ignore case while comparing parameter values during parameterized hit evaluation. The case of the parameter value is always ignored during parameterized invalidation. Possible values: YES, NO

matchCookies

The option to look for parameters in the cookie header. Possible values: YES, NO

invalRestrictedToHost

The option to consider the Host header during parameterized invalidation. Possible values: YES, NO

pollEveryTime

The option to poll every time for the objects in this content group. Possible values: YES, NO Default value: NO

ignoreReloadReq

For a request, the option to force the system to reload a cached object from the origin. To guard against Denial of Service attacks, you should set this flag to YES. To get RFC-compliant behavior, you should set it to NO. Possible values: YES, NO Default value: YES

removeCookies

The option to remove cookies from response. Possible values: YES, NO Default value: YES

prefetch

The option to refresh an object immediately before it goes stale. Possible values: YES, NO Default value: YES

prefetchPeriod

The duration in seconds of the period during which prefetch should be attempted, immediately before the object's calculated expiry time. Default value: VAL_NOT_SET Maximum value: 4294967294

prefetchPeriodMilliSec

The duration in milliseconds of the period during which prefetch should be attempted, immediately before the calculated expiry time. Default value: VAL_NOT_SET Maximum value: 4294967290

prefetchMaxPending

The maximum number of outstanding prefetches on the contentgroup.

flashCache

The option to do flash cache on Integrated caching. Possible values: YES, NO Default value: NO

expireAtLastByte

The option to expire the content immediately after receving the last body byte. Possible values: YES, NO Default value: NO

insertVia

The option to insert a Via header. Possible values: YES, NO Default value: YES

insertAge

The option to insert an Age header. Possible values: YES, NO Default value: YES

insertETag

The option to insert an ETag header. Possible values: YES, NO Default value: YES

cacheControl

The option to insert a Cache-Control header.

quickAbortSize

The quick abort size. If the client aborts when the downloaded response size is less than or equal to the quick-abort-size, then the Integrated Cache will stop downloading the response. Maximum value: 4194303

minResSize

The minimum size of the response. Maximum value: 2097151

maxResSize

The maximum size of the response. Default value: 80 Maximum value: 2097151

memLimit

The memory limit in MB for the content group. The limit is not exact - a group's memory utilization may overshoot the limit, only to stabilize later. Default value: 65536

ignoreReqCachingHdrs

The option to ignore the Cache-control and Pragma headers in the incoming request. Possible values: YES, NO Default value: YES

minHits

The minimum number of accesses for an object to be stored in Cache.

alwaysEvalPolicies

The option to force policy evaluation for each response arriving from the origin. Possible values: YES, NO Default value: NO

pinned

The option for IC from flushing objects from this contentgroup under memory pressure. Set YES for IC to take this state. Possible values: YES, NO Default value: NO

lazyDnsResolve

Setting this parameter to NO causes DNS resolution for every response. Setting this parameter to YES causes DNS resolution only when the destination IP in the request does not match the destination IP of the stored object. Possible values: YES, NO Default value: YES

hitSelector

The selector used for hit selection.

invalSelector

The selector used for invalidation.

Top

unset cache contentGroup

Synopsis

unset cache contentGroup <name> [-weakPosRelExpiry] [-heurExpiryParam] [-relExpiry] [-relExpiryMilliSec] [-absExpiry] [-absExpiryGMT] [-weakNegRelExpiry] [-hitParams] [-invalParams] [-ignoreParamValueCase] [-matchCookies] [-invalRestrictedToHost] [-pollEveryTime] [-ignoreReloadReq] [-removeCookies] [-prefetch] [-prefetchPeriod] [-prefetchPeriodMilliSec] [-prefetchMaxPending] [-flashCache] [-expireAtLastByte] [-insertVia] [-insertAge] [-insertETag] [-cacheControl] [-quickAbortSize] [-minResSize] [-maxResSize] [-memLimit] [-ignoreReqCachingHdrs] [-minHits] [-alwaysEvalPolicies] [-pinned] [-lazyDnsResolve] [-hitSelector] [-invalSelector]

Description

Use this command to remove cache contentGroup settings.Refer to the set cache contentGroup command for meanings of the arguments.

Top

show cache contentGroup

Synopsis

show cache contentGroup [<name>]

Description

Display all content groups. To display a single content group, specify the name of the content group.

Parameters

name

The name of the content group.

Top

expire cache contentGroup

Synopsis

expire cache contentGroup <name>

Description

Expire the objects in the specified content group.

Parameters

name

The name of the content group whose objects are to be expired.

Top

flush cache contentGroup

Synopsis

flush cache contentGroup <name> [-query <string> | -selectorValue <string>] [-host <string>]

Description

Flush the objects in the specified content group.

Parameters

name

The name of the content group whose objects are to be flushed.

query

If a query string is specified, then the selected objects in this group will be flushed using parameterized invalidation. Otherwise, all objects in the group will be flushed.

host

To be set only if parameterized invalidation is being done. Objects belonging only to the specified host will be flushed. The host argument can be provided if and only if -invalRestrictedToHost is set to YES for the given group.

selectorValue

The value of the selector to be used for flushing objects in the contentgroup.

Top

cache forwardProxy

[add | rm | show]

add cache forwardProxy

Synopsis

add cache forwardProxy <IPAddress> <port>

Description

Add a forward proxy known to Integrated cache.

Parameters

IPAddress

The IP address of the forward proxy.

port

The port of the forward proxy. Minimum value: 1

Top

rm cache forwardProxy

Synopsis

rm cache forwardProxy <IPAddress> <port>

Description

Remove a forward proxy known to Integrated cache.

Parameters

IPAddress

The IP address of the forward proxy.

port

The port of the forward proxy. Minimum value: 1

Top

show cache forwardProxy

Synopsis

show cache forwardProxy

Description

Display all forward proxies known to Integrated cache.

Top

cache selector

[add | rm | set | show]

add cache selector

Synopsis

add cache selector <selectorName> <rule> ...

Description

Create Integrated Cache selectors. A selector is an abstraction for a collection of PIXL expressions. After creating a selector, you can use it as either a hitSelector (for doing hit selection) or as an invalSelector (for invalidating cached objects), or both. You need to specify at least one expression when you create a selector.

Parameters

selectorName

The name of the Integrated Cache selector.

rule

The set of PIXL expressions.

Top

rm cache selector

Synopsis

rm cache selector <selectorName>

Description

Use this command to remove Integrated Cache selectors.

Parameters

selectorName

The name of the Integrated Cache selector.

Top

set cache selector

Synopsis

set cache selector <selectorName> <rule> ...

Description

Change the set of expressions associated with Integrated Cache selectors.

Parameters

selectorName

The name of the Integrated Cache selector.

rule

The PIXL expressions.

Top

show cache selector

Synopsis

show cache selector [<selectorName>]

Description

Display Integrated Cache selectors.

Parameters

selectorName

The name of the Integrated Cache selector.

Top

cache object

[show | expire | flush]

show cache object

Synopsis

show cache object [(-url <URL> (-host <string> [-port <port>] [-groupName <string>] [-httpMethod (GET | POST)])) | -locator <positive_integer> | -httpStatus <positive_integer> | -group <string> | -ignoreMarkerObjects (ON | OFF) | -includeNotReadyObjects (ON | OFF)]

Description

Show a list of all cached objects, or the properties of a particular cache object.

Parameters

url

The URL of the object.

locator

The id of the cached object.

httpStatus

HTTP status of the object.

host

The hostname of the object.

port

The host port of the object. Default value: 80 Minimum value: 1

groupName

The name of the content group to be in which the cell is present

httpMethod

The HTTP request method that caused the object to be stored. Possible values: GET, POST Default value: NS_HTTP_METHOD_GET

group

The name of the content group whose objects should be listed.

ignoreMarkerObjects

Ignore marker objects Possible values: ON, OFF

includeNotReadyObjects

Include objects not-ready for a cache hit Possible values: ON, OFF

Top

expire cache object

Synopsis

expire cache object (-locator <positive_integer> | (-url <URL> (-host <string> [-port <port>] [-groupName <string>] [-httpMethod (GET | POST)])))

Description

Expire a cached object.

Parameters

locator

The id of the cached object.

url

The URL of the object to be expired.

host

The host of the object to be expired.

port

The host port of the object to be expired. Default value: 80 Minimum value: 1

groupName

The name of the content group to be in which the cell is present.

httpMethod

The HTTP request method that caused the object to be stored. Possible values: GET, POST Default value: NS_HTTP_METHOD_GET

Top

flush cache object

Synopsis

flush cache object (-locator <positive_integer> | (-url <URL> (-host <string> [-port <port>] [-groupName <string>] [-httpMethod (GET | POST)])))

Description

Flush a cached object.

Parameters

locator

The ID of the cached object.

url

The URL of the object to be flushed.

host

The host of the object to be flushed.

port

The host port of the object to be flushed. Default value: 80 Minimum value: 1

groupName

The name of the content group to be in which the cell is present.

httpMethod

The HTTP request method that caused the object to be stored. Possible values: GET, POST Default value: NS_HTTP_METHOD_GET

Top

cache stats

show cache stats

Synopsis

show cache stats - alias for 'stat cache'

Description

show cache stats is an alias for stat cache

cache global

[bind | unbind | show]

bind cache global

Synopsis

bind cache global <policy> -priority <positive_integer> [-gotoPriorityExpression <expression>] [-type <type>] [-invoke (<labelType> <labelName>)]

Description

Bind the cache policy to one of the two global lists of cache policies. A policy becomes active only after it is bound. All HTTP traffic will be evaluated against these two policy banks. There is a request time policy bank and a response time policy bank. The flow type of the policy implicitly determines which bank it gets bound to. Each bank of policies is an ordered list ordered by policies priority values. Policy Bank Evaluation The goal of evaluation is to traverse the ordered list of policies in the bank, find out which policies match and build a result set that will contain the actions of all the matching policies. While evaluating a policy if any PIXL expression cannot be evaluated then UNDEF processing will get triggered. There are also other scenarios during policy traversal when UNDEF processing can get triggered. If an UNDEF event occurs while processing a policy, then (i) policy bank traversal ends, (ii) the result set of actions that was built so far is wiped out (iii) the current policy's undefAction is put in the result set and the evaluation ends.

Parameters

policy

The name of the Integrated Cache policy to be bound.

Top

unbind cache global

Synopsis

unbind cache global <policy> [-type <type>] [-priority <positive_integer>]

Description

Inactivate the policy.

Parameters

policy

The name of the Integrated Cache policy to unbind

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Top

show cache global

Synopsis

show cache global [-type <type>]

Description

Display the cache global bindings.

Parameters

type

The bindpoint to which policy is bound. Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

Example

show cache global

Top

cache parameter

[set | unset | show]

set cache parameter

Synopsis

set cache parameter [-memLimit <MBytes>] [-via <string>] [-verifyUsing <verifyUsing>] [-maxPostLen <positive_integer>] [-prefetchMaxPending <positive_integer>] [-enableBypass (YES | NO)] [-undefAction (NOCACHE | RESET)]

Description

Modify the global configuration of the Integrated Cache.

Parameters

memLimit

The memory limit for Integrated Cache.

via

The string to be inserted in the "Via" header. A Via header is inserted in all responses served from a content group if its insertVia flag is set.

verifyUsing

The criteria for deciding whether a cached object can be served for an incoming HTTP request. a. If the value of this attribute is set to HOSTNAME, then URL , host name and host port values in the incoming HTTP request header must match before a cached object can be served. The IP address and the TCP port of the destination host are not matched. For certain deployments the HOSTNAME setting can be a security risk. A rogue client can access a rogue server via the Integrated Cache using the following HTTP request : GET / HTTP/1.1 Host: sensitive.foo.com Integrated Cache will store the rogue page served by the rogue server. Any subsequent client trying to access the root page from sensitive.foo.com will be served the rogue page. The HOSTNAME setting should only be set if it is certain that no rogue client can access a rogue server via the Integrated Cache. The YES setting can lead to more hits if DNS-based load balancing is in use and the same content can be served by multiple backend servers. b. If the attribute is set to HOSTNAME_AND_IP, then the following items must match: URL, host name, host port in the incoming HTTP request header, and the IP address and TCP port of the destination server. c. If the attribute is set to DNS, then the following items should match: URL, host name and host port in the incoming HTTP request, and the TCP port. The hostname is used to do a DNS lookup of the destination server's IP address, and is compared with the set of addresses returned by the DNS lookup. The default value of this attribute is DNS.

Possible values: HOSTNAME, HOSTNAME_AND_IP, DNS

maxPostLen

maximum number of POST body bytes to consider when evaluating parameters for a content group for which you have configured hitParams and invalParams. Default value: 4096 Maximum value: 131072

prefetchMaxPending

The maximum number of outstanding prefetches in the IC.

enableBypass

The bypass parameter. When this value is set to NO, an incoming request will serve a hit if a matching object is found in cache storage, regardless of the cacheability policy configuration. If set to YES, the bound request cacheability policies are evaluated before attempting any hit selection in the cache storage. If the request matches a policy with a NOCACHE action, the request will bypass all cache processing. This flag does not affect processing of requests that match any invalidation policy. Possible values: YES, NO

undefAction

Set the default cache undef action. If an UNDEF event is triggered during policy evaluation and if the current policy's undefAction is not specified, then this global undefAction value is used. Can be NOCACHE or RESET. NOCACHE is the default value of default cache undef action. Possible values: NOCACHE, RESET

Top

unset cache parameter

Synopsis

unset cache parameter [-memLimit] [-via] [-verifyUsing] [-maxPostLen] [-prefetchMaxPending] [-enableBypass] [-undefAction]

Description

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

Top

show cache parameter

Synopsis

show cache parameter

Description

Display the global configuration of the Integrated Cache.

Top

CLI Commands

This group of commands can be used to perform operations on the following entities:

- config
- whoami
- exit
- quit
- man
- history
- help
- source
- batch
- unalias
- alias
- cls
- cli attribute
- cli prompt
- cli mode

config

Synopsis

config

Description

Enter this command to enter contextual mode.

whoami

whoami

Synopsis

whoami

Description

Show the current user.

exit

exit

Synopsis

exit

Description

Use this command to back out one level in config mode, or to terminate the CLI when not in config mode.);

quit

quit

Synopsis

quit

Description

Use this command to terminate the CLI. Note: typing <Ctrl>+<d> will also terminate the CLI.

man

man

Synopsis

man [(commandName)]

Description

Use this command to invoke the man page for the specified command. You can specify the command in full, or partially, if it is uniquely resolvable.

Parameters

commandName

The name of the command.

Example

man add vs

history

history

Synopsis

history

Description

Use this command to see the history of the commands executed on CLI.

Example

history

```
1 add snmp trap SPECIFIC 10.102.130.228
2 save config
3 show system session
4 swhell
5 shell
6 what
7 shell
8 help  stat lbvserver
...
```

help

help

Synopsis

help [(commandName) | <groupName> | -all]

Description

Use this command to display help information for a CLI command, for a group of commands, or for all CLI commands.

Parameters

commandName

The name of a command for which you want full usage information.

groupName

The name of a command group for which you want basic usage information.

all

Use this option to request basic usage information for all commands.

Example

1.To view help information for adding a virtual server, enter the following CLI command:
help add vserver
The following information is displayed:
Usage: add vserver <vServerName> <serviceType> [<IPAddress> port>] [-type (CONTENT | ADDRESS)] [-cach

where:
serviceType = (HTTP | FTP | TCP | UDP | SSL | SSL_BRIDGE | SSL_TCP | NNTP| DNS | ANY)
<cacheType> = (TRANSPARENT | REVERSE | FORWARD)
Done
2.To view help information for all DNS commands, enter the following command:
help dns
The following information is displayed:
add aaaaRec <hostname> <IPv6Address> ... [-TTL <secs>]
rm aaaaRec <hostname> [<IPv6Address> ...]
show aaaaRec [<hostname> | -type <type>]
add addRec <hostname> <IPAddress> ... [-TTL <secs>] [-private <ip_addr>]
rm addRec <hostname> [<IPAddress> ...]
show addRec [<hostname> | -type <type>]

```
add cnameRec <aliasName> <canonicalName> [-TTL <secs>]
rm cnameRec <aliasName>
show cnameRec [<aliasName> |  -type <type>]
add mxRec <domain> -mx <string> -pref <positive_integer> [-TTL <secs>]
rm mxRec <domain> <mx>
set mxRec <domain> -mx <string> [-pref <positive_integer>] [-TTL <secs>]
show mxRec [<domain> |  -type <type>]
add nsRec <domain> [-p <string>] [-s <string>] [-TTL <secs>]
rm nsRec <domain> [-p <string> |  -s <string>]
show nsRec [<domain> |  -type <type>]
set dns parameter [-timeout <secs>] [-retries <positive_integer>] [-minTTL <secs>] [-maxTTL <secs>] [-TTL (
show dns parameter
add soaRec <domain> -contact <string> -serial <positive_integer> -refresh <secs> -retry <secs> -expire <secs>
rm soaRec <domain>
set soaRec <domain> [-contact <string>] [-serial <positive_integer>][-refresh <secs>] [-retry <secs>] [-expire
show soaRec [<domain> |  -type <type>]
add dns ptrRec <reverseDomain> <domain> ... [-TTL <secs>]
rm dns ptrRec <reverseDomain> [<domain> ...]
show dns ptrRec [<reverseDomain> | -type <type>]
add dns srvRec <domain> <target> -priority <positive_integer>
   -weight <positive_integer> -port <positive_integer>
rm dns srvRec <domain> [<target> ...]
set dns srvRec <domain> <target> [-priority <positive_integer>]
   [-weight <positive_integer>] [-port <positive_integer>] [-TTL <secs>]
show dns srvRec [(<domain>  [<target>]) | -type <type>]
Done
```

source

source

Synopsis

source <fileName>

Description

Use this command to read the contents of a file and execute each line as a separate CLI command. Each command in the file being read must be on a separate line. Lines starting with # are considered comments.

Parameters

fileName

The name of the file to be sourced.

Example

source cmds.txt

batch

batch

Synopsis

batch -fileName <input_filename> [-outfile <output_filename>] [-ntimes <positive_integer>]

Description

Use this command to read the contents of a file and execute each line as a separate CLI command. Each command in the file must be on a separate line. Lines starting with # are considered comments.

Parameters

fileName

The name of the batch file.

outfile

The name of the file where the executed batch file will write its output. The default is standard output.

ntimes

The number of times the batch file will be executed. Default value: 1

Example

batch -f cmds.txt

unalias

unalias

Synopsis

unalias <pattern>

Description

Remove an alias

Parameters

pattern

Name of the alias

Example

unalias info

alias

alias

Synopsis

alias [<pattern> [(command)]]

Description

Create (short) aliases for (long) commands. Aliases are saved across NSCLI sessions. If no argument is specified, the alias command will display existing aliases.

Parameters

pattern

Alias name. (Can be a regular expression.)

Example

alias info "show ns info"

cls

cls

Synopsis

cls

Description

Clear the screen and reposition cursor at top right.

cli attribute

show cli attribute

Synopsis

show cli attribute

Description

Display attributes of the NetScaler CLI

cli prompt

[clear | set | show]

clear cli prompt

Synopsis

clear cli prompt

Description

Use this command to return the CLI prompt to the default (a single '>').

Top

set cli prompt

Synopsis

set cli prompt <promptString>

Description

Use this command to customize the CLI prompt.

Parameters

promptString

The prompt string. The following special values are allowed: %! - will be replaced by the history event number %u - will be replaced by the NetScaler user name %h - will be replaced by the NetScaler hostname %t - will be replaced by the current time %T - will be replaced by the current time (24 hr format) %d - will be replaced by the current date %s - will be replaced by the node state

Example

```
> set cli prompt "%h %T"
 Done
lb-ns1 15:16>
```

Top

show cli prompt

Synopsis

show cli prompt

Description

Use this command to display the current CLI prompt, with special values like '%h' unexpanded.

Example

```
10.101.4.22 15:20> sh cli prompt
       CLI prompt is set to "%h %T"
 Done
```

Top

cli mode

[set | unset | show]

set cli mode

Synopsis

set cli mode [-page (ON | OFF)] [-total (ON | OFF)] [-color (ON | OFF)]
[-disabledFeatureAction <disabledFeatureAction>] [-timeout <secs>] [-regex (ON | OFF)]

Description

Use this command to specify how the CLI should display command output.

Parameters

page

Determines whether output that spans more than one screen is "paged". Specify ON to pause the display after each screen of ouput. Possible values: ON, OFF Default value: OFF

total

Determines whether CLI "show" commands display a total count of objects before displaying the objects themselves. Possible values: ON, OFF Default value: OFF

color

Specifies whether output can be shown in color, if the terminal supports it. Possible values: ON, OFF Default value: OFF

disabledFeatureAction

Specifies what will happen when a configuration command is issued for a disabled feature. The following values are allowed: NONE - The action is allowed, and no warning message is issued.; ALLOW - The action is allowed, but a warning message is issued.; DENY - The action is not allowed.; HIDE - Commands that configure disabled features are hidden, and the CLI behaves as if they did not exist. Possible values: NONE, ALLOW, DENY, HIDE Default value: NS_ALLOW

timeout

CLI session inactivity timeout, in seconds. Timeout cannot have values in between 1 and 9. Default value: 300 Maximum value: 100000000

regex

If ON, regular expressions can be used as argument values Possible values: ON, OFF Default value: ON

Top

unset cli mode

Synopsis

unset cli mode [-page] [-total] [-color] [-disabledFeatureAction] [-timeout] [-regex]

Description

Use this command to remove cli mode settings.Refer to the set cli mode command for meanings of the arguments.

Top

show cli mode

Synopsis

show cli mode

Description

Use this command to display the current settings of parameters that can be set with the 'set cli mode' command.

Top

Cluster Commands

This group of commands can be used to perform operations on the following entities:

- cluster
- cluster instance
- cluster node
- cluster files
- cluster sync

cluster

join cluster

Synopsis

join cluster -clip <ip_addr> {-password }

Description

Joins the appliance to the cluster. You must execute this command from the NetScaler IP (NSIP) address of the node you want to add to the cluster. This command is the second part of the two-step process of adding a cluster node. The first part is adding this node to the cluster by using the .add cluster node. command from the cluster IP address. Join is not permitted if any of the node in cluster is in sync state.

Parameters

clip

The cluster IP address to which you are trying to add the node.

password

The password for the nsroot account of the configuration coordinator (CCO).

cluster instance

[add | rm | set | unset | enable | disable | show | stat]

add cluster instance

Synopsis

add cluster instance <clId> [-deadInterval <secs>] [-helloInterval <msecs>] [-preemption (ENABLED | DISABLED)]

Description

Adds a cluster instance to the appliance. Execute this command only on the first node that you add to the cluster.

Parameters

clId

A unique number that identifies the cluster. Minimum value: 1 Maximum value: 16

deadInterval

The amount of time (in seconds) after which the nodes that do not respond to the heartbeats are assumed to be down. Default value: 3 Minimum value: 3 Maximum value: 60

helloInterval

The amount of time (in milliseconds) after which heartbeats are sent to each cluster node to check the health status. Default value: 200 Minimum value: 200 Maximum value: 1000

preemption

Enable or disable the preemption of a cluster node that is configured as SPARE by a node that is configured as ACTIVE. When preemption is enabled, ACTIVE nodes are given precedence over SPARE nodes. This means that when an ACTIVE node comes online and finds that a SPARE node is serving traffic, it preempts the SPARE node and starts serving traffic. When preemption is disabled, the SPARE node continues serving traffic even after an ACTIVE node comes back online. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add cluster instance 1

Top

rm cluster instance

Synopsis

rm cluster instance <clId>

Description

Removes the cluster instance from the node. Execute this command on the NetScaler IP (NSIP) address of the node that you want to remove from the cluster. After executing this command, you must execute the rm cluster node. command on the cluster IP address.

Parameters

clId

A unique number that identifies the cluster. Minimum value: 1 Maximum value: 16

Example

rm cluster instance 1

Top

set cluster instance

Synopsis

set cluster instance <clId> [-deadInterval <secs>] [-helloInterval <msecs>] [-preemption (ENABLED | DISABLED)]

Description

Modifies the attributes of a cluster instance.

Parameters

clId

The ID of the cluster instance whose properties you want to set. Minimum value: 1 Maximum value: 16

deadInterval

The amount of time (in seconds) after which the nodes that do not respond to the heartbeats are assumed to be down. Default value: 3 Minimum value: 3 Maximum value: 60

helloInterval

The amount of time (in milliseconds) after which heartbeats are sent to each cluster node to check the health status. Default value: 200 Minimum value: 200 Maximum value: 1000

preemption

Enable or disable the preemption of a cluster node that is configured as SPARE by a node that is configured as ACTIVE. When preemption is enabled, ACTIVE nodes are given precedence over SPARE nodes. This means that when an ACTIVE node comes online and finds that a SPARE node is serving traffic, it preempts the SPARE node and starts serving traffic. When preemption is disabled, the SPARE node continues serving traffic even after an ACTIVE node comes back online. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set cluster instance 1 -preemption ENABLED

Top

unset cluster instance

Synopsis

unset cluster instance <clId> [-deadInterval] [-helloInterval] [-preemption]

Description

Use this command to remove cluster instance settings.Refer to the set cluster instance command for meanings of the arguments.

Top

enable cluster instance

Synopsis

enable cluster instance <clId>

Description

Enables a cluster instance.

Parameters

clId

The ID of the cluster instance that you want to enable. Minimum value: 1 Maximum value: 16

Example

enable cluster instance 1

Top

disable cluster instance

Synopsis

disable cluster instance <clId>

Description

Disables a cluster instance.

Parameters

clId

The ID of the cluster instance that you want to disable. Minimum value: 1 Maximum value: 16

Example

disable cluster instance 1

Top

show cluster instance

Synopsis

show cluster instance [<clId>]

Description

Displays details of the cluster instance and the cluster nodes.

Parameters

clId

A unique number that identifies the cluster. Minimum value: 1 Maximum value: 16

Example

An example of the command's output is as follows:

```
1)Cluster ID: 1
        Dead Interval: 3 secs
        Hello Interval: 200 msecs
        Preemption: DISABLED
        Propagation: ENABLED
        Cluster Status: ENABLED(admin), ENABLED(operational), UP
        Member Nodes:
        Node ID       Node IP          Health    Admin State      Operational State
        -------       -------          ------    -----------      -----------------
1)      1             1.1.1.1*         UP        ACTIVE           ACTIVE(Configuration Coordinator)
2)      2             1.1.1.2          UP        ACTIVE           ACTIVE
 Done
 *: Local node
```

Top

stat cluster instance

Synopsis

stat cluster instance [<clId>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Displays the statistics of the cluster instance.

Parameters

clId

The ID of the cluster instance whose statistics must be displayed. Minimum value: 1 Maximum value: 16

Top

cluster node

[add | set | unset | rm | show | stat]

add cluster node

Synopsis

add cluster node <nodeId> <IPAddress> [-state <state>] [-backplane <interface_name>]

Description

Adds a NetScaler appliance to a cluster.

Parameters

nodeId

A unique number that identifies the cluster node. Maximum value: 31

IPAddress

The NetScaler IP (NSIP) address of the appliance that you want to add to the cluster. Only IPv4 addresses are supported.

state

The configured state of the cluster node. ACTIVE - The node serves traffic. SPARE - The node does not serve traffic till an ACTIVE node goes down. PASSIVE - The node does not serve traffic till explicitly made ACTIVE. This state is useful during temporary maintenance activities where it is desirable that the node takes part in the consensus protocol, but does not serve traffic. Possible values: ACTIVE, SPARE, PASSIVE Default value: NSACL_NODEST_PASSIVE

backplane

The interface to be used to communicate with the other cluster nodes. The interface must be specified in the three-tuple form, n/c/u, where n represents the node ID. Minimum value: 1

Example

add cluster node 1 1.1.1.1 -backplane 1/1/1 -state ACTIVE

Top

set cluster node

Synopsis

set cluster node <nodeId> [-state <state>] [-backplane <interface_name>]

Description

Modifies the attributes of a cluster node.

Parameters

nodeId

The ID of the cluster node whose properties you want to set. Maximum value: 31

state

The configured state of the cluster node. ACTIVE - The node serves traffic. SPARE - The node does not serve traffic till an ACTIVE node goes down. PASSIVE - The node does not serve traffic till explicitly made ACTIVE. This state is useful during temporary maintenance activities where it is desirable that the node takes part in the consensus protocol, but does not serve traffic. Possible values: ACTIVE, SPARE, PASSIVE Default value: NSACL_NODEST_PASSIVE

backplane

The interface to be used to communicate with the other cluster nodes. The interface must be specified in the three-tuple form, n/c/u, where n represents the node ID. Minimum value: 1

Example

set cluster node 1 -state PASSIVE

Top

unset cluster node

Synopsis

unset cluster node <nodeId> [-state] [-backplane]

Description

Use this command to remove cluster node settings.Refer to the set cluster node command for meanings of the arguments.

Top

rm cluster node

Synopsis

rm cluster node <nodeId>

Description

Removes a node from the cluster. You must execute this command on the cluster IP address after executing the rm cluster instance. command from the node that you want to remove from the cluster.

Parameters

nodeId

The ID of the cluster node that you want to remove from the cluster. Maximum value: 31

Example

rm cluster node 1

Top

show cluster node

Synopsis

show cluster node [<nodeId>]

Description

Displays details of the cluster node.

Parameters

nodeId

The ID of the cluster node whose details must be displayed. If an ID is not provided, details of all nodes of the cluster are displayed. Default value: 255 Maximum value: 31

Example

An example of the command's output is as follows:

```
      1 cluster node:
1)Node ID: 1
      IP:              1.1.1.1*
      Backplane:         1/1/1
      Health:           UP
      Admin State:       ACTIVE
      Operational State:   ACTIVE(Configuration Coordinator)
      Sync State:        DISABLED
 Done
 *: Local node
```

Top

stat cluster node

Synopsis

stat cluster node [<nodeId>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Displays the statistics of the cluster node.

Parameters

nodeId

The ID of the cluster node whose statistics must be displayed. If an ID is not provided, statistics of all nodes of the cluster are displayed. Maximum value: 31

Top

cluster files

sync cluster files

Synopsis

sync cluster files [<Mode> ...]

Description

Synchronize SSL Certificates, SSL CRL lists, SSL VPN bookmarks, and other files from the CCO to other cluster nodes. This command must be executed only from the cluster IP address. This command will be automatically triggered from the CCO when a new node is added to a cluster and periodically during the lifetime of the cluster, to synchronize updated files between the cluster nodes. Note: Files on non-CCO nodes are not deleted if they do no not exist on the CCO. The command can be configured to synchronize directories or files which are specified by the following modes: Mode Paths all /nsconfig/ssl/ /var/netscaler/ssl/ /var/vpn/bookmark/ /nsconfig/dns/ /nsconfig/htmlinjection/ /netscaler/htmlinjection/ens/ /nsconfig/monitors/ /nsconfig/nstemplates/ /nsconfig/ssh/ /nsconfig/rc.netscaler /nsconfig/resolv.conf /nsconfig/inetd.conf /nsconfig/syslog.conf /nsconfig/snmpd.conf /nsconfig/ntp.conf /nsconfig/httpd.conf /nsconfig/sshd_config /nsconfig/hosts /nsconfig/enckey /var/nslw.bin/etc/krb5.conf /var/nslw.bin/etc/krb5.keytab /var/lib/likewise/db/ /var/download/ /var/wi/tomcat/webapps/ /var/wi/tomcat/conf/Catalina/localhost/ /var/wi/java_home/lib/security/cacerts /var/wi/java_home/jre/lib/security/cacerts ssl /nsconfig/ssl/ /var/netscaler/ssl/ bookmarks /var/vpn/bookmark/ dns /nsconfig/dns/ htmlinjection /nsconfig/htmlinjection/ imports /var/download/ misc /nsconfig/license/ /nsconfig/rc.conf all_plus_misc Includes *all* files and /nsconfig/license/ and /nsconfig/rc.conf.

Parameters

Mode

Specifies the directories and files to be synchronized. Possible values: all, bookmarks, ssl, htmlinjection, imports, misc, dns, all_plus_misc. Default value: all

Example

sync cluster files ssl or sync cluster files all

cluster sync

force cluster sync

Synopsis

force cluster sync

Description

Synchronize the configurations of a cluster node from the CCO. This command must be executed from the NSIP of the node that needs to be synchronized.

Example

force cluster sync

Compression Commands

This group of commands can be used to perform operations on the following entities:

- cmp
- cmp action
- cmp policy
- cmp policylabel
- cmp stats
- cmp global
- cmp parameter

cmp

stat cmp

Synopsis

stat cmp [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display compression statistics.

cmp action

[add | rm | show | rename]

add cmp action

Synopsis

add cmp action <name> <cmpType>

Description

Create a compression action. The action thus created can be associated with the compression policy. The built-in compression actions NOCOMPRESS/COMPRESS/GZIP/DEFLATE are always present on the system. These actions are: NOCOMPRESS action - can be used to define a policy that disables compression for the matching policy.COMPRESS action - can be used to enable compression for a specific policy. This action will do GZIP or DEFLATE, based on the browser. GZIP action - can be used to enable GZIP compression for a specific policy. With this action, GZIP compression will be performed if the browser supports GZIP, other wise compression is disabled. DEFLATE action - can be used to enable DEFLATE compression for a specific policy. With this action, DEFLATE compression will be performed if the browser supports DEFLATE, otherwise compression is disabled.

Parameters

name

The name of the compression action.

cmpType

The type of compression action. Possible values: compress, gzip, deflate, nocompress

deltaType

The type of delta action (if delta type compression action is defined). Possible values: PERURL, PERPOLICY Default value: NS_ACT_CMP_DELTA_TYPE_PERURL

Example

add cmp action nocmp NOCOMPRESS

Top

rm cmp action

Synopsis

rm cmp action <name>

Description

Remove the specified compression action.

Parameters

name

The name of the compression action.

Example

rm cmp action cmp_action_name

Top

show cmp action

Synopsis

show cmp action [<name>]

Description

Display the compression actions defined including the built-in actions.

Parameters

name

The name of the compression action.

Example

Example 1

The following example shows output from the show cmp action command when no custom cmp actions have

```
> show cmp action
      3 Compression actions:
```

1) Name: GZIP Compression Type: gzip
2) Name: NOCOMPRESS Compression Type: nocompress
3) Name: DEFLATE Compression Type: deflate
4) Name: COMPRESS Compression Type: compress
Done

Done
Example 2
The following command creates a compression action:
add cmp action nocmp NOCOMPRESS
The following example shows output from the show cmp action command after the previous command has be
> show cmp action
3 Compression actions:
1) Name: GZIP Compression Type: gzip
2) Name: NOCOMPRESS Compression Type: nocompress
3) Name: DEFLATE Compression Type: deflate
4) Name: COMPRESS Compression Type: compress

1 Compression action:
1) Name: nocmp Compression Type: nocompress
Done

Top

rename cmp action

Synopsis

rename cmp action <name>@ <newName>@

Description

Rename a cmp action.

Parameters

name

The name of the cmp action.

newName

The new name of the cmp action.

Example

rename cmp policy oldname newname

Top

cmp policy

[add | rm | set | unset | show | stat | rename]

add cmp policy

Synopsis

add cmp policy <name> -rule <expression> -resAction <string>

Description

Create a HTTP compression policy.

Parameters

name

The name of the HTTP compression policy to be created.

rule

The rule associated with the HTTP compression policy.

resAction

The compression action that needs to be performed when the rule matches. The string value can be either be a created compression action (user-defined) or one of the following built-in compression actions: NOCOMPRESS action - can be used to define a policy that disables compression for the matching policy.COMPRESS action - can be used to enable compression for a specific policy. This action will do GZIP or DEFLATE, based on the browser. GZIP action - can be used to enable GZIP compression for a specific policy. With this action, GZIP compression will be performed if the browser supports GZIP, other wise compression is disabled. DEFLATE action - can be used to enable DEFLATE compression for a specific policy. With this action, DEFLATE compression will be performed if the browser supports DEFLATE, otherwise compression is disabled.

Example

Example 1:

add cmp policy pdf_cmp -rule "RES.HTTP.HEADER Content-Type CONTAINS application/pdf" -resAction COMP

After creating the above compression policy, you must activate it by binding it globally:
bind cmp global pdf_cmp

The NetScaler system will use the configured pdf_cmp compression policy to perform compression of pdf file

Example 2:

The following command disables compression for all the access from the specific subnet.
add cmp policy local_sub_nocmp -rule "SOURCEIP == 10.1.1.0 -netmask 255.255.255.0" -resAction NOCOMPRE
bind cmp global local_sub_nocmp

Top

rm cmp policy

Synopsis

rm cmp policy <name>

Description

Remove a HTTP compression policy.

Parameters

name

The name of the HTTP compression policy to be removed.

Example

rm cmp policy cmp_policy_name
The "show cmp policy" command shows all currently defined HTTP compression policies.

Top

set cmp policy

Synopsis

set cmp policy <name> [-rule <expression>] [-resAction <string>]

Description

Modify a HTTP compression policy. Use the "show cmp policy" command to view all configured HTTP compression policies.

Parameters

name

The name of the HTTP compression policy to be modified.

rule

The new rule to be associated with the HTTP compression policy.

resAction

The compression action to be associated with the HTTP compression policy.

Example

Example 1:

add cmp policy pdf_cmp -rule "RES.HTTP.HEADER Content-Type CONTAINS application/pdf" -resAction COMP

After creating the above compression policy, you must activate it by binding it globally:
bind cmp global pdf_cmp

The NetScaler system will use the configured pdf_cmp compression policy to perform compression for pdf fil

To disable pdf compression for Internet Explorer, you can change the above compression policy by issuing th

set cmp policy pdf_cmp -rule "RES.HTTP.HEADER Content-Type CONTAINS application/pdf && RES.HTTP.HEA

To view the changed cmp policy, enter the following command:

```
>show cmp policy pdf_cmp
      Name: pdf_cmp   Rule: (RES.HTTP.HEADER Content-Type CONTAINS application/pdf && REQ.HTTP.HEA
      Response action: COMPRESS       Hits: 2
      Bytes In:...609284      Bytes Out:... 443998
      Bandwidth saving...27.13%       Ratio 1.37:1
 Done
```

Top

unset cmp policy

Synopsis

unset cmp policy <name> [-rule] [-resAction]

Description

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

Top

show cmp policy

Synopsis

show cmp policy [<name>] show cmp policy stats - alias for 'stat cmp policy'

Description

Display the configured HTTP compression policies.

Parameters

name

The name of the HTTP compression policy whose details are to be displayed.

Example

```
> show cmp policy
        4 Compression policies:
1)      Name: ns_cmp_content_type       Rule: ns_content_type
        Response action: COMPRESS       Hits: 1
        Bytes In:...4325        Bytes Out:... 1530
        Bandwidth saving...64.62%       Ratio 2.83:1
2)      Name: ns_cmp_msapp      Rule: (ns_msie && ns_msword || (ns_msexcel || ns_msppt))
        Response action: COMPRESS       Hits: 7
        Bytes In:...796160      Bytes Out:... 197730
        Bandwidth saving...75.16%       Ratio 4.03:1
3)      Name: ns_cmp_mscss      Rule: (ns_msie && ns_css)
        Response action: COMPRESS       Hits: 0
4)      Name: ns_nocmp_mozilla_47       Rule: (ns_mozilla_47 && ns_css)
        Response action: NOCOMPRESS     Hits: 0
 Done

You can also view an individual cmp policy by giving the cmp policy name as an argument:
> show cmp policy ns_cmp_msapp
        Name: ns_cmp_msapp      Rule: (ns_msie && ns_msword || (ns_msexcel || ns_msppt))
        Response action: COMPRESS       Hits: 7
        Bytes In:...796160      Bytes Out:... 197730
        Bandwidth saving...75.16%       Ratio 4.03:1
 Done
```

Top

stat cmp policy

Synopsis

stat cmp policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display cmp policy statistics.

Parameters

name

The name of the compress policy for which statistics will be displayed. If not given statistics are shown for all compress policies.

Example

stat cmp policy

Top

rename cmp policy

Synopsis

rename cmp policy <name>@ <newName>@

Description

Rename a cmp policy.

Parameters

name

The name of the cmp policy.

newName

The new name of the cmp policy.

Example

rename cmp policy oldname newname

Top

cmp policylabel

[add | rm | bind | unbind | show | stat | rename]

add cmp policylabel

Synopsis

add cmp policylabel <labelName> -type (REQ | RES)

Description

Create a HTTP compression policy label.

Parameters

labelName

The name of the HTTP compression policy label to be created.

type

Specifies when policies bound to this policy label will be evaluated. Possible values: REQ, RES

Example

add cmp policylabel cmp_pol_label -type REQ

Top

rm cmp policylabel

Synopsis

rm cmp policylabel <labelName>

Description

Remove a HTTP compression policy label.

Parameters

labelName

The name of the HTTP compression policy label to be removed.

Example

rm cmp policylabel cmp_pol_label

Top

bind cmp policylabel

Synopsis

bind cmp policylabel <labelName> -policyName <string> -priority <positive_integer> [-gotoPriorityExpression <expression>] [-invoke (<labelType> <labelName>)]

Description

Bind an ADVANCED HTTP compression policy to a HTTP compression policy label.

Parameters

labelName

Name of the HTTP compression policy label.

policyName

The HTTP compression policy name.

Example

bind cmp policylabel cmp_pol_label -policyName cmp_pol -priority 1

Top

unbind cmp policylabel

Synopsis

unbind cmp policylabel <labelName> <policyName> [-priority <positive_integer>]

Description

Unbind an ADVANCED HTTP compression policy from a HTTP compression policy label.

Parameters

labelName

Name of the HTTP compression policy label.

policyName

The HTTP compression policy name.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind cmp policylabel cmp_pol_label cmp_pol

Top

show cmp policylabel

Synopsis

show cmp policylabel [<labelName>]

Description

Display all HTTP compression policy labels or all policies bound to a HTTP compression policy label.

Parameters

labelName

The name of the HTTP compression policy label.

Example

i) show cmp policylabel cmp_pol_label
ii) show cmp policylabel

Top

stat cmp policylabel

Synopsis

stat cmp policylabel [<labelName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of cmp policylabel(s).

Parameters

labelName

The name of the compress policy label for which statistics will be displayed. If not given statistics are shown for all compress policylabels.

Top

rename cmp policylabel

Synopsis

rename cmp policylabel <labelName>@ <newName>@

Description

Rename a cmp policy label.

Parameters

labelName

The name of the cmp policylabel.

newName

The new name of the cmp policylabel.

Example

rename cmp policylabel oldname newname

Top

cmp stats

show cmp stats

Synopsis

show cmp stats - alias for 'stat cmp'

Description

show cmp stats is an alias for stat cmp

cmp global

[bind | unbind | show]

bind cmp global

Synopsis

bind cmp global <policyName> [-priority <positive_integer>] [-state (ENABLED | DISABLED)] [-gotoPriorityExpression <expression>] [-type <type>] [-invoke (<labelType> <labelName>)]

Description

Activate the compression policy globally. Note that for compression feature to work, a compression license is required. To activate the compression feature, use the "enable ns feature cmp" command. When you enable the compression feature, all of the built-in compression policies are bound globally.

Parameters

policyName

The name of the HTTP compression policy.

Example

add cmp policy pdf_cmp -rule "RES.HTTP.HEADER Content-Type CONTAINS application/pdf" -resAction COMP

After creating the above compression policy, you must activate it by binding it globally:
bind cmp global pdf_cmp

After binding pdf_cmp compression policy globally, the policy gets activated and the NetScaler system will p

To view the globally active compression policies, enter the following command:

```
> show cmp global
      5 Globally Active Compression Policies:
1)    Policy Name: ns_cmp_content_type       Priority: 0
2)    Policy Name: ns_nocmp_mozilla_47       Priority: 0
3)    Policy Name: ns_cmp_mscss      Priority: 0
4)    Policy Name: ns_cmp_msapp      Priority: 0
5)    Policy Name: pdf_cmp    Priority: 0
 Done
```

Top

unbind cmp global

Synopsis

unbind cmp global <policyName> [-type <type> [-priority <positive_integer>]]

Description

Deactivate a globally bound HTTP compression policy.

Parameters

policyName

The name of the globally bound HTTP compression policy to be deactivated.

Example

To view the globally active compression policies, enter the following command:

```
> show cmp global
        5 Globally Active Compression Policies:
1)      Policy Name: ns_cmp_content_type        Priority: 0
2)      Policy Name: ns_nocmp_mozilla_47        Priority: 0
3)      Policy Name: ns_cmp_mscss       Priority: 0
4)      Policy Name: ns_cmp_msapp       Priority: 0
5)      Policy Name: pdf_cmp    Priority: 0
 Done
```

To deactivate this globally active compression policy on the NetScaler system, enter the following command

```
unbind cmp global pdf_cmp
```

Top

show cmp global

Synopsis

show cmp global [-type <type>]

Description

Display the globally bound HTTP compression policies.

Parameters

type

The bindpoint to which the policy is bound. Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

Example

```
> show cmp global
        4 Globally Active Compression Policies:
1)      Policy Name: ns_cmp_content_type        Priority: 0
2)      Policy Name: ns_nocmp_mozilla_47        Priority: 0
3)      Policy Name: ns_cmp_mscss       Priority: 0
4)      Policy Name: ns_cmp_msapp       Priority: 0
 Done
```

Top

cmp parameter

[set | unset | show]

set cmp parameter

Synopsis

set cmp parameter [-cmpLevel <cmpLevel>] [-quantumSize <positive_integer>] [-serverCmp (ON | OFF)] [-minResSize <positive_integer>] [-cmpBypassPct <positive_integer>] [-cmpOnPush (ENABLED | DISABLED)] [-policyType (CLASSIC | ADVANCED)] [-addVaryHeader (ENABLED | DISABLED)] [-externalCache (YES | NO)]

Description

Configurable parameters for compression.

Parameters

cmpLevel

Compression level. Possible values: optimal, bestspeed, bestcompression Default value: NSCMPLVL_OPTIMAL

quantumSize

Minimum amount of data to compress as one unit. Default value: 57344 Minimum value: 8 Maximum value: 63488

serverCmp

Compression at back-end server. Possible values: ON, OFF Default value: ON

heurExpiry

Heuristic basefile expiry. Possible values: ON, OFF Default value: OFF

heurExpiryThres

Threshold compression ratio for heuristic basefile expiry, multiplied by 100. For example, to set the threshold ratio to 1.25, specify 125. Default value: 100 Minimum value: 1 Maximum value: 1000

heurExpiryHistWt

For heuristic basefile expiry, weightage to be given to historical delta compression ratio, specified as percentage. For example, to give 25% weightage to historical ratio (and

therefore 75% weightage to the ratio for current delta compression transaction), specify 25. Default value: 50 Minimum value: 1 Maximum value: 100

minResSize

Size of the smallest HTTP response that will be compressed.

cmpBypassPct

CPU usage (%) at which NetScaler should start progressively bypassing compression on HTTP requests. Default value: 100 Maximum value: 100

cmpOnPush

Enable/disable compression on PUSH packet Possible values: ENABLED, DISABLED Default value: DISABLED

policyType

The type of the HTTP compression global policy bindings to be used for virtual servers that have no HTTP compression policies bound. Possible values: CLASSIC, ADVANCED Default value: NS_EXPR_TYPE_CLASSIC

addVaryHeader

Enable/disable vary header insertion during compression for HTTP/1.1 client. Possible values: ENABLED, DISABLED Default value: DISABLED

externalCache

Enable insertion of Cache-Control: private response directive to indicate response message is intended for a single user and must not be cached by a shared or proxy cache. Possible values: YES, NO Default value: NO

Example

set cmp param -cmpLevel bestspeed -quantumSize 20480

Top

unset cmp parameter

Synopsis

unset cmp parameter [-cmpLevel] [-quantumSize] [-serverCmp] [-minResSize] [-cmpBypassPct] [-cmpOnPush] [-policyType] [-addVaryHeader] [-externalCache]

Description

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

Top

show cmp parameter

Synopsis

show cmp parameter

Description

Display configurable parameters for compression.

Top

Cache Redirection Commands

This group of commands can be used to perform operations on the following entities:

- cr policy
- cr vserver

cr policy

[add | rm | set | show]

add cr policy

Synopsis

add cr policy <policyName> -rule <expression>

Description

Add a cache redirection policy. To associate the policy created with a cache redirection virtual server, use the ###bind cr vserver#### command.

Parameters

policyName

The name of the cache redirection policy.

rule

A condition defined by an expression. When the condition is valid, the request is directed to the origin server. Expression logic is: expression names, separated by the logical operators || and &&, and possibly grouped using parenthesis. Note: If the expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes. The following are valid expressions: l ns_ext_cgi||ns_ext_asp 2 ns_non_get && (ns_header_cookie||ns_header_pragma)

Top

rm cr policy

Synopsis

rm cr policy <policyName>

Description

Remove a Cache Redirection policy. You can delete a user-defined cache redirection policy that is not bound to a cache redirection virtual server. If the policy is bound to a virtual server, you must first unbind the policy, and then remove it from the system.

Parameters

policyName

The name of the cache policy to be removed. You cannot remove a positive cacheability policy/content group if it has been configured as the target of a dynamic invalidation policy. In this case, to remove the policy, you must use the following procedure, which removes the dynamic invalidation policy and the action associated with the dynamic invalidation policy: a. Enter the ###show cache action### command at the system prompt. This will display all cache actions. b. Identify the action in which the contentGroupPolicy attribute matches the policy you want to remove. Enter the ###show cache policy### command at the system prompt. c. Identify the policies that the action you chose in step (b) is associated with. d. Remove the policies you identified in step (c). Enter the ###rm cache policy### command. e. Remove the action you identified in step (b). Enter the ###rm cache action### command.

Top

set cr policy

Synopsis

set cr policy <policyName> -rule <expression>

Description

Changes the rule for a cache redirection policy.

Parameters

policyName

The name of the cache redirection policy.

rule

The condition defined by an expression. When the condition is valid, the request is directed to the origin server. Expression logic is: expression names, separated by the logical operators || and &&, and possibly grouped using parenthesis. Note: If the expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes. The following are valid expressions: l ns_ext_cgi||ns_ext_asp 2 ns_non_get && (ns_header_cookie||ns_header_pragma)

Top

show cr policy

Synopsis

show cr policy [<policyName>]

Description

Display all existing cache redirection policies.

Parameters

policyName

The name of the cache redirection policy.

Top

cr vserver

[add | rm | set | unset | bind | unbind | enable | disable | show | stat | rename]

add cr vserver

Synopsis

add cr vserver <name> <serviceType> [<IPAddress> <port> [-range <positive_integer>]] [-cacheType <cacheType>] [-redirect <redirect>] [-onPolicyMatch (CACHE | ORIGIN)] [-redirectURL <URL>] [-cltTimeout <secs>] [-precedence (RULE | URL)] [-arp (ON | OFF)] [-map (ON | OFF)] [-format (ON | OFF)] [-via (ON | OFF)] [-dnsVserverName <string>] [-destinationVServer <string>] [-domain <string>] [-soPersistenceTimeOut <positive_integer>] [-soThreshold <positive_integer>] [-reuse (ON | OFF)] [-state (ENABLED | DISABLED)] [-downStateFlush (ENABLED | DISABLED)] [-backupVServer <string>] [-disablePrimaryOnDown (ENABLED | DISABLED)] [-l2Conn (ON | OFF)] [-Listenpolicy <expression> [-Listenpriority <positive_integer>]] [-tcpProfileName <string>] [-httpProfileName <string>] [-comment <string>] [-srcIPExpr <expression>] [-originUSIP (ON | OFF)] [-usePortRange (ON | OFF)] [-appflowLog (ENABLED | DISABLED)] [-netProfile <string>] [-icmpVsrResponse (PASSIVE | ACTIVE)]

Description

Add a cache redirection virtual server.

Parameters

name

Name of the cache redirection virtual server.

serviceType

The type of service handled by the virtual server. Note: Use service type HTTP to configure content switching on this virtual server. Possible values: HTTP, SSL, NNTP

IPAddress

The IP address of the cache redirection virtual server. 1. To specify a specific virtual server address, type its numeric value. 2. To specify a wildcard virtual server address, type an asterisk (*).

cacheType

The supported cache server type. Note: For this command to work, you must select one of the cache types. Possible values: TRANSPARENT, REVERSE, FORWARD Default value: CRD_TRANSPARENT

redirect

The redirect policy. The valid redirect policies are: l. CACHE - Directs all requests to the cache. 2. POLICY - Applies the cache redirection policy to determine whether the request should be directed to the cache or to the origin. This is the default setting. 3. ORIGIN - Directs all requests to the origin server. Possible values: CACHE, POLICY, ORIGIN Default value: CRD_POLICY

onPolicyMatch

Decide where to redirect the requests if the cache redirection policy is hit. The valid options are: 1. CACHE - Directs all the requests to the cache if cache redirection policy is hit. 2. ORIGIN - Directs all requests to the origing server if the cache redirection policy is hit. Note: For this option to work, you must select the cache redirection type as POLICY. Possible values: CACHE, ORIGIN Default value: CRD_ORIGIN

redirectURL

The URL where traffic is redirected if the virtual server in the system becomes unavailable. You can enter up to 127 characters as the URL argument.WARNING!Make sure that the domain you specify in the URL does not match the domain specified in the -d domainName argument of the add cs policy CLI command. If the same domain is specified in both arguments, the request will be continuously redirected to the same unavailable virtual server in the system - then the user may not get the requested content.

cltTimeout

The timeout value in seconds for idle client connection Maximum value: 31536000

precedence

You can use this argument only when configuring content switching on the specified virtual server. This argument applies only if the URL- and RULE-based policies have both been configured on the same virtual server. This argument specifies the type of policy (URL or RULE) that takes precedence on the content switching virtual server. The default setting is RULE. l URL - In this case, the incoming request is matched against the URL-based policies before it is matched against the rule-based policies. l RULE - In this case, the incoming request is matched against the rule-based policies before it is matched against the URL-based policies. For all URL-based policies, the precedence hierarchy is: 1. Domain and exact URL 2. Domain, prefix and suffix 3. Domain and suffix 4. Domain and prefix 5. Domain only 6. Exact URL 7. Prefix and suffix 8. Suffix only 9. Prefix only 10. Default Possible values: RULE, URL Default value: CS_PRIORITY_RULE

via

Determines whether the system will insert a Via: header in the HTTP requests. Possible values: ON, OFF Default value: ON

cacheVserver

The name of the default target cache virtual server to which requests are redirected.

dnsVserverName

The name of the DNS virtual server used to resolve domain names arriving at the forward proxy virtual server. Note: This parameter applies only to forward proxy virtual servers, not reverse and transparent.

destinationVServer

The destination virtual server for a transparent or forward proxy cache redirection virtual server. All requests to the transparent or forward proxy cache redirection virtual server are directed to this destination virtual server.

domain

The default domain for reverse proxies. Domains are configured in the system so that they direct an incoming request from a particular configured source domain to a particular configured target domain. There may be several configured pairs of source and target domains. You can select one pair to be the default. Then, if a source domain is not present in the host header or URL of an incoming request, the request will be sent to the target domain of the selected default pair.

reuse

Specifies whether TCP connections to cache or origin servers will be reused across client connections. Note: You should include this argument only if the service type argument is set to HTTP. The default setting is ON. If you set this argument to OFF and: -redirect is set to CACHE: TCP connections to the cache servers are not reused. -redirect is set to ORIGIN: TCP connections to the origin servers are not reused. -redirect is set to POLICY: TCP connections to the origin servers are not reused. If you set this argument to ON, connections are reused to both origin and cache servers. Possible values: ON, OFF Default value: ON

state

The initial state (enabled or disabled) of the cache redirection virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

downStateFlush

Perform delayed cleanup of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

backupVServer

The Backup Virtual Server.

disablePrimaryOnDown

When this argument is enabled, traffic will continue reaching backup vservers even after primary comes UP from DOWN state. Possible values: ENABLED, DISABLED Default value: DISABLED

l2Conn

Use L2 Parameters to identify a connection Possible values: ON, OFF

Listenpolicy

Use this parameter to specify the listen policy for CR Vserver. The string can be either an existing expression name (configured using add policy expression command) or else it can be an in-line expression with a maximum of 1499 characters. Default value: "none"

Listenpriority

Use this parameter to specify the priority for listen policy of CR Vserver. Default value: 101 Maximum value: 100

tcpProfileName

The name of the TCP profile.

httpProfileName

Name of the HTTP profile.

comment

Comments associated with this virtual server.

srcIPExpr

Use this parameter to specify the expression used to extract the Source IP to be used from the requests coming from the Cache. The string can be either an existing expression name (configured using add policy expression command) or else it can be an in-line expression with a maximum of 1499 characters.

originUSIP

For requests going to the Origin specify whether to use the SourceIP or not. Possible values: ON, OFF Default value: OFF

usePortRange

Select the source port for requests going to the origin. Possible values: ON, OFF Default value: OFF

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

The name of the network profile.

icmpVsrResponse

Can be active or passive Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

Top

rm cr vserver

Synopsis

rm cr vserver <name>@ ...

Description

Remove a virtual server.

Parameters

name

The name of the virtual server to be removed.

Example

rm vserver cr_vip

Top

set cr vserver

Synopsis

set cr vserver <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-redirect <redirect>] [-onPolicyMatch (CACHE | ORIGIN)] [-precedence (RULE | URL)] [-arp (ON | OFF)] [-via (ON | OFF)] [-dnsVserverName <string>] [-destinationVServer <string>] [-domain <string>] [-reuse (ON | OFF)] [-backupVServer <string>] [-disablePrimaryOnDown (ENABLED | DISABLED)] [-redirectURL <URL>] [-cltTimeout <secs>] [-downStateFlush (ENABLED | DISABLED)] [-l2Conn (ON | OFF)] [-Listenpolicy <expression>] [-Listenpriority <positive_integer>] [-tcpProfileName <string>] [-httpProfileName <string>] [-netProfile <string>] [-comment <string>] [-srcIPExpr <expression>] [-originUSIP (ON | OFF)] [-usePortRange (ON | OFF)] [-appflowLog (ENABLED | DISABLED)] [-icmpVsrResponse (PASSIVE | ACTIVE)]

Description

Change the attributes of a configured cache redirection vserver.

Parameters

name

Name of the cache redirection virtual server.

IPAddress

The new IP address of the virtual server.

redirect

The redirect policy. Possible values: CACHE, POLICY, ORIGIN Default value: CRD_POLICY

onPolicyMatch

Decide where to redirect the requests if the cache redirection policy is hit. The valid options are: 1. CACHE - Directs all the requests to the cache if cache redirection policy is hit. 2. ORIGIN - Directs all requests to the origing server if the cache redirection policy is hit. Note: For this option to work, you must select the cache redirection type as POLICY. Possible values: CACHE, ORIGIN Default value: CRD_ORIGIN

precedence

The type of policy (URL or RULE) that takes precedence on the content redirection virtual server. Possible values: RULE, URL Default value: CS_PRIORITY_RULE

via

The state of the system in inserting a Via: header in the HTTP requests. Possible values: ON, OFF Default value: ON

cacheVserver

The name of the default target cache virtual server to which requests are to be redirected.

dnsVserverName

The name of the DNS virtual server to be used to resolve domain names arriving at the forward proxy virtual server.

destinationVServer

The destination virtual server for the transparent or forward proxy cache redirection virtual server.

domain

The default domain for reverse proxies.

reuse

The state of reuse of TCP connections to the cache or origin servers across client connections. Possible values: ON, OFF Default value: ON

backupVServer

The Backup Virtual Server.

disablePrimaryOnDown

When this argument is enabled, traffic will continue reaching backup vservers even after primary comes UP from DOWN state. Possible values: ENABLED, DISABLED Default value: DISABLED

redirectURL

The redirect URL.

cltTimeout

The client timeout value in seconds. Maximum value: 31536000

downStateFlush

Perform delayed cleanup of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

l2Conn

Use L2 Parameters to identify a connection Possible values: ON, OFF

Listenpolicy

Use this parameter to specify the listen policy for CR Vserver. The string can be either an existing expression name (configured using add policy expression command) or else it can be an in-line expression with a maximum of 1499 characters. Default value: "none"

Listenpriority

Use this parameter to specify the priority for listen policy of CR Vserver. Default value: 101 Maximum value: 100

tcpProfileName

The name of the TCP profile.

httpProfileName

Name of the HTTP profile.

netProfile

The name of the network profile.

comment

Comments associated with this virtual server.

srcIPExpr

Use this parameter to specify the expression used to extract the Source IP to be used from the requests coming from the Cache. The string can be either an existing expression name (configured using add policy expression command) or else it can be an in-line expression with a maximum of 1499 characters.

originUSIP

For requests going to the Origin specify whether to use the SourceIP or not. Possible values: ON, OFF Default value: OFF

usePortRange

Select the source port for requests going to the origin. Possible values: ON, OFF Default value: OFF

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

icmpVsrResponse

Can be active or passive Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

Top

unset cr vserver

Synopsis

unset cr vserver <name> [-dnsVserverName] [-destinationVServer] [-domain] [-backupVServer] [-cltTimeout] [-redirectURL] [-l2Conn] [-originUSIP] [-usePortRange] [-srcIPExpr] [-tcpProfileName] [-httpProfileName] [-appflowLog] [-netProfile] [-icmpVsrResponse] [-redirect] [-onPolicyMatch] [-precedence] [-arp] [-via] [-reuse] [-disablePrimaryOnDown] [-downStateFlush] [-Listenpolicy] [-Listenpriority] [-comment]

Description

Unset the attributes of the configured cache redirection virtual server. To set the cache redirection virtual server attributes, you can use either the ###add cr vserver### or the ###set cr vserver### command..Refer to the set cr vserver command for meanings of the arguments.

Top

bind cr vserver

Synopsis

bind cr vserver <name> [-lbvserver <string> | (-policyName <string> [-priority <positive_integer>]) | <targetVserver>]

Description

For the system's cache redirection feature, this command binds the cache redirection policy to the cache redirection virtual server.

Parameters

name

The name of the cache redirection virtual server to which the cache redirection policy will be bound.

lbvserver

The virtual server name (created with the add lb vserver command) to which content will be switched.

policyName

The name of the cache redirection policy. This policy must be of the type map or cache redirection policy (created using the ###add policy map### or ###add cr policy### commands).

Top

unbind cr vserver

Synopsis

unbind cr vserver <name> [-policyName <string> | -lbvserver <string>]

Description

This command unbinds a cache redirection policy from a cache redirection virtual server.

Parameters

name

The name of the cache redirection virtual server from which to unbind the policy.

policyName

The name of the policy (previously created using the ###add cr policy### or ###add policy map### command).

lbvserver

The virtual server name (created with the add lb vserver command) to which content will be switched. Default value: "default_lb"

Top

enable cr vserver

Synopsis

enable cr vserver <name>@

Description

Enable a virtual server. Note: Virtual servers, when added, are enabled by default.

Parameters

name

The name of the virtual server to be enabled.

Example

enable vserver cr_vip

Top

disable cr vserver

Synopsis

disable cr vserver <name>@

Description

Disables a virtual server (takes it out of service).

Parameters

name

The name of the virtual server to be disabled. Notes: 1. The system still responds to ARP and/or ping requests for the IP address of this virtual server. 2. Because the virtual server is still configured in the system, you can enable the virtual server using the ###enable vserver### command.

Example

disable vserver cr_vip

Top

show cr vserver

Synopsis

show cr vserver [<name>]

Description

Display a specified cache redirection virtual server, or all configured cache redirection virtual servers.

Parameters

name

The name of the cache redirection virtual server.

Top

stat cr vserver

Synopsis

stat cr vserver [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display cache redirection vserver statistics.

Parameters

name

The name of the vserver for which statistics will be displayed. If not given statistics are shown for all cr vservers.

Top

rename cr vserver

Synopsis

rename cr vserver <name>@ <newName>@

Description

Rename a cache redirection virtual server.

Parameters

name

The name of the content switching virtual server.

newName

The new name of the virtual server.

Example

rename cr vserver vscr1 vscrnew

Top

Content Switching Commands

This group of commands can be used to perform operations on the following entities:

- cs policy
- cs policylabel
- cs vserver
- cs parameter
- cs action

cs policy

[add | rm | set | unset | show]

add cs policy

Synopsis

add cs policy <policyName> [-url <string> | -rule <expression> | -action <string>] [-domain <string>]

Description

Add a content switching policy. The policy created can be associated with a content switching virtual server using the bind cs vserver CLI command

Parameters

policyName

The name of the new content switching policy.

url

The URL, with wildcards. Specify the string value in this format: // [[prefix] [*]] [.suffix]

rule

The condition for applying this policy. Expression logic is as follows: - Expression names separated by the logical operators || and &&. - Expression names may be grouped using parenthesis. - If the expression contains blanks (e.g., between an expression name and a logical operator), then the entire argument must be enclosed in double quotes. The following example shows valid expression logic: ns_ext_cgi||ns_ext_asp "ns_non_get && (ns_header_cookie||ns_header_pragma)"

domain

The domain name. The string value can range to 63 characters.

action

Content switching action to be used by the policy.

Example

To match the requests that have URL "/", you would enter the following command:
add cs policy <policyName> -url /
To match with all URLs that start with "/sports/", you would enter the following command:
add cs policy <policyName> -url /sports/*
To match requests with URLs that start with "/sports", you would enter the following command:
add cs policy <policyName> -url /sports*
To match requests with the URL "/sports/tennis/index.html", you would enter the following command:
add cs policy <policyName> -url /sports/tennis/index.html
To match requests that have URLs with the extension "jsp", you would enter the following command:
add cs policy <policyName> -url /*.jsp
To match requests with URLs that start with "/sports/" and the file extension "jsp", you would enter the follo
add cs policy <policyName> -url /sports/*.jsp
To match requests with URLs that contain "sports", you would enter the following commands:
add pol expression sports_url "URL contains sports"
add cs policy <policyName> -rule sports_url
To match requests with URL queries that contain "gold" or cookie headers that contain "gold", you would ente
add pol expression gold_query "URLQUERY contains gold"
add pol expression gold_cookie "Header COOKIE contains gold"
add cs policy <policyName> -rule "(gold_query ||gold_cookie)"
To match requests with the domain name www.domainxyz.com, you enter the following command:
add cs policy <policyName> -domain "www.domainxyz.com"
To match requests with the domain name www.domainxyz.com and URLs with the extension "jsp", you would
add cs policy <policyName> -url /*.jsp -domain "www.domainxyz.com"
To match requests with the domain name www.domainxyz.com and URLs that contain "sports", you would en
add pol expression sports_url "URL contains sports"
add cs policy <policyName> -rule sports_url -domain "www.domainxyz.com"
To match a policy with a rule and provide action:
add cs policy <policyname> -rule "http.req.method.eq(GET)" -action act1

Top

rm cs policy

Synopsis

rm cs policy <policyName>

Description

Remove the specified content switching policy. Note: The policy must be unbound from the content switching virtual server before it is removed.

Parameters

policyName

The name of the content switching policy to be removed.

Top

set cs policy

Synopsis

set cs policy <policyName> [-url <string> | -rule <expression>] [-domain <string>] [-action <string>]

Description

Change a previously configured content switching policy.

Parameters

policyName

Name of the policy.

url

The URL, with wildcards.

rule

The condition for applying this policy.

domain

The domain name.

action

The content switching action name.

Top

unset cs policy

Synopsis

unset cs policy <policyName> [-url] [-rule] [-domain] [-action]

Description

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

Top

show cs policy

Synopsis

show cs policy [<policyName>]

Description

Display all of the content switching policies.

Parameters

policyName

The name of the policy to be displayed. if no name is given then all policies will be displayed.

Top

cs policylabel

[add | rm | bind | unbind | show]

add cs policylabel

Synopsis

add cs policylabel <labelName> <cspolicylabeltype>

Description

Add a content switching policy label.

Parameters

labelName

Name of the content switching policy label.

cspolicylabeltype

The type of the policy label. Possible values: HTTP, TCP, RTSP, SSL, SSL_TCP, UDP, DNS, SIP_UDP, ANY, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER

Example

add cs policylabel trans_http_url HTTP

Top

rm cs policylabel

Synopsis

rm cs policylabel <labelName>

Description

Remove a content switching policy label.

Parameters

labelName

Name of the content switching policy label.

Example

rm cs policylabel trans_http_url

Top

bind cs policylabel

Synopsis

bind cs policylabel <labelName> <policyName> <priority> [-targetVserver <string> | -gotoPriorityExpression <expression> | (-invoke (<labelType> <labelName>))]

Description

Bind the content switching policy to one of the labels.

Parameters

labelName

Name of the content switching policy label.

policyName

Name of the policy to be bound to content switching policy label.

priority

Priority with which the policy is to be bound. Minimum value: 1 Maximum value: 2147483647

targetVserver

The virtual server name (created with the add lb vserver command) to which content will be switched.

gotoPriorityExpression

Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE. o If gotoPriorityExpression is not present or if it is equal to END then the policy bank evaluation ends here o Else if the gotoPriorityExpression is equal to NEXT then the next policy in the priority order is evaluated. t o Else gotoPriorityExpression is evaluated. The result of gotoPriorityExpression (which has to be a number) is processed as follows: - An UNDEF

event is triggered if . gotoPriorityExpression cannot be evaluated . gotoPriorityExpression evaluates to number which is smaller than the maximum priority in the policy bank but is not same as any policy's priority . gotoPriorityExpression evaluates to a priority that is smaller than the current policy's priority - If the gotoPriorityExpression evaluates to the priority of the current policy then the next policy in the priority order is evaluated. - If the gotoPriorityExpression evaluates to the priority of a policy further ahead in the list then that policy will be evaluated next.

invoke

Invoke flag.

Example

i) bind cs policylabel cs_lab pol_cs 2 -targetVserver lb_vs

Top

unbind cs policylabel

Synopsis

unbind cs policylabel <labelName> <policyName>

Description

Unbind entities from content switching label.

Parameters

labelName

Name of the content switching policy label.

policyName

The name of the policy to be unbound.

Example

unbind cs policylabel cs_lab pol_cs

Top

show cs policylabel

Synopsis

show cs policylabel [<labelName>]

Description

Display policy label or policies bound to content switching policylabel.

Parameters

labelName

Name of the content switching policy label.

Example

i) show cs policylabel cs_lab
ii) show cs policylabel

Top

cs vserver

[add | rm | set | unset | bind | unbind | enable | disable | show | stat | rename]

add cs vserver

Synopsis

add cs vserver <name> <serviceType> ((<IPAddress> [-range <positive_integer>]) | (-IPPattern <ippat> -IPMask <ipmask>)) <port> [-state (ENABLED | DISABLED)] [-stateupdate (ENABLED | DISABLED)] [-cacheable (YES | NO)] [-redirectURL <URL>] [-cltTimeout <secs>] [-precedence (RULE | URL)] [-caseSensitive (ON | OFF)] [-soMethod <soMethod>] [-soPersistence (ENABLED | DISABLED)] [-soPersistenceTimeOut <positive_integer>] [-soThreshold <positive_integer>] [-redirectPortRewrite (ENABLED | DISABLED)] [-downStateFlush (ENABLED | DISABLED)] [-backupVServer <string>] [-disablePrimaryOnDown (ENABLED | DISABLED)] [-insertVserverIPPort <insertVserverIPPort> [<vipHeader>]] [-rtspNat (ON | OFF)] [-AuthenticationHost <string>] [-Authentication (ON | OFF)] [-Listenpolicy <expression> [-Listenpriority <positive_integer>]] [-authn401 (ON | OFF)] [-authnVsName <string>] [-push (ENABLED | DISABLED)] [-pushVserver <string>] [-pushLabel <expression>] [-pushMultiClients (YES | NO)] [-tcpProfileName <string>] [-httpProfileName <string>] [-comment <string>] [-mssqlServerVersion <mssqlServerVersion>] [-l2Conn (ON | OFF)] [-mysqlProtocolVersion <positive_integer>] [-mysqlServerVersion <string>] [-mysqlCharacterSet <positive_integer>] [-mysqlServerCapabilities <positive_integer>] [-appflowLog (ENABLED | DISABLED)] [-netProfile <string>] [-icmpVsrResponse (PASSIVE | ACTIVE)]

Description

Add a content switching virtual server.

Parameters

name

The content switching virtual server name.

serviceType

The service type of the virtual server. Possible values: HTTP, SSL, TCP, FTP, RTSP, SSL_TCP, UDP, DNS, SIP_UDP, ANY, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER

IPAddress

The IP address of the virtual server.

IPPattern

The IP Pattern of the virtual server.

range

An IP address range. Default value: 1 Minimum value: 1 Maximum value: 254

port

A port number for the virtual server. Minimum value: 1

state

The initial state, enabled or disabled, of the virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

stateupdate

To enable the state update for a CSW vserver Possible values: ENABLED, DISABLED Default value: DISABLED

cacheable

Use this option to specify whether a virtual server, used for load balancing or content switching, routes requests to the cache redirection virtual server before sending it to the configured servers. Possible values: YES, NO Default value: NO

redirectURL

The URL where traffic is redirected if the virtual server in the system becomes unavailable. You can enter up to 127 characters as the URL argument.WARNING!Make sure that the domain you specify in the URL does not match the domain specified in the -d domainName argument of the add cs policy CLI command. If the same domain is specified in both arguments, the request will be continuously redirected to the same unavailable virtual server in the system - then the user may not get the requested content.

cltTimeout

The timeout value in seconds for idle client connection Default value: VAL_NOT_SET Maximum value: 31536000

precedence

This sets the precedence between RULE-based and URL-based policies on the content switching virtual server. The default precedence is RULE. With the precedence set to RULE, incoming requests are evaluated against the content switching policies created with the -rule argument (using the add cs policy CLI command). If none of the rules match, the URL in the request is evaluated against the content switching policies created with the -url argument (using the add cs policy CLI command). Possible values: RULE, URL Default value: CS_PRIORITY_RULE

caseSensitive

The URL lookup case option on the content switching vserver. If the case sensitivity of a content switching virtual server is set to 'ON', the URLs /a/1.html and /A/1.HTML are treated differently, and can be switched to different targets with appropriate content

switching policies. If the case sensitivity is set to 'OFF', the URLs /a/1.html and /A/1.HTML are treated the same, and are switched to the same target. Possible values: ON, OFF Default value: ON

soMethod

The spillover factor based on which the traffic will be given to the backupvserver once the main virtual server reaches the spillover threshold. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence

The state of the spillover persistence. Possible values: ENABLED, DISABLED Default value: DISABLED

soThreshold

If the spillover method is set to CONNECTION or DYNAMICCONNECTION, this value is treated as the maximum number of connections a lb vserver will handle before spillover takes place. If the spillover method is set to BANDWIDTH, this value is treated as the amount of incoming and outgoing traffic (in Kbps) a vserver will handle before spillover takes place. Minimum value: 1 Maximum value: 4294967287

redirectPortRewrite

Enable port rewrite while performing HTTP redirect. Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush

Perform delayed cleanup of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

backupVServer

The backup virtual server for content switching.

disablePrimaryOnDown

When this argument is enabled, traffic will continue reaching backup vservers even after primary comes UP from DOWN state. Possible values: ENABLED, DISABLED Default value: DISABLED

insertVserverIPPort

The virtual IP and port header insertion option for the vserver. VIPADDR - Header contains the vserver's IP address and port number without any translation. OFF - The virtual IP and port header insertion option is disabled. V6TOV4MAPPING - Header contains the mapped IPv4 address corresponding to the IPv6 address of the vserver and the port number. An IPv6 address can be mapped to a user-specified IPv4 address using the set ns ip6 command. Possible values: OFF, VIPADDR, V6TOV4MAPPING

rtspNat

Use this parameter to enable natting for RTSP data connection. Possible values: ON, OFF Default value: OFF

AuthenticationHost

FQDN of authentication vserver

Authentication

This option toggles on or off the application of authentication of incoming users to the vserver. Possible values: ON, OFF Default value: OFF

Listenpolicy

Use this parameter to specify the listen policy for CS Vserver. The string can be either an existing expression name (configured using add policy expression command) or else it can be an in-line expression with a maximum of 1499 characters. Default value: "none"

Listenpriority

Use this parameter to specify the priority for listen policy of CS Vserver. Default value: 101 Maximum value: 100

authn401

This option toggles on or off the HTTP 401 response based authentication. Possible values: ON, OFF Default value: OFF

authnVsName

Name of authentication vserver

push

Process traffic on bound Push vserver. Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver

The lb vserver of type PUSH/SSL_PUSH to which server pushes the updates received on the client facing non-push lb vserver.

pushLabel

Use this parameter to specify the expression to extract the label in response from server. The string can be either a named expression (configured using add policy expression command) or else it can be an in-line expression with a maximum of 63 characters. Default value: "none"

pushMultiClients

Specify if multiple web 2.0 connections from the same client can connect to this vserver and expect updates. Possible values: YES, NO Default value: NO

tcpProfileName

The name of the TCP profile.

httpProfileName

Name of the HTTP profile.

comment

Comments associated with this virtual server.

mssqlServerVersion

The version of the MSSQL server Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2 Default value: TDS_PROT_2008B

l2Conn

Use L2 Parameters to identify a connection Possible values: ON, OFF

mysqlProtocolVersion

The protocol version returned by the mysql vserver. Default value: 10

mysqlServerVersion

The server version string returned by the mysql vserver. Default value: NSA_MYSQL_SERVER_VER_DEFAULT

mysqlCharacterSet

The character set returned by the mysql vserver. Default value: 8

mysqlServerCapabilities

The server capabilities returned by the mysql vserver. Default value: 41613

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

The name of the network profile.

icmpVsrResponse

Can be active or passive Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

Example

1. You can use precedence when certain client attributes (e.g., browser type) require to be served with diff
If the precedence is configured as URL, the incoming request URL is evaluated against the content switching
2. Precedence can also be used when certain content (such as images) is the same for all clients, but other

Top

rm cs vserver

Synopsis

rm cs vserver <name>@ ...

Description

Remove a virtual server.

Parameters

name

The name of the virtual server to be removed.

Example

rm vserver cs_vip

Top

set cs vserver

Synopsis

set cs vserver <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-IPPattern <ippat>] [-IPMask <ipmask>] [-stateupdate (ENABLED | DISABLED)] [-precedence (RULE | URL)] [-caseSensitive (ON | OFF)] [-backupVServer <string>] [-redirectURL <URL>] [-cacheable (YES | NO)] [-cltTimeout <secs>] [-soMethod <soMethod>] [-soPersistence (ENABLED | DISABLED)] [-soPersistenceTimeOut <positive_integer>] [-soThreshold <positive_integer>] [-redirectPortRewrite (ENABLED | DISABLED)] [-downStateFlush (ENABLED | DISABLED)] [-disablePrimaryOnDown (ENABLED | DISABLED)] [-insertVserverIPPort <insertVserverIPPort> [<vipHeader>]] [-rtspNat (ON | OFF)] [-AuthenticationHost <string>] [-Authentication (ON | OFF)] [-Listenpolicy <expression>] [-Listenpriority <positive_integer>] [-authn401 (ON | OFF)] [-authnVsName <string>] [-push (ENABLED | DISABLED)] [-pushVserver <string>] [-pushLabel <expression>] [-pushMultiClients (YES | NO)] [-tcpProfileName <string>] [-httpProfileName <string>] [-comment <string>] [-l2Conn (ON | OFF)] [-mssqlServerVersion <mssqlServerVersion>] [-mysqlProtocolVersion <positive_integer>] [-mysqlServerVersion <string>] [-mysqlCharacterSet <positive_integer>] [-mysqlServerCapabilities <positive_integer>] [-appflowLog (ENABLED | DISABLED)] [-netProfile <string>] [-icmpVsrResponse (PASSIVE | ACTIVE)]

Description

Change the parameters of a content switching virtual server.

Parameters

name

Identifies the virtual server name (created with the add cs vserver command).

IPAddress

The new IP address of the virtual server.

IPPattern

The IP Pattern of the virtual server.

IPMask

The IP Mask of the virtual server IP Pattern

stateupdate

To enable the state update for a CSW vserver Possible values: ENABLED, DISABLED Default value: DISABLED

precedence

The precedence on the content switching virtual server between rule-based and URL-based policies. The default precedence is set to RULE. If the precedence is configured as RULE, the incoming request is applied against the content switching policies created with the -rule argument. If none of the rules match, then the URL in the request is applied against the content switching policies created with the -url option. For example, this precedence can be used if certain client attributes (such as a specific type of browser) need to be served different content and all other clients can be served from the content distributed among the servers. If the precedence is configured as URL, the incoming request URL is applied against the content switching policies created with the -url option. If none of the policies match, then the request is applied against the content switching policies created with the -rule option. Also, this precedence can be used if some content (such as images) is the same for all clients, but other content (such as text) is different for different clients. In this case, the images will be served to all clients, but the text will be served to specific clients based on specific attributes, such as Accept-Language. Possible values: RULE, URL Default value: CS_PRIORITY_RULE

caseSensitive

The URL lookup case option on the content switching vserver. If case sensitivity of a content switching virtual server is set to 'ON', the URLs /a/1.html and /A/1.HTML are treated differently and may have different targets (set by content switching policies). If case sensitivity is set to 'OFF', the URLs /a/1.html and /A/1.HTML are treated the same, and will be switched to the same target. Possible values: ON, OFF Default value: ON

backupVServer

The backup virtual server for content switching.

redirectURL

The redirect URL for content switching.

cacheable

The option to specify whether a virtual server used for content switching will route requests to the cache redirection virtual server before sending it to the configured servers. Possible values: YES, NO Default value: NO

cltTimeout

Client timeout in seconds. Default value: VAL_NOT_SET Maximum value: 31536000

soMethod

The spillover factor. When traffic on the main virtual server reaches this threshold, additional traffic is sent to the backupvserver. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence

The state of the spillover persistence. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut

The spillover persistency entry timeout. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold

If the spillover method is set to CONNECTION or DYNAMICCONNECTION, this value is treated as the maximum number of connections a lb vserver will handle before spillover takes place. If the spillover method is set to BANDWIDTH, this value is treated as the amount of incoming and outgoing traffic (in Kbps) a vserver will handle before spillover takes place. Minimum value: 1 Maximum value: 4294967287

redirectPortRewrite

SSL redirect port rewrite. Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush

Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

disablePrimaryOnDown

When this argument is enabled, traffic will continue reaching backup vservers even after primary comes UP from DOWN state. Possible values: ENABLED, DISABLED Default value: DISABLED

insertVserverIPPort

The virtual IP and port header insertion option for the vserver. VIPADDR - Header contains the vserver's IP address and port number without any translation. OFF - The virtual IP and port header insertion option is disabled. V6TOV4MAPPING - Header contains the mapped IPv4 address that corresponds to the IPv6 address of the vserver and the port number. An IPv6 address can be mapped to a user-specified IPv4 address using the set ns

ip6 command. Possible values: OFF, VIPADDR, V6TOV4MAPPING

rtspNat

Use this parameter to enable natting for RTSP data connection. Possible values: ON, OFF Default value: OFF

AuthenticationHost

FQDN of authentication vserver

Authentication

This option toggles on or off the application of authentication of incoming users to the vserver. Possible values: ON, OFF Default value: OFF

Listenpolicy

Use this parameter to specify the listen policy for CS Vserver. The string can be either an existing expression name (configured using add policy expression command) or else it can be an in-line expression with a maximum of 1499 characters. Default value: "none"

Listenpriority

Use this parameter to specify the priority for listen policy of CS Vserver. Default value: 101 Maximum value: 100

authn401

This option toggles on or off the HTTP 401 response based authentication. Possible values: ON, OFF Default value: OFF

authnVsName

Name of authentication vserver

push

Process traffic on bound Push vserver. Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver

The lb vserver of type PUSH/SSL_PUSH to which server pushes the updates received on the client facing non-push lb vserver.

pushLabel

Use this parameter to specify the expression to extract the label in response from server. The string can be either a named expression (configured using add policy expression command) or else it can be an in-line expression with a maximum of 63 characters. Default value: "none"

pushMultiClients

Specify if multiple web 2.0 connections from the same client can connect to this vserver and expect updates. Possible values: YES, NO Default value: NO

tcpProfileName

The name of the TCP profile.

httpProfileName

Name of the HTTP profile.

comment

Comments associated with this virtual server.

l2Conn

Use L2 Parameters to identify a connection Possible values: ON, OFF

mssqlServerVersion

The version of the MSSQL server Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2 Default value: TDS_PROT_2008B

mysqlProtocolVersion

The protocol version returned by the mysql vserver. Default value: 10

mysqlServerVersion

The server version string returned by the mysql vserver. Default value: NSA_MYSQL_SERVER_VER_DEFAULT

mysqlCharacterSet

The character set returned by the mysql vserver. Default value: 8

mysqlServerCapabilities

The server capabilities returned by the mysql vserver. Default value: 41613

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

The name of the network profile.

icmpVsrResponse

Can be active or passive Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

Top

unset cs vserver

Synopsis

unset cs vserver <name> [-caseSensitive] [-backupVServer] [-cltTimeout] [-redirectURL] [-AuthenticationHost] [-authnVsName] [-pushVserver] [-pushLabel] [-tcpProfileName] [-httpProfileName] [-l2Conn] [-mysqlProtocolVersion] [-mysqlServerVersion] [-mysqlCharacterSet] [-mysqlServerCapabilities] [-appflowLog] [-netProfile] [-icmpVsrResponse] [-stateupdate] [-precedence] [-cacheable] [-soMethod] [-soPersistence] [-soPersistenceTimeOut] [-soThreshold] [-redirectPortRewrite] [-downStateFlush] [-disablePrimaryOnDown] [-insertVserverIPPort] [-vipHeader] [-rtspNat] [-Authentication] [-Listenpolicy] [-Listenpriority] [-authn401] [-push] [-pushMultiClients] [-comment] [-mssqlServerVersion]

Description

Unset the parameters of a content switching virtual server..Refer to the set cs vserver command for meanings of the arguments.

Top

bind cs vserver

Synopsis

bind cs vserver <name> [-lbvserver <string> | (-policyName <string> [-targetLBVserver <string>] [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-type (REQUEST | RESPONSE)] [-invoke (<labelType> <labelName>)])]

Description

Bind a content switching policy between a content-based virtual server and an address-based virtual server. You can assign multiple policies to the virtual server pair. Do not specify the optional policyName when adding a default policy on the content switching virtual server. When binding policies to the content-based virtual server, GotoPriorityExpression applies only to content switching policies with advance policy expression in the rule part. It also applies to application firewall, tranformation, rewrite and responder policies. Flowtype and invoke apply only to rewrite and responder policies.

Parameters

name

The virtual server name (created with the add cs vserver or add cr vserver command) for which the content switching policy will be set.

lbvserver

The virtual server name (created with the add lb vserver command) to which content will be switched.

policyName

The content switch policy name (created with the add cs policy command).

targetVserver

The virtual server name (created with the add lb vserver command) to which content will be switched.

Example

i) bind cs vserver csw-vip1 -policyname csw-policy1 -priority 13
ii) bind cs vserver csw-vip2 -policyname csw-ape-policy2 -priority 14 -gotoPriorityExpression NEXT
iii) bind cs vserver csw-vip3 -policyname rewrite-policy1 -priority 17 -gotoPriorityExpression 'HTTP.REQ.HE

Top

unbind cs vserver

Synopsis

unbind cs vserver <name> [(-policyName <string> [-type (REQUEST | RESPONSE)]) | -lbvserver <string>] [-priority <positive_integer>]

Description

Remove all content switching policies for the specified content switching virtual server. To remove the default policy, do not specify the optional policy name.

Parameters

name

The virtual server name (created with the add cs vserver or add cr vserver command) for which the content switching policy will be set.

policyName

The content switch policy name (created with the add cs policy command).

lbvserver

The virtual server name (created with the add lb vserver command) to which content will be switched. Default value: "default_lb"

Top

enable cs vserver

Synopsis

enable cs vserver <name>@

Description

Enable a virtual cs server. Note: Virtual servers, when added, are enabled by default.

Parameters

name

The name of the virtual server to be enabled.

Example

enable vserver cs_vip

Top

disable cs vserver

Synopsis

disable cs vserver <name>@

Description

Disable (makes out of service) a virtual cs server.

Parameters

name

The name of the virtual server to be disabled.

Example

disable vserver cs_vip

Top

show cs vserver

Synopsis

show cs vserver [<name>] show cs vserver stats - alias for 'stat cs vserver'

Description

Display the list of content switching virtual servers configured in the system. To show the information for a particular virtual server and the content policies bound to that virtual server, enter the name of the content switching virtual server.

Parameters

name

The name of the content switching virtual server.

Top

stat cs vserver

Synopsis

stat cs vserver [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display content switch vserver statistics.

Parameters

name

The name of the vserver for which statistics will be displayed. If not given statistics are shown for all cs vservers.

Top

rename cs vserver

Synopsis

rename cs vserver <name>@ <newName>@

Description

Rename a content virtual server.

Parameters

name

The name of the content switching virtual server.

newName

The new name of the virtual server.

Example

rename cs vserver cs1 cs2

Top

cs parameter

[set | unset | show]

set cs parameter

Synopsis

set cs parameter [-stateupdate (ENABLED | DISABLED)]

Description

Set a common CS parameter

Parameters

stateupdate

enable/disable state update Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set cs parameter -stateupdate (ENABLED|DISABLED)

Top

unset cs parameter

Synopsis

unset cs parameter -stateupdate

Description

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

Top

show cs parameter

Synopsis

show cs parameter

Description

Show CS parameters

Example

show cs parameter

Top

cs action

[add | rm | set | unset | show | rename]

add cs action

Synopsis

add cs action <name> (-targetLBVserver <string> | -targetVserverExpr <expression>) [-comment <string>]

Description

add cs action <action name > <target lb vserver>.

Parameters

name

Name of the cs action to be added.

targetLBVserver

Name of the Target lb vserver.

targetVserverExpr

String builder expression which when evaluated, gives the vserver name

comment

Comments associated with this cs action.

Example

i) add cs action act1 -targetLBVserver lb1
ii) add csaction act2 -targetVserverExpr '"lb" + CLIENT.IP.DST.GET1'
iii) add csaction act3 -targetVserverExpr '"lb1" + client.tcp.dstport'

Top

rm cs action

Synopsis

rm cs action <name>

Description

Remove a configured cs action.

Parameters

name

Name of the cs action.

Example

rm cs action act_before

Top

set cs action

Synopsis

set cs action <name> (-targetLBVserver <string> | -targetVserverExpr <expression>) [-comment <string>]

Description

Modify a cs action.

Parameters

name

Name of the cs action to be added.

targetLBVserver

Name of the Target lb vserver.

targetVserverExpr

String builder expression which when evaluated, gives the vserver name

comment

Comments associated with this cs action.

Example

set cs action act1 -targetLBVserver lb2 -comment 'for url'

Top

unset cs action

Synopsis

unset cs action <name> -comment

Description

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

Top

show cs action

Synopsis

show cs action [<name>]

Description

Display configured cs action(s).

Parameters

name

Name of the CS action.

Example

show cs action

Top

rename cs action

Synopsis

rename cs action <name>@ <newName>@

Description

Rename a cs action.

Parameters

name

The name of the Content Switching action.

newName

The new name of the Content Switching action.

Example

rename cs action oldname newname

Top

DB Commands

[add | rm | set | show]

add db user

Synopsis

add db user <userName> {-password }

Description

Adds a database user. The user name and password that you specify in this command is added to the nsconfig file and used to authenticate the user.

Parameters

userName

The name of the database user. Must be the same as the user name specified in the database.

password

The password for logging on to the database. Must be the same as the password specified in the database.

Example

add db user johndoe -password secret

Top

rm db user

Synopsis

rm db user <userName>

Description

Removes a database user from the NetScaler appliance. Requests from the user are no longer authenticated or routed to the database server.

Parameters

userName

The name of the database user to be removed.

Top

set db user

Synopsis

set db user <userName>

Description

Modifies the parameters for an existing database user. Use this command on the NetScaler if you change user settings in the database.

Parameters

userName

The name of the database user.

password

The database users password. If you use the CLI, you are prompted for this password after specifying the user name.

Example

set db user johndoe
The above command sets the password for johndoe to abcd (Password to be suplied on prompt)

Top

show db user

Synopsis

show db user [<userName>] [-loggedIn]

Description

Displays information about a database user or users. To show all users, do not include a parameter. To display detailed information about one user, specify the users name. You can also show which users are currently logged on.

Parameters

userName

The name of the database user about which to display detailed information. Must be the same as the user name specified in the database.

loggedIn

Display the names of all database users that are logged on to the NetScaler appliance.

Top

DNS Commands

This group of commands can be used to perform operations on the following entities:

- dns
- dns aaaaRec
- dns addRec
- dns txtRec
- dns cnameRec
- dns mxRec
- dns nsRec
- dns ptrRec
- dns srvRec
- dns soaRec
- dns suffix
- dns nameServer
- dns view
- dns policy
- dns zone
- dns key
- dns proxyRecords
- dns records
- dns stats
- dns parameter
- dns policylabel
- dns global
- dns action
- dns nsecRec

dns

stat dns

Synopsis

stat dns [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display DNS statistics.

dns aaaaRec

[add | rm | show]

add dns aaaaRec

Synopsis

add dns aaaaRec <hostName> <IPv6Address> ... [-TTL <secs>]

Description

Add an AAAA address record for the specified domain name.

Parameters

hostName

The domain name for which the address record is added.

IPv6Address

Specify one or more IP addresses for the domain name.

TTL

Specify the time to live, in seconds. Default value: 3600 Maximum value: 2147483647

Example

add dns aaaarec www.mynw.com 3::4:5 -ttl 10

Top

rm dns aaaaRec

Synopsis

rm dns aaaaRec <hostName> [<IPv6Address> ...]

Description

This command removes the specified IPv6 address from the address record for the given domain name. If IPv6 address is not specified, the entire address record for the given domain name is removed.

Parameters

hostName

The host name for which the AAAA record is to be removed.

IPv6Address

Specify one or more IPv6 addresses for the AAAA record to be removed. If all IPv6 records within a domain are removed, the domain name entry is also removed.

Example

rm dns aaaarec www.mynw.com

Top

show dns aaaaRec

Synopsis

show dns aaaaRec [<hostName> | -type <type>] [<IPv6Address>]

Description

Show the IPv6 address0 record for the specified host name. If a host name is not specified, all IPv6 address records are displayed.

Parameters

hostName

The domain name for which the address record is to be displayed.

IPv6Address

Specify one or more IP addresses for the domain name.

type

Specify the address record type. The record type can take 3 values: ADNS - If this is specified, all of the authoritative address records will be displayed. PROXY - If this is specified, all of the proxy address records will be displayed. ALL - If this is specified, all of the address records will be displayed. Possible values: ALL, ADNS, PROXY

Top

dns addRec

[add | rm | show]

add dns addRec

Synopsis

add dns addRec <hostName> <IPAddress> ... [-TTL <secs>]

Description

Add an address record for the specified domain name.

Parameters

hostName

The domain name for which the address record is being added.

IPAddress

One or more IP addresses for the domain name.

TTL

Time to live, in seconds. Default value: 3600 Maximum value: 2147483647

Example

Add dns addrec www.mynw.com 65.200.211.139 -ttl 10

Top

rm dns addRec

Synopsis

rm dns addRec <hostName> [<IPAddress> ...]

Description

Remove the specified ipaddress from the address record for the given domain name. If IP address is not specified, the entire address record for the given domain name is removed.

Parameters

hostName

The host name for which the address record is to be removed.

IPAddress

One or more IP addresses for the address record to be removed. If all address records within a domain are removed, the domain name entry is also removed.

Example

rm dns addrec www.mynw.com

Top

show dns addRec

Synopsis

show dns addRec [<hostName> | -type <type>]

Description

Display the address record for the specified host name. If a host name is not specified, all address records are displayed.

Parameters

hostName

The domain name.

type

The address record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative address records will be displayed. PROXY - If this is specified, all of the proxy address records will be displayed. ALL - If this is specified, all of the address records will be displayed. Possible values: ALL, ADNS, PROXY

Top

dns txtRec

[add | rm | show]

add dns txtRec

Synopsis

add dns txtRec <domain> <string> ... [-TTL <secs>]

Description

Add an TXT record for the specified domain name.

Parameters

domain

The owner domain name of the TXT record.

string

The text of the txt record. Maximum of 6 strings are allowed.

TTL

Time to live, in seconds. Default value: 3600 Maximum value: 2147483647

Example

add dns txtRec spf.m.test. "v=spf1 ip4:1.2.3.0/24 ip4:1.3.4.0/24 ?all"
add dns txtRec comments.m.test. "This is a CHARSTR" "This is another CHARSTR"

Top

rm dns txtRec

Synopsis

rm dns txtRec <domain> (<string> ... | -recordId <positive_integer>@)

Description

Remove the given TXT record for the given domain name.

Parameters

domain

The owner domain name of the TXT record.

string

The text of the txt record. Maximum of 6 strings are allowed.

recordId

The record identifier of the record to be removed. Minimum value: 1 Maximum value: 65535

Example

```
rm dns txtRec spf.m.test. "v=spf1 ip4:1.2.3.0/24 ip4:1.3.4.0/24 ?all"
 rm dns txtRec comments.m.test. "This is a CHARSTR" "This is another CHARSTR"
 rm dns txtRec comments.m.test. -recordId 1411
```

Top

show dns txtRec

Synopsis

show dns txtRec [<domain> | -type <type>]

Description

Display the TXT record for the specified domain. If the domain name is not specified, all of the TXT records are displayed.

Parameters

domain

The owner domain name of the TXT record.

type

The TXT record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative TXT records will be displayed. PROXY - If this is specified, all of the proxy TXT records will be displayed. ALL - If this is specified, all of the TXT records will be displayed. Possible values: ALL, ADNS, PROXY Default value: NSDNS_AUTH_HOST

Example

show dns txtRec spf.m.test.
show dns txtRec

Top

dns cnameRec

[add | rm | show]

add dns cnameRec

Synopsis

add dns cnameRec <aliasName> <canonicalName> [-TTL <secs>]

Description

Add a canonical name record.

Parameters

aliasName

Alias name for the specified domain.

canonicalName

The domain for which cnamerec is created.

TTL

Time to live, in seconds. Default value: 3600 Maximum value: 2147483647

Example

add dns cnameRec www.mynw.org www.mynw.com -ttl 20

Top

rm dns cnameRec

Synopsis

rm dns cnameRec <aliasName>

Description

Remove the canonical name record.

Parameters

aliasName

The name of the alias to be removed.

Example

rm dns cnamerec www.mynw.org

Top

show dns cnameRec

Synopsis

show dns cnameRec [<aliasName> | -type <type>]

Description

Display the cname records. If no alias name is specified, all "cname" records are displayed.

Parameters

aliasName

The alias name. If an alias name is not specified, all "cname" records are displayed.

type

The cname record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative cname records will be displayed. PROXY - If this is specified, all of the proxy cname records will be displayed. ALL - If this is specified, all of the cname records will be displayed. Possible values: ALL, ADNS, PROXY Default value: NSDNS_AUTH_HOST

Example

show dns cnameRec www.mynw.org

Top

dns mxRec

[add | rm | set | unset | show]

add dns mxRec

Synopsis

add dns mxRec <domain> -mx <string> -pref <positive_integer> [-TTL <secs>]

Description

Add the DNS mail exchange (MX) record.

Parameters

domain

The domain for which the added MX record is added.

mx

The MX record name.

pref

The route priority number. Note: A domain name can have multiple mail routes, with a priority number assigned to each. The mail route with the lowest number identifies the server responsible for the domain. Other mail servers listed are used as backups. Maximum value: 65535

TTL

Time to live, in seconds. Default value: 3600 Maximum value: 2147483647

Top

rm dns mxRec

Synopsis

rm dns mxRec <domain> <mx>

Description

Remove the DNS mail exchange record.

Parameters

domain

The domain for the mail exchange record to be removed.

mx

The mail exchange record name.

Top

set dns mxRec

Synopsis

set dns mxRec <domain> -mx <string> [-pref <positive_integer>] [-TTL <secs>]

Description

Set the DNS MX (mail exchange) record parameters.

Parameters

domain

The domain to be associated with the MX record.

mx

The name of the MX record.

pref

The priority number of the domain's mail route. Because one domain name can have multiple mail routes, you must specify a priority number for each domain's route. The mail route with the lowest number identifies the server responsible for the domain. Other mail servers listed are used as backups. Maximum value: 65535

TTL

The time to live, in seconds. Default value: 3600 Maximum value: 2147483647

Top

unset dns mxRec

Synopsis

unset dns mxRec <domain> -mx <string> -TTL

Description

Use this command to remove dns mxRec settings.Refer to the set dns mxRec command for meanings of the arguments.

Top

show dns mxRec

Synopsis

show dns mxRec [<domain> | -type <type>]

Description

Display the mail exchange (MX) record for the specified domain. If a domain name is not specified, all mail exchange records are displayed.

Parameters

domain

The domain name.

type

The MX record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative MX records will be displayed. PROXY - If this is specified, all of the proxy MX records will be displayed. ALL - If this is specified, all of the MX records will be displayed. Possible values: ALL, ADNS, PROXY Default value: NSDNS_AUTH_HOST

Top

dns nsRec

[add | rm | show]

add dns nsRec

Synopsis

add dns nsRec <domain> <nameServer> [-TTL <secs>]

Description

Add the name server record for a given domain name.

Parameters

domain

The domain name for which a name server record is added.

nameServer

The nameserver for the domain.

TTL

Time to live, in seconds. Default value: 3600 Maximum value: 2147483647

Top

rm dns nsRec

Synopsis

rm dns nsRec <domain> <nameServer>

Description

Remove the name server record for a domain.

Parameters

domain

The domain name whose name server record is to be removed.

nameServer

The name server for the domain to be removed.

Top

show dns nsRec

Synopsis

show dns nsRec [<domain> | -type <type>]

Description

Display the name server record for a domain. If no domain name is specified, all of the name server records are displayed.

Parameters

domain

The domain name for the name server record.

type

The name server record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative name server records will be displayed. PROXY - If this is specified, all of the proxy name server records will be displayed. ALL - If this is specified, all of the name server records will be displayed. Possible values: ALL, ADNS, PROXY

Top

dns ptrRec

[add | rm | show]

add dns ptrRec

Synopsis

add dns ptrRec <reverseDomain> <domain> ... [-TTL <secs>]

Description

Add a PTR record for the specified reverse domain name.

Parameters

reverseDomain

Reverse domain name with suffixes, e.g.: in-addr.arpa. or ip6.arpa..

domain

The domain name for which reverse mapping is being done.

TTL

Time to live, in seconds. Default value: 3600 Maximum value: 2147483647

Example

add dns ptrrec 1.1.1.in-addr.arpa. abc.com

Top

rm dns ptrRec

Synopsis

rm dns ptrRec <reverseDomain> [<domain> ...]

Description

Remove a PTR record corresponding to a given reverse domain name and domain name.

Parameters

reverseDomain

The reverse domain name of the PTR record being removed.

domain

The domain name whose reverse mapping is being removed.

Example

rm dns ptrrec 1.1.1.1.in-addr.arpa. ptr.com

Top

show dns ptrRec

Synopsis

show dns ptrRec [<reverseDomain> | -type <type>]

Description

Display the PTR record for the specified reverse domain name and domain name.

Parameters

reverseDomain

The reverse domain name of the PTR record being displayed.

type

PTR record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative ptr records will be displayed. PROXY - If this is specified, all of the proxy ptr records will be displayed. ALL - If this is specified, all of the ptr records will be displayed. Possible values: ALL, ADNS, PROXY

Top

dns srvRec

[add | rm | set | unset | show]

add dns srvRec

Synopsis

add dns srvRec <domain> <target> -priority <positive_integer> -weight <positive_integer> -port <positive_integer> [-TTL <secs>]

Description

Add an SRV record for the specified domain name.

Parameters

domain

The domain name that is offering the services. The domain name includes the service offered and transport layer protocol, e.g.: _ftp._tcp.abc.com.

target

The target host that is hosting the specified service.

priority

The target host priority. This helps in server selection by the client. Maximum value: 65535

weight

Weight for the target host. This helps in server selection by the client in case of same priority Maximum value: 65535

port

Port on which the target host is listening for client requests. Maximum value: 65535

TTL

The time to live, measured in seconds. Default value: 3600 Maximum value: 2147483647

Top

rm dns srvRec

Synopsis

rm dns srvRec <domain> <target> ...

Description

Remove the SRV record for a given domain name and target.

Parameters

domain

The domain name of the SRV record to be removed.

target

The target host that is hosting the service to be removed.

Top

set dns srvRec

Synopsis

set dns srvRec <domain> <target> [-priority <positive_integer>] [-weight <positive_integer>] [-port <positive_integer>] [-TTL <secs>]

Description

Set the SRV record attributes.

Parameters

domain

The domain name for which the service is configured.

target

The target host that is hosting the service whose attributes are to be changed

priority

Priority of the target host. This helps in server selection by the client. Maximum value: 65535

weight

Weight for the target host. This helps in server selection by the client in case of same priority Maximum value: 65535

port

Port on which the target host is listening for client requests. Maximum value: 65535

TTL

The time to live, measured in seconds. Default value: 3600 Maximum value: 2147483647

Top

unset dns srvRec

Synopsis

unset dns srvRec <domain> <target> -TTL

Description

Use this command to remove dns srvRec settings.Refer to the set dns srvRec command for meanings of the arguments.

Top

show dns srvRec

Synopsis

show dns srvRec [(<domain> [<target>]) | -type <type>]

Description

Display the SRV record for the specified domain. If the domain name is not specified, all of the SRV records are displayed.

Parameters

domain

The domain name for which the SRV record will be displayed.

target

The target host that is hosting the service whose attributes are to be displayed

type

SRV record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative SRV records will be displayed. PROXY - If this is specified, all of the proxy SRV records will be displayed. ALL - If this is specified, all of the SRV records will be displayed. Possible values: ALL, ADNS, PROXY

Top

dns soaRec

[add | rm | set | unset | show]

add dns soaRec

Synopsis

add dns soaRec <domain> -originServer <string> -contact <string> [-serial <positive_integer>] [-refresh <secs>] [-retry <secs>] [-expire <secs>] [-minimum <secs>] [-TTL <secs>]

Description

Add the Start of Authority (SOA) record.

Parameters

domain

The domain name for which the SOA record is added.

originServer

The name of the origin server for the given domain.

contact

The contact person for this ADNS. Typically this is an email address for which the at sign (@) has been replaced by a period (.).

serial

The secondary server uses this parameter to determine if it requires a zone transfer from the primary server. If the secondary server's number is lower than the primary's, the secondary server knows that its records are out of date. This parameter is not used by a primary server. Default value: 100 Maximum value: 4294967294

refresh

The number of seconds between a successful serial number check on the primary server's zone, and the next attempt. It is usually 2-24 hours. This value is not used by a primary server. Default value: 3600 Maximum value: 4294967294

retry

When a refresh attempt fails, a server will retry after the specified number of seconds. This parameter is not used by a primary server. Default value: 3 Maximum value: 4294967294

expire

Measured in seconds. If the refresh and retry attempts fail after the specified number of seconds, the server will stop serving the zone. The typical value is 1 week. This parameter is not used by a primary server. Default value: 3600 Maximum value: 4294967294

minimum

The default TTL for every record in the zone. You can override this value for a particular record. Typical values range from eight hours to four days. This value is often set at ten minutes or less when changes are being made to a zone. Default value: 5 Maximum value: 2147483647

TTL

The time to live, in seconds. Default value: 3600 Maximum value: 2147483647

Top

rm dns soaRec

Synopsis

rm dns soaRec <domain>

Description

Remove the Start of Authority (SOA) record for a given domain name.

Parameters

domain

The domain name for the SOA record to be removed.

Top

set dns soaRec

Synopsis

set dns soaRec <domain> [-originServer <string>] [-contact <string>] [-serial <positive_integer>] [-refresh <secs>] [-retry <secs>] [-expire <secs>] [-minimum <secs>] [-TTL <secs>]

Description

Set the DNS Start Of Authority (SOA) record attributes.

Parameters

domain

The domain name for which the SOA record attributes are set.

originServer

The origin server name for the given domain.

contact

The contact person for this ADNS. Typically it is the email address, with the at sign (@) replaced by a period (.).

serial

The secondary server number. This number is used by a secondary server to determine if it requires a zone transfer from the primary server. If the secondary server's number is lower than the primary's, the secondary server determines that its records are out of date. This parameter is not used by a primary server. Default value: 100 Minimum value: 1 Maximum value: 4294967294

refresh

The refresh time in seconds. Refresh determines the number of seconds between a successful check on the serial number on the zone of the primary, and the next attempt (usually 2-24 hours). This parameter is used by a primary server. Default value: 3600 Maximum value: 4294967294

retry

The retry time in seconds. If a refresh attempt fails, a server will retry after the specified number of seconds. Not used by a primary server. Default value: 3 Maximum value: 4294967294

expire

The expire time in seconds. If the refresh and retry attempts fail after the specified number of seconds, the server will stop serving the zone. The typical value is 1 week. Not used by a primary server. Default value: 3600 Maximum value: 4294967294

minimum

The default TTL for every record in the zone. You can override this value for a specific record. Typical values range from eight hours to four days. This value is often set to 10 minutes or less when changes are being made to a zone. Default value: 5 Maximum value: 2147483647

TTL

The time to live, measured in seconds. Default value: 3600 Maximum value: 2147483647

Top

unset dns soaRec

Synopsis

unset dns soaRec <domain> [-serial] [-refresh] [-retry] [-expire] [-minimum] [-TTL]

Description

Use this command to remove dns soaRec settings.Refer to the set dns soaRec command for meanings of the arguments.

Top

show dns soaRec

Synopsis

show dns soaRec [<domain> | -type <type>]

Description

Display the specified Start of Authority record. If the domain name is not specified, all of the SOA records are displayed.

Parameters

domain

The domain name.

type

The SOA record type. The type can take 3 values : ADNS - If this is specified, all of the authoritative SOA records will be displayed. PROXY - If this is specified, all the proxy SOA records will be displayed. ALL - If this is specified, all the SOA records will be displayed. Possible values: ALL, ADNS, PROXY

Top

dns suffix

[add | rm | show]

add dns suffix

Synopsis

add dns suffix <dnsSuffix>

Description

Append suffixes while resolving the domain names.

Parameters

dnsSuffix

Suffix to be appended while resolving the domain name.

Example

add dns suffix netscaler.com

If the incoming domain name "engineering" is not resolved by itself, the system will append the suffix netsca

Top

rm dns suffix

Synopsis

rm dns suffix <dnsSuffix>

Description

Remove the DNS suffixes.

Parameters

dnsSuffix

Suffix name to be removed.

Top

show dns suffix

Synopsis

show dns suffix [<dnsSuffix>]

Description

Display all the configured DNS suffixes.

Parameters

dnsSuffix

Suffix to be appended while resolving the domain name.

Top

dns nameServer

[add | rm | enable | disable | show]

add dns nameServer

Synopsis

add dns nameServer ((<IP> [-local]) | <dnsVserverName>) [-state (ENABLED | DISABLED)] [-type <type>]

Description

Add a name server. Two types of name servers can be added: 1. IP Address-based name server. In this case, the user must specify the Ipaddress of the name server to be contacted. 2. Vserver-based name server. In this case, the user must specify the name of the DNS vserver configured in the System.

Parameters

IP

The IP address of the name server.

dnsVserverName

The name of the dns vserver

local

IP is a local recursive nameserver.

state

The administrative state of the nameserver. Possible values: ENABLED, DISABLED Default value: ENABLED

type

The protocol type of the name server. While adding a vserver-based name server UDP_TCP is not a valid type. Possible values: UDP, TCP, UDP_TCP Default value: NSA_UDP

Example

Adding an-IP based nameserver IP:
add nameserver 10.102.4.1,
Adding a vserver-based name server:
add nameserver dns_vsvr
where dns_vsvr is the name of a DNS vserver created in the system.

Top

rm dns nameServer

Synopsis

rm dns nameServer (<IP> | <dnsVserverName>)

Description

Remove the NameServer.

Parameters

IP

The IP address of the name server.

dnsVserverName

The name of the dns vserver.

Example

Deleting an IP-based nameserver:
rm nameserver 10.102.4.1,
Deleting a vserver-based nameserver:
rm nameserver dns_vsvr

Top

enable dns nameServer

Synopsis

enable dns nameServer (<IP> | <dnsVserverName>)

Description

Enable a nameserver.

Parameters

IP

The IP address of the name server.

dnsVserverName

The name of the dns vserver.

Example

enable dns nameserver 10.14.43.149

Top

disable dns nameServer

Synopsis

disable dns nameServer (<IP> | <dnsVserverName>)

Description

Disable a nameserver.

Parameters

IP

The IP address of the name server.

dnsVserverName

The name of the dns vserver

Example

disable dns nameserver 10.14.43.149

Top

show dns nameServer

Synopsis

show dns nameServer [<IP> | <dnsVserverName>]

Description

Display the name servers configured in the system and the state of the name servers.

Parameters

IP

The IP address of the name server.

dnsVserverName

The name of the dns vserver.

Top

dns view

[add | rm | show]

add dns view

Synopsis

add dns view <viewName>

Description

Adds a dns view, used for dns view-based policies and for binding a view-specific IP for a gslb service.

Parameters

viewName

Name of the view name.

Example

add dns view privateview

Top

rm dns view

Synopsis

rm dns view <viewName>

Description

Removes a dns view that is used for dns view-based policies, and for binding a view-specific IP for a gslb service.

Parameters

viewName

Name of the view name.

Example

rm dns view privateview

Top

show dns view

Synopsis

show dns view [<viewName>]

Description

Displays the dns views configured in the system.

Parameters

viewName

The name of the view to be displayed.

Top

dns policy

[add | rm | set | show]

add dns policy

Synopsis

add dns policy <name> <rule> <actionName>

Description

Add a dns policy. DNS policies that can be added are Interface, IP,VLAN expressions.

Parameters

name

Name of the dns policy.

rule

Expression to be used by the dns policy.

viewName

The view name that must be used for the given policy.

preferredLocation

The location used for the given policy. This is deprecated attribute. Please use -prefLocList

preferredLocList

The location list in priority order used for the given policy.

drop

The dns packet must be dropped. Possible values: YES, NO

cacheBypass

By pass dns cache for this. Possible values: YES, NO

actionName

Name of the dns action added using add dns action command.

Example

```
add dns policy pol1 "dns.req.question.type.ne(aaaa)" -actionName act1
add dns policy pol2 "CLIENT.IP.SRC.IN_SUBNET(1.1.1.1/24)" -actionName action1
add dns policy pol1 dns.res.question.domain.contains("citrix") -actionName act2
```

Top

rm dns policy

Synopsis

rm dns policy <name>

Description

Removes a dns policy.

Parameters

name

Name of the dns policy.

Top

set dns policy

Synopsis

set dns policy <name> [<rule>] [-actionName <string>]

Description

Used to change the expression or action of an already existing policy. DNS policies that can be set are Interface,IP,VLAN expressions.

Parameters

name

Name of the dns policy.

rule

Expression to be used by dns policy.

viewName

The view name that must be used for the given policy

preferredLocation

The location used for the given policy. This is deprecated attribute. Please use -prefLocList

preferredLocList

The location list in priority order used for the given policy.

drop

The dns packet must be dropped. Possible values: YES, NO

cacheBypass

By pass dns cache for this. Possible values: YES, NO

actionName

Name of the dns action added using add dns action command.

Example

```
set dns policy pol1 -rule "dns.req.question.type.ne(aaaa)"
set dns policy pol2 -rule "CLIENT.IP.SRC.IN_SUBNET(1.1.1.1/24)"
set dns policy pol1 -rule dns.res.header.rcode.eq(nxdomain)
```

Top

show dns policy

Synopsis

show dns policy [<name>]

Description

Used to display the policy-related information.

Parameters

name

Name of the dns policy.

Top

dns zone

[add | set | unset | rm | sign | unsign | show]

add dns zone

Synopsis

add dns zone <zoneName> -proxyMode (YES | NO)

Description

Add a DNS zone on NetScaler

Parameters

zoneName

The name of the zone being added.

proxyMode

zone deployed in proxy mode. Possible values: YES, NO Default value: ENABLED

Example

add dns zone foo.bar -proxyMode NO -dnssec ENABLED

Top

set dns zone

Synopsis

set dns zone <zoneName> [-proxyMode (YES | NO)]

Description

set a DNS zone parameters on NetScaler

Parameters

zoneName

The name of the zone being added.

proxyMode

zone deployed in proxy mode. Possible values: YES, NO Default value: ENABLED

Example

set dns zone foo.bar -proxyMode NO -dnssec ENABLED

Top

unset dns zone

Synopsis

unset dns zone <zoneName> -proxyMode

Description

Use this command to remove dns zone settings.Refer to the set dns zone command for meanings of the arguments.

Top

rm dns zone

Synopsis

rm dns zone <zoneName>

Description

Remove the ZONE record for a given zone name.

Parameters

zoneName

The name of the zone to be removed.

Top

sign dns zone

Synopsis

sign dns zone <zoneName> [-keyName <string> ...]

Description

sign a dns zone with the given key

Parameters

zoneName

The name of the zone being signed.

keyName

The name given to a public/private key pair.

Example

sign dns zone abc.com. -keyname abc.com.zsk abc.com.ksk

Top

unsign dns zone

Synopsis

unsign dns zone <zoneName> [-keyName <string> ...]

Description

Unsign a zone with the specified key

Parameters

zoneName

The name of the zone being signed.

keyName

The name given to a public/private key pair.

Example

unsign dns zone abc.com. -keyname abc.com.zsk abc.com.ksk

Top

show dns zone

Synopsis

show dns zone [<zoneName> | -type <type>]

Description

Show a DNS zone on NetScaler

Parameters

zoneName

The name of the zone whose info is to be displayed.

type

Zone type. The type can take 3 values: ADNS - If this is specified, all of the authoritative zones will be displayed. PROXY - If this is specified, all of the proxy zones will be displayed. ALL - If this is specified, all of the zones will be displayed. Possible values: ALL, ADNS, PROXY

Example

show dns zone foo.bar

Top

dns key

[add | create | set | unset | rm | show]

add dns key

Synopsis

add dns key <keyName> <publickey> <privatekey> [-expires <positive_integer> [<units>]] [-notificationPeriod <positive_integer> [<units>]] [-TTL <secs>]

Description

Add a DNSKEY on NetScaler

Parameters

keyName

The name given to a public/private key pair.

publickey

File name of the public key to be used for signing zone

privatekey

File name of the private key to be used for signing zone

expires

Number of days since signing with a key, when the key expires. Default value: 120 Minimum value: 1 Maximum value: 32767

notificationPeriod

Number of days before the expiry of a key, when an notification should be generated. Default value: 7 Minimum value: 1 Maximum value: 32767

TTL

Time to live, in seconds. Default value: 3600 Maximum value: 2147483647

Example

add dns key secure.example.zsk -public secure.example-rsasha1-1024.key
-private /nsconfig/dns/secure.example-rsasha1-1024.private

Top

create dns key

Synopsis

create dns key -zoneName <string> -keyType <keyType> -algorithm RSASHA1 -keySize <positive_integer> -fileNamePrefix <string>

Description

Create a public-private key for dnssec operations.

Parameters

zoneName

The name of the zone for which the key is being added.

keyType

The type of key. Possible values: KSK, KeySigningKey, ZSK, ZoneSigningKey Default value: NS_DNSKEY_ZSK

algorithm

The type of algorithm to be generated. Possible values: RSASHA1 Default value: NS_DNSKEYALGO_RSASHA1

keySize

The size in bits of the key to be created. Default value: 512

fileNamePrefix

The string to be used as file name for the generated public, private and ds key files.

Example

create dns key -zone dnssec.bar -algorithm RSASHA1 -keySize 1024

Top

set dns key

Synopsis

set dns key <keyName> [-expires <positive_integer> [<units>]] [-notificationPeriod <positive_integer> [<units>]] [-TTL <secs>]

Description

Add a DNSKEY on NetScaler

Parameters

keyName

The name given to a public/private key pair.

expires

Number of days since signing with a key, when the key expires. Default value: 120 Minimum value: 1 Maximum value: 32767

notificationPeriod

Number of days before the expiry of a key, when an notification should be generated. Default value: 7 Minimum value: 1 Maximum value: 32767

TTL

Time to live, in seconds. Default value: 3600 Maximum value: 2147483647

Example

add dns key secure.example.zsk -public secure.example-rsasha1-1024.key -private /nsconfig/dns/secure.example-rsasha1-1024.private

Top

unset dns key

Synopsis

unset dns key <keyName> [-expires] [-units] [-notificationPeriod] [-units] [-TTL]

Description

Use this command to remove dns key settings.Refer to the set dns key command for meanings of the arguments.

Top

rm dns key

Synopsis

rm dns key <keyName>

Description

Remove a DNSKEY on NetScaler

Parameters

keyName

The name given to a public/private key pair.

Example

rm dns key secure.example.zsk

Top

show dns key

Synopsis

show dns key [<keyName>]

Description

Show a DNSKEY's on NetScaler

Parameters

keyName

The name of the key whose info is to be displayed.

Example

show dns key

Top

dns proxyRecords

flush dns proxyRecords

Synopsis

flush dns proxyRecords

Description

Flush all the DNS proxy records.

dns records

stat dns records

Synopsis

stat dns records [<dnsRecordType>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics for DNS records.

Parameters

dnsRecordType

DNS Record/Query type

dns stats

show dns stats

Synopsis

show dns stats - alias for 'stat dns'

Description

show dns stats is an alias for stat dns

dns parameter

[set | unset | show]

set dns parameter

Synopsis

set dns parameter [-retries <positive_integer>] [-minTTL <secs>] [-maxTTL <secs>] [-cacheRecords (YES | NO)] [-nameLookupPriority (WINS | DNS)] [-recursion (ENABLED | DISABLED)] [-resolutionOrder <resolutionOrder>] [-dnssec (ENABLED | DISABLED)] [-maxPipeline <positive_integer>] [-dnsRootReferral (ENABLED | DISABLED)]

Description

Set TTL parameters.

Parameters

retries

The DNS resolver request retry count. Default value: 5 Minimum value: 1 Maximum value: 5

minTTL

The minimum time to live value, in seconds. If any DNS entry has a time to live value of less than the minimum, it is saved as the minimum time to live value. Maximum value: 604800

maxTTL

The maximum time to live value allowed, in seconds. If the DNS entry has a time to live value of more than the maximum, it is saved as the maximum time to live value. Default value: 604800 Minimum value: 1 Maximum value: 604800

cacheRecords

The state of dns records caching. Possible values: YES, NO Default value: YES

nameLookupPriority

The name lookup priority, as DNS or WINS. Possible values: WINS, DNS Default value: NS_WINSFIRST

recursion

Allow recursive name resolution by NetScaler. Possible values: ENABLED, DISABLED Default value: DISABLED

resolutionOrder

The order in which DNS resolver send A/AAAA query for the domain. Possible values: OnlyAQuery, OnlyAAAAQuery, AThenAAAAQuery, AAAAThenAQuery Default value: NS_FOUR

dnssec

To enable the DNS security extensions Possible values: ENABLED, DISABLED Default value: ENABLED

maxPipeline

To set the maximum value of the concurrent DNS pipeline. A setting of zero makes the pipeline infinite Default value: NSNATPCB_MAXPIPELINE

dnsRootReferral

This option is used to enable/disable the sending NS root referrals. Possible values: ENABLED, DISABLED Default value: DISABLED

Top

unset dns parameter

Synopsis

unset dns parameter [-retries] [-minTTL] [-maxTTL] [-cacheRecords] [-nameLookupPriority] [-recursion] [-resolutionOrder] [-dnssec] [-maxPipeline] [-dnsRootReferral]

Description

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

Top

show dns parameter

Synopsis

show dns parameter

Description

Display dns parameter. Displays the following value: DNS Retries - The DNS resolver request timeout. minTTL - The minimum allowed value for time to live. If a DNS entry has a time to live value less than the minimum, it is saved as the minimum time to live. maxTTL - The maximum allowed value for time to live. If any DNS entry has a time to live value less than the maximum, it is saved as the maximum time to live.

Top

dns policylabel

[add | rm | bind | unbind | show | stat | rename]

add dns policylabel

Synopsis

add dns policylabel <labelName> <transform>

Description

Add a dns policy label.

Parameters

labelName

Name of the dns policy label.

transform

The type of transformations allowed by the policies bound to the label. Possible values: dns_req, dns_res

Example

add dns policylabel trans_dns dns_req

Top

rm dns policylabel

Synopsis

rm dns policylabel <labelName>

Description

Remove a dns policy label.

Parameters

labelName

Name of the dns policy label.

Example

rm dns policylabel trans_dns

Top

bind dns policylabel

Synopsis

bind dns policylabel <labelName> <policyName> <priority> [<gotoPriorityExpression>] [-invoke (<labelType> <labelName>)]

Description

Bind the dns policy to one of the labels.

Parameters

labelName

Name of the dns policy label.

policyName

The dns policy name.

Example

i) bind dns policylabel trans_dns pol_1 1 2 -invoke reqvserver CURRENT
ii) bind rewrite policylabel trans_http_url pol_2 2

Top

unbind dns policylabel

Synopsis

unbind dns policylabel <labelName> <policyName> [-priority <positive_integer>]

Description

Unbind entities from dns label.

Parameters

labelName

Name of the dns policy label.

policyName

The dns policy name.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind dns policylabel trans_dns pol_1

Top

show dns policylabel

Synopsis

show dns policylabel [<labelName>]

Description

Display policy label or policies bound to dns policylabel.

Parameters

labelName

Name of the dns policy label.

Example

i) show dns policylabel trans_dns
ii) show dns policylabel

Top

stat dns policylabel

Synopsis

stat dns policylabel [<labelName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of dns policylabel(s).

Parameters

labelName

The name of the dns policy label for which statistics will be displayed. If not given statistics are shown for all dns policylabels.

Top

rename dns policylabel

Synopsis

rename dns policylabel <labelName>@ <newName>@

Description

Rename a dns policy label.

Parameters

labelName

The name of the dns policylabel.

newName

The new name of the dns policylabel.

Example

rename dns policylabel oldname newname

Top

dns global

[bind | unbind | show]

bind dns global

Synopsis

bind dns global <policyName> <priority> [-gotoPriorityExpression <string>] [-type <type>] [-invoke (<labelType> <labelName>)]

Description

Binds the DNS policy with the given priority.

Parameters

policyName

The name of the policy to be bound to dns global.

Example

bind dns global pol9 9

Top

unbind dns global

Synopsis

unbind dns global <policyName>

Description

Unbinds the DNS policy with the given priority.

Parameters

policyName

Name of the policy to be bound to dns global.

Example

unbind dns global pol9

Top

show dns global

Synopsis

show dns global [-type <type>]

Description

Display the DNS global bindings.

Parameters

type

Bindpoint, specifying where to bind the policy. Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

Example

show dns global
show dns global -type REQ_DEFAULT
show dns global -type RES_DEFAULT

Top

dns action

[add | rm | set | unset | show]

add dns action

Synopsis

add dns action <actionName> <actionType> [-IPAddress <ip_addr|ipv6_addr> ... | -viewName <string> | -preferredLocList <string> ...] [-TTL <secs>]

Description

Add a dns action.

Parameters

actionName

Name of the dns action.

actionType

The type of DNS action that is being configured. Possible values: ViewName, GslbPrefLoc, Drop, Cache_Bypass, Rewrite_Response

IPAddress

List of IP address to be returned in case of rewrite_response actiontype. They can be of IPV4 or IPV6 type. In case of set command We will remove all the IP address previously present in the action and will add new once given in set dns action command.

TTL

Time to live, in seconds. Default value: 3600 Maximum value: 2147483647

viewName

The view name that must be used for the given action.

preferredLocList

The location list in priority order used for the given action.

Example

add dns action <actionName> <actionType> (-IPAddress <ip_addr|ipv6_addr> ... | -viewName <string> | -pre
add dns action action1 Rewrite_Response -ipAddress 10.102.27.153 10.102.27.154 33::33 44::44 -TTL 4000
add dns action action1 GslbPrefLoc -preferredLocList india.10.102.81.175.80 us.10.102.81.176.80
add dns action action1 ViewName -viewName dnsview1

Top

rm dns action

Synopsis

rm dns action <actionName>

Description

Removes a dns Action.

Parameters

actionName

Name of the dns action.

Example

rm dns action action1

Top

set dns action

Synopsis

set dns action <actionName> [-IPAddress <ip_addr|ipv6_addr> ...] [-TTL <secs>] [-viewName <string>] [-preferredLocList <string> ...]

Description

Set a dns Action. Use this command to set the values for Ip address and TTL, If Ipaddress is given in set dns action command we will discard the previous set and will apply this new set of ipaddress given.

Parameters

actionName

Name of the dns action.

IPAddress

List of IP address to be returned in case of rewrite_response actiontype. They can be of IPV4 or IPV6 type. In case of set command We will remove all the IP address previously present in the action and will add new once given in set dns action command.

TTL

Time to live, in seconds. Default value: 3600 Maximum value: 2147483647

viewName

The view name that must be used for the given action.

preferredLocList

The location list in priority order used for the given action.

Example

```
set dns action <actionName> [-IPAddress <ip_addr|ipv6_addr> ...] [-TTL <secs>] [-viewName <string>] [-pref
set dns action action1  -ipAddress 10.102.27.153 10.102.27.154 33::33 44::44 -TTL 4000
set dns action action1  -viewName dnsview2
set dns action action1  -preferredLocList india.10.102.81.175.80
```

Top

unset dns action

Synopsis

unset dns action <actionName> -TTL

Description

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

Top

show dns action

Synopsis

show dns action [<actionName>]

Description

Used to display the action-related information.

Parameters

actionName

Name of the dns action.

Example

show dns action <Action-Name>
show dns action action1
show dns action

Top

dns nsecRec

show dns nsecRec

Synopsis

show dns nsecRec [<hostName> | -type <type>]

Description

Show the nsec records on NetScaler

Parameters

hostName

The domain name whose info is to be displayed.

type

NSEC record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative NSEC records will be displayed. PROXY - If this is specified, all of the proxy NSEC records will be displayed. ALL - If this is specified, all of the NSEC records will be displayed. Possible values: ALL, ADNS, PROXY

Example

show dns nsecRec foo.bar

DOS Commands

This group of commands can be used to perform operations on the following entities:

- dos
- dos policy
- dos stats

dos

stat dos

Synopsis

stat dos [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Displays DoS protection statistics.

dos policy

[add | rm | set | unset | show | stat]

add dos policy

Synopsis

add dos policy <name> -qDepth <positive_integer> [-cltDetectRate <positive_integer>]

Description

Adds a DoS protection policy to the appliance. Note: For DoS protection to be applied to a service, bind the DoS policy to the service by using the 'bind service' command.

Parameters

name

The name for the HTTP DoS protection policy. The name can include a maximum of 31 characters that include letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. The name can begin with a letter, number, or the underscore (_) symbol.

qDepth

The queue depth. It is the queue size (the number of outstanding service requests on the system) that must be reached before DoS protection is activated on the service to which the DoS protection policy is bound. Minimum value: 21

cltDetectRate

The client detect rate. It is an integer that represents the percentage of traffic to which the HTTP DoS policy must be applied. Maximum value: 100

Example

add dos policy dospol -qdepth 100 -cltDetectRate 90

Top

rm dos policy

Synopsis

rm dos policy <name>

Description

Removes a DoS protection policy from the appliance.

Parameters

name

The name of the DoS protection policy to be removed.

Example

rm dos policy dospol

Top

set dos policy

Synopsis

set dos policy <name> [-qDepth <positive_integer>] [-cltDetectRate <positive_integer>]

Description

Modifies the attributes of a DoS protection policy.

Parameters

name

The name of the DoS protection policy to be modified.

qDepth

The queue depth. It is the queue size (the number of outstanding service requests on the system) that must be reached before DoS protection is activated on the service to which the DoS protection policy is bound. Minimum value: 21

cltDetectRate

The client detect rate. It is an integer that represents the percentage of traffic to which the HTTP DoS policy must be applied. Minimum value: 1 Maximum value: 100

Example

set dos policy dospol -qdepth 1000

Top

unset dos policy

Synopsis

unset dos policy <name> -cltDetectRate

Description

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

Top

show dos policy

Synopsis

show dos policy [<name>]

Description

Displays details of the DoS protection policy.

Parameters

name

The name of the DoS protection policy whose details must be displayed. If a name is not provided, details of all DoS protection policies available on the appliance are displayed.

Example

```
> show dos policy
        1 configured DoS policy:
1)      Policy: dospol  QDepth: 100     ClientDetectRate: 90
 Done
```

Top

stat dos policy

Synopsis

stat dos policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Displays DoS protection policy statistics.

Parameters

name

The name of the DoS protection policy whose statistics must be displayed. If a name is not provided, statistics of all the DoS protection policies available on the appliance are displayed.

Top

dos stats

show dos stats

Synopsis

show dos stats - alias for 'stat dos'

Description

show dos stats is an alias for stat dos

Filter Commands

This group of commands can be used to perform operations on the following entities:

- filter action
- filter htmlinjectionvariable
- filter policy
- filter prebodyInjection
- filter postbodyInjection
- filter htmlinjectionparameter
- filter global

filter action

[add | rm | set | unset | show]

add filter action

Synopsis

add filter action <name> <qual> [<serviceName>] [<value>] [<respCode>] [<page>]

Description

Create a content filtering action. The action thus created can be associated with the content filtering policy. The two built-in filter actions RESET and DROP are always present on the system. Use the RESET filter action to send a TCP reset for the HTTP requests. Use the DROP filter action to drop the HTTP requests silently without sending a TCP FIN for closing the connection.

Parameters

name

The name for the filter action.

qual

The name of the qualifier. Possible values: reset, add, corrupt, forward, errorcode, drop

serviceName

The service to which HTTP requests are forwarded. This parameter is required when the qualifier is FORWARD.

value

The string containing the header_name and header_value. When the qualifier is ADD use this option as header_name:header_value. When the qualifier is Corrupt use this option to specify only the header_name.

respCode

The response code to be returned for HTTP requests. Use this parameter when the qualifier is ERRORCODE. Minimum value: 1

page

The HTML page that will be returned for the HTTP requests. Use this parameter when the qualifier is ERRORCODE.

Example

```
add filter action bad_url_action errorcode 400 "<HTML>Bad URL.</HTML>"
add filter action forw_action FORWARD service1
add filter action add_header_action add "HEADER:value"
```

Top

rm filter action

Synopsis

rm filter action <name>

Description

Remove a created filter action.

Parameters

name

The name of the filter action.

Example

```
rm filter action filter_action_name
```

Top

set filter action

Synopsis

set filter action <name> [-serviceName <string>] [-value <string>] [-respCode <positive_integer>] [-page <string>]

Description

Modify an existing content filtering action.

Parameters

name

The name for the filter action.

serviceName

The service to which HTTP requests are forwarded. This parameter can be set only when the action qualifier is FORWARD.

value

The string containing the header_name and header_value. When the qualifier is ADD use this option as header_name:header_value. When the qualifier is Corrupt use this option to specify only the header_name.

respCode

The response code to be returned for HTTP requests. Use this parameter when the qualifier is ERRORCODE. Minimum value: 1

page

The HTML page that will be returned for the HTTP requests. Use this parameter when the action qualifier is ERRORCODE.

Example

```
set filter action bad_url_action -respcode 400 -page "<HTML>Bad URL.</HTML>"
set filter action forw_action -serviceName service1
set filter action add_header_action -value "HEADER:value"
```

Top

unset filter action

Synopsis

unset filter action <name> -page

Description

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

Top

show filter action

Synopsis

show filter action [<name>]

Description

Display the created filter actions. The filter actions RESET and DROP are always displayed, irrespective of whether an action has been defined. They are built-in actions and cannot be modified.

Parameters

name

The name for the filter action.

Example

Example 1
The following shows an example of the output of the show filter action command when no filter actions have
1) Name: RESET Filter Type: reset
2) Name: DROP Filter Type: drop
Done

Example 2
The following command creates a filter action:
add filter action bad_url_action errorcode 400 "<HTML>Bad URL.</HTML>"
The following shows an example of the output of the show filter action command after the previous commar
Name: bad_url_action Filter Type: errorcode
StatusCode: 400
Response Page: <HTML>Bad URL.</HTML>
Done

Top

filter htmlinjectionvariable

[add | rm | set | unset | show]

add filter htmlinjectionvariable

Synopsis

add filter htmlinjectionvariable <variable> [-value <string>]

Description

Add a new HTML injection variable

Parameters

variable

The name of the HTML injection variable to be added.

value

Value to be assigned to the new variable.

varId

ID of the system variable. Used only in builtins. Possible values: IID, UTIME, XID, PAGEID, REQRTBEG, REQRTEND, REQSTBEG, REQSTEND, RESRTBEG, RESRTEND, RESSTBEG, RESSTEND, CLTRTT, CTYPE, TRANSID, SYSVSVR, SYSSERV

Example

add htmlinjectionvariable EDGESIGHT_SERVER_IP -value 1.1.1.1

Top

rm filter htmlinjectionvariable

Synopsis

rm filter htmlinjectionvariable <variable>

Description

Remove a HTML injection variable

Parameters

variable

The name of the HTML injection variable to be removed.

Example

rm htmlinjectionvariable EDGESIGHT_SERVER_IP

Top

set filter htmlinjectionvariable

Synopsis

set filter htmlinjectionvariable <variable> [-value <string>]

Description

Set the value of a HTML injection variable

Parameters

variable

The name of the HTML injection variable to be set.

value

Value to be set in the new variable.

Example

set htmlinjectionvariable EDGESIGHT_SERVER_IP -value 2.2.2.2

Top

unset filter htmlinjectionvariable

Synopsis

unset filter htmlinjectionvariable <variable> -value

Description

Use this command to remove filter htmlinjectionvariable settings.Refer to the set filter htmlinjectionvariable command for meanings of the arguments.

Top

show filter htmlinjectionvariable

Synopsis

show filter htmlinjectionvariable [<variable>]

Description

Display HTML injection variable

Parameters

variable

The name of the HTML injection variable to be displayed.

Example

show htmlinjectionvariable EDGESIGHT_SERVER_IP

Top

filter policy

[add | rm | set | show]

add filter policy

Synopsis

add filter policy <name> -rule <expression> (-reqAction <string> | -resAction <string>)

Description

Create a content filtering policy.

Parameters

name

The name of the new filter policy.

rule

The expression which sets the condition for application of the policy.

reqAction

The name of the action to be performed on the request. The string value can be a created filter action or one of the following built-in actions: RESET - Sends the TCP reset and closes the connection to the peer. DROP - Silently closes the connection to the peer without sending the TCP FIN. Note that the request action can not be specified if the rule has some condition to be evaluated for response.

resAction

The action to be performed on the response. The string value can be a filter action created filter action or a built-in action.

Example

Example 1:
add policy expression e1 "sourceip == 66.33.22.0 -netmask 255.255.255.0"
add policy expression e2 "URL == /admin/account.asp"
add filter policy ip_filter -rule "e1 && e2" -reqAction RESET
After creating above filter policy, it can be activated by binding it globally:
bind filter global ip_filter

With the configured ip_filter (name of the filter policy), the NetScaler system sends a TCP reset to all HTTP

Example 2:
To silently drop (without sending FIN) all the HTTP requests in which the URL has root.exe or cmd.exe, belo
add filter policy nimda_filter -rule "URL contains root.exe || URL contains cmd.exe" -reqAction DROP
bind filter global nimda_filter

Example 3:
add filter policy url_filter -rule "url == /foo/secure.asp && SOURCEIP != 65.186.55.0 -netmask 255.255.255.0
bind filter global url_filter

With the above configured filter policy named url_filter, the NetScaler system sends RESET to all HTTP requ

Note: In above examples, the RESET and DROP are built-in actions in the NetScaler system.

"show filter action" and "show filter policy" CLI commands show the configured filter actions and policies in N

Top

rm filter policy

Synopsis

rm filter policy <name>

Description

Remove a filter policy.

Parameters

name

The name of filter policy.

Example

rm filter policy filter_policy_name
The "show filter policy" command shows all filter policies that are currently defined.

Top

set filter policy

Synopsis

set filter policy <name> [-rule <expression>] [-reqAction <string> | -resAction <string>]

Description

Modify the created filter policy.

Parameters

name

The name of the filter policy.

rule

The expression which sets the condition for application of the policy.

reqAction

Request action.

resAction

Response action.

Example

Example 1:
A filter policy to allow access of URL /foo/secure.asp only from 65.186.55.0 network can be created using be
add filter policy url_filter -rule "URL == /foo/secure.asp && SOURCEIP != 65.186.55.0 -netmask 255.255.255.
This policy is activated using:
bind filter global url_filter

Later, to allow access of this url from second network 65.202.35.0 too, above filter policy can be changed by
set filter policy url_filter -rule "URL == /foo/secure.asp && SOURCEIP != 65.186.55.0 -netmask 255.255.255.0

Changed filter policy can be viewed by using following command:
show filter policy url_filter
Name: url_filter Rule: (URL == /foo/secure.asp && (SOURCEIP != 65.186.55.0 -netmask 255.255.255.0
Request action: RESET
Response action:
Hits: 0
Done

Top

show filter policy

Synopsis

show filter policy [<name>]

Description

Display the filter policies.

Parameters

name

The name of the filter policy.

Example

```
show filter policy
1)      Name: nimda_filter Rule: (URL CONTAINS root.exe || URL CONTAINS cmd.exe)
        Request action: RESET
        Response action:
        Hits: 0
2)      Name: ip_filter Rule: (src_ips && URL == /admin/account.asp)
        Request action: RESET
        Response action:
        Hits: 0
 Done

Individual filter policy can also be viewed by giving filter policy name as argument:
show filter policy ip_filter
        Name: ip_filter Rule: (src_ips && URL == /admin/account.asp)
        Request action: RESET
        Response action:
        Hits: 0
 Done
```

Top

filter prebodyInjection

[set | unset | show]

set filter prebodyInjection

Synopsis

set filter prebodyInjection <prebody>

Description

Set file name for prebody

Parameters

prebody

The file name for prebody.

Example

set filter prebodyInjection ens/prebody.js

Top

unset filter prebodyInjection

Synopsis

unset filter prebodyInjection [-prebody]

Description

Unset file name for prebody.Refer to the set filter prebodyInjection command for meanings of the arguments.

Example

unset filter prebodyInjection

Top

show filter prebodyInjection

Synopsis

show filter prebodyInjection

Description

Display the file for prebody.

Top

filter postbodyInjection

[set | unset | show]

set filter postbodyInjection

Synopsis

set filter postbodyInjection <postbody>

Description

Unset file name for postbody

Parameters

postbody

The file name for postbody.

Example

set filter postbodyInjection ens/postbody.js

Top

unset filter postbodyInjection

Synopsis

unset filter postbodyInjection [-postbody]

Description

Remove file name for prebody.Refer to the set filter postbodyInjection command for meanings of the arguments.

Example

unset filter postbodyInjection

Top

show filter postbodyInjection

Synopsis

show filter postbodyInjection

Description

Display the file for postbody.

Top

filter htmlinjectionparameter

[set | unset | show]

set filter htmlinjectionparameter

Synopsis

set filter htmlinjectionparameter [-rate <positive_integer>] [-frequency <positive_integer>] [-strict (ENABLED | DISABLED)] [-htmlsearchlen <positive_integer>]

Description

Set the various HTML injection parameters

Parameters

rate

if rate is X, HTML injection will be done for 1 out of X policy matches Default value: 1 Minimum value: 1

frequency

if frequency is X, HTML injection will be done atleast once per X milisecond Default value: 1 Minimum value: 1

strict

enable/disable searching for <html> tag for HTML injection Possible values: ENABLED, DISABLED Default value: ENABLED

htmlsearchlen

HTTP body length in which to search for <html> tag Default value: 1024 Minimum value: 1

Example

set htmlinjection parameter -rate 10 -frequency 1

Top

unset filter htmlinjectionparameter

Synopsis

unset filter htmlinjectionparameter [-rate] [-frequency] [-strict] [-htmlsearchlen]

Description

Unset the previously set HTML injection parameters.Refer to the set filter htmlinjectionparameter command for meanings of the arguments.

Example

a) unset htmlinjectionparameter -rate
b) unset htmlinjectionparameter -frequency
c) unset htmlinjectionparameter -rate -frequency

Top

show filter htmlinjectionparameter

Synopsis

show filter htmlinjectionparameter

Description

Display the HTML injection parameters

Example

rate : 10

Top

filter global

[bind | unbind | show]

bind filter global

Synopsis

bind filter global (<policyName> [-priority <positive_integer>]) [-state (ENABLED | DISABLED)]

Description

Activate the filter policy globally.Note that the content filtering license is required for filtering.

Parameters

policyName

The name of the filter policy to be bound.

Example

To send RESET for all the HTTP requests which are not get or head type, following filter policy can be create
add filter policy reset_invalid_req -rule "METHOD != GET && METHOD != HEAD" -reqAction RESET
This filter policy can be activated globally for NetScaler system by giving command:
bind filter global reset_invalid_req

Globally active filter policies can be seen using command:
show filter global
1) Policy Name: reset_invalid_req Priority: 0
 Done

Top

unbind filter global

Synopsis

unbind filter global <policyName>

Description

Deactivate a filter policy globally.

Parameters

policyName

The name of the filter policy to be unbound.

Example

Globally active filter policies can be seen using command:
show filter global
1) Policy Name: reset_invalid_req Priority: 0
Done
This globally active filter policy can be deactivated on NetScaler system by giving command:
unbind filter global reset_invalid_req

Top

show filter global

Synopsis

show filter global

Description

Display the globally activated filter policies.

Example

show filter global
1) Policy Name: url_filter Priority: 0
2) Policy Name: reset_invalid_req Priority: 0
Done

Top

GSLB Commands

This group of commands can be used to perform operations on the following entities:

- gslb site
- gslb service
- gslb vserver
- gslb runningConfig
- gslb domain
- gslb ldnsentries
- gslb parameter
- gslb ldnsentry
- gslb config
- gslb syncStatus

gslb site

[add | rm | set | unset | show | stat]

add gslb site

Synopsis

add gslb site <siteName> [<siteType>] <siteIPAddress> [-publicIP <ip_addr|ipv6_addr|*>] [-metricExchange (ENABLED | DISABLED)] [-nwMetricExchange (ENABLED | DISABLED)] [-sessionExchange (ENABLED | DISABLED)] [-triggerMonitor <triggerMonitor>] [-parentSite <string>]

Description

Add the site entity participating in GSLB in system

Parameters

siteName

The name of the site that is participating in the GSLB

siteType

Specify whether the site is LOCAL or REMOTE. If this option is not specified, then it will be automatically detected whether the site should be considered LOCAL or REMOTE. This decision is based on whether the siteIPAddress is found to be already configured in the system, for e.g., MIP or SNIP Possible values: REMOTE, LOCAL Default value: NS_NORMAL

siteIPAddress

The IP address of the site. This IP address will be a System owned IP address. SNIP or MIP can be used as Site IP address

publicIP

The Public IP. This parameter is in effect only for a LOCAL site. This parameter is required only if the local System is in a private address space and has a public IP hosted on an external FW or NAT device.

metricExchange

The state of MEP. When metric exchange is DISABLED, then the site does not exchange metrics with other sites. When this option is disabled, a simple ROUNDROBIN method will be used for Global Server Load Balancing. Possible values: ENABLED, DISABLED Default value: ENABLED

nwMetricExchange

Disable or enable exchange of network metrics like RTT. Possible values: ENABLED, DISABLED Default value: ENABLED

sessionExchange

Disable or enable exchange of persistence session entries. Possible values: ENABLED, DISABLED Default value: ENABLED

triggerMonitor

A setting that defines when bound monitors if any should be triggered for services belonging to this site. Possible values: ALWAYS, MEPDOWN, MEPDOWN_SVCDOWN Default value: NSGSLB_TRIGMON_ALWAYS

parentSite

Parent site of this site.

Example

add site new_york LOCAL 192.168.100.12 -publicIP 65.200.211.139

Top

rm gslb site

Synopsis

rm gslb site <siteName>

Description

Remove the site entity configured in system

Parameters

siteName

The name of the site entity to be removed. When the site is removed, all the services created under that site will be removed.

Example

rm gslb site new_york

Top

set gslb site

Synopsis

set gslb site <siteName> [-metricExchange (ENABLED | DISABLED)] [-nwMetricExchange (ENABLED | DISABLED)] [-sessionExchange (ENABLED | DISABLED)] [-triggerMonitor <triggerMonitor>]

Description

Enable or disable the Metric Exchange between sites

Parameters

siteName

The name of the site.

metricExchange

State of metric exchange for the site. If metric exchange is disabled, a simple ROUNDROBIN method is used to perform Global Server load balancing Possible values: ENABLED, DISABLED Default value: ENABLED

nwMetricExchange

Disable or enable exchange of network metrics like RTT. Possible values: ENABLED, DISABLED Default value: ENABLED

sessionExchange

Disable or enable exchange of persistence session entries. Possible values: ENABLED, DISABLED Default value: ENABLED

triggerMonitor

A setting that defines when bound monitors if any should be triggered for services belonging to this site. Possible values: ALWAYS, MEPDOWN, MEPDOWN_SVCDOWN Default value: NSGSLB_TRIGMON_ALWAYS

Example

set gslb site new_york - metricExchange DISABLED

Top

unset gslb site

Synopsis

unset gslb site <siteName> [-metricExchange] [-nwMetricExchange] [-sessionExchange] [-triggerMonitor]

Description

Use this command to remove gslb site settings.Refer to the set gslb site command for meanings of the arguments.

Top

show gslb site

Synopsis

show gslb site [<siteName>] show gslb site stats - alias for 'stat gslb site'

Description

Display the configured site entities in system

Parameters

siteName

The name of the site. If sitename is specified, all the services created under that site will be displayed.

Example

show site new_york

Top

stat gslb site

Synopsis

stat gslb site [<siteName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display Gslb site statistics.

Parameters

siteName

The name of the GSLB site for which statistics will be displayed. If not given statistics are shown for all gslb sites.

Top

gslb service

[add | rm | set | unset | bind | unbind | show | stat | rename]

add gslb service

Synopsis

add gslb service <serviceName> [-cnameEntry <string> | <IP> | <serverName> | <serviceType> | <port> | -publicIP <ip_addr|ipv6_addr|*> | -publicPort <port> | -sitePersistence <sitePersistence> | -sitePrefix <string>] [-maxClient <positive_integer>] [-healthMonitor (YES | NO)] [-siteName <string>] [-state (ENABLED | DISABLED)] [-cip (ENABLED | DISABLED) [<cipHeader>]] [-cookieTimeout <mins>] [-cltTimeout <secs>] [-svrTimeout <secs>] [-maxBandwidth <positive_integer>] [-downStateFlush (ENABLED | DISABLED)] [-maxAAAUsers <positive_integer>] [-monThreshold <positive_integer>] [-hashId <positive_integer>] [-comment <string>] [-appflowLog (ENABLED | DISABLED)]

Description

Add a GSLB service in the system.

Parameters

serviceName

The name of the service.

cnameEntry

The cname of the gslb service.

IP

The IP address of the server for which the service will be added

serverName

The name of the server for which the service will be added

serviceType

The type of service that is being added Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, RADIUS, RDP, RTSP, MYSQL, MSSQL Default value: NSSVC_SERVICE_UNKNOWN

port

The port on which the service is running Minimum value: 1

publicIP

The IP address on a NAT box in front of the system to which a private IP of the service maps. This is applicable to GSLB local services. This is optional

publicPort

The port on a NAT box in front of the system to which the private port of service maps. This is applicable to GSLB local services.This is optional

maxClient

The maximum number of open connections to the service. This argument is optional Maximum value: 4294967294

healthMonitor

Health monitoring state of the gslb service. Possible values: YES, NO Default value: YES

siteName

The GSLB site name. This parameter is mandatory. This option specifies whether the service is a local GSLB service or remote GSLB service

state

The state of the service(s). This parameter is optional. This is not applicable to the local GSLB services. Possible values: ENABLED, DISABLED Default value: ENABLED

cip

State of insertion of the Client IP header for the service. This parameter is used while connection proxy based Site persistency is enabled, and it inserts real client's IP address in the HTTP request Possible values: ENABLED, DISABLED Default value: DISABLED

cipHeader

The client IP header to be used in the HTTP request. If client IP insertion is enabled and the client IP header is not specified then the value that has been set by the set ns param CLI command will be used as the Client IP header.

sitePersistence

The state of cookie based Site persistency. Possible values: ConnectionProxy, HTTPRedirect, NONE

cookieTimeout

The timeout value in minutes for the cookie when cookie based Site persistency is enabled Maximum value: 1440

sitePrefix

Specify the site prefix string. When the service is bound to a GSLB vserver, then for each bound service-domain pair, a GSLB Site domain will be generated internally by concatenating the service's siteprefix and the domain's name. If a special string "NONE" is specified, the siteprefix string will be unset

cltTimeout

The idle time in seconds after which the client connection is terminated. This will be used while doing site persistency Maximum value: 31536000

svrTimeout

The idle time in seconds after which the server connection is terminated. This will be used while doing site persistency Maximum value: 31536000

maxBandwidth

A positive integer to identify the maximum bandwidth allowed for the service

downStateFlush

Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED

maxAAAUsers

The maximum number of concurrent SSLVPN users allowed to login at a time. Maximum value: 65535

monThreshold

The monitoring threshold. Maximum value: 65535

hashId

The hash identifier for the service. This must be unique for each service. This parameter is used by hash based load balancing methods. Minimum value: 1

comment

Comments associated with this gslb service.

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

Example

add gslb service sj_svc 203.12.123.12 http 80 -site san_jos

Top

rm gslb service

Synopsis

rm gslb service <serviceName>

Description

Remove a gslb service configured in system.

Parameters

serviceName

The name of the service entity to be removed

Example

rm gslb service sj_svc

Top

set gslb service

Synopsis

set gslb service <serviceName> [-IPAddress <ip_addr|ipv6_addr|*>] [-publicIP <ip_addr|ipv6_addr|*>] [-publicPort <port>] [-cip (ENABLED | DISABLED) [<cipHeader>]] [-sitePersistence <sitePersistence>] [-sitePrefix <string>] [-maxClient <positive_integer>] [-healthMonitor (YES | NO)] [-maxBandwidth <positive_integer>] [-downStateFlush (ENABLED | DISABLED)] [-maxAAAUsers <positive_integer>] [-viewName <string> <viewIP>] [-monThreshold <positive_integer>] [-weight <positive_integer> <monitorName>] [-hashId <positive_integer>] [-comment <string>] [-appflowLog (ENABLED | DISABLED)]

Description

Set parameters in the gslb service

Parameters

serviceName

The name of the gslb service.

IPAddress

The new IP address of the service.

publicIP

The IP address on a NAT box in front of the system to which a private IP service maps. This is optional. It is only valid for LOCAL GSLB service

publicPort

The port on a NAT box in front of the system to which the private port of service maps. This is optional. It is only valid for local service Minimum value: 1

cip

Insertion of the Client IP header for the service. This option is used while connection proxy based Site persistency is enabled Possible values: ENABLED, DISABLED Default value: DISABLED

sitePersistence

The state of cookie based Site persistency. Possible values: ConnectionProxy, HTTPRedirect, NONE

sitePrefix

The site prefix string.

maxClient

Maximum number of Clients. Maximum value: 4294967294

healthMonitor

Health monitoring state of the gslb service. Possible values: YES, NO Default value: YES

maxBandwidth

Maximum bandwidth.

downStateFlush

Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

maxAAAUsers

The maximum number of concurrent SSLVPN users allowed to login at a time. Maximum value: 65535

viewName

The name of view for the given IP

monThreshold

The monitoring threshold. Maximum value: 65535

weight

The weight for the specified monitor. Minimum value: 1 Maximum value: 100

hashId

The hash identifier for the service. This must be unique for each service. This parameter is used by hash based load balancing methods. Minimum value: 1

comment

Comments associated with this gslb service.

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set gslb service sj_svc -sitePersistence ConnectionProxy

Top

unset gslb service

Synopsis

unset gslb service <serviceName> [-publicIP] [-publicPort] [-cip] [-cipHeader] [-sitePersistence] [-sitePrefix] [-maxClient] [-healthMonitor] [-maxBandwidth] [-downStateFlush] [-maxAAAUsers] [-viewIP] [-monThreshold] [-monitorName] [-hashId] [-comment] [-appflowLog]

Description

Use this command to remove gslb service settings.Refer to the set gslb service command for meanings of the arguments.

Top

bind gslb service

Synopsis

bind gslb service <serviceName> ((-viewName <string> <viewIP>) | (-monitorName <string>@ [-monState (ENABLED | DISABLED)] [-weight <positive_integer>]))

Description

Binding a view specific IP to this service

Parameters

serviceName

The name of the gslb service

viewName

The name of view for the given IP

monitorName

The name of the service or a service group to which the monitor is to be bound.

Example

bind gslb service -viewName privateview 1.2.3.4

Top

unbind gslb service

Synopsis

unbind gslb service <serviceName> (-viewName <string> | -monitorName <string>@)

Description

Unbinding a view from the service

Parameters

serviceName

The name of the gslb service

viewName

The name of view for the given IP

monitorName

Name of the monitor to unbind.

Example

unbind gslb service -viewName privateview

Top

show gslb service

Synopsis

show gslb service [<serviceName>] show gslb service stats - alias for 'stat gslb service'

Description

Display the gslb services configured in the system.

Parameters

serviceName

The name of the gslb service.

Example

show gslb service sj_svc

Top

stat gslb service

Synopsis

stat gslb service [<serviceName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of a service.

Parameters

serviceName

The name of the service.

Top

rename gslb service

Synopsis

rename gslb service <serviceName>@ <newName>@

Description

Rename a gslb service.

Parameters

serviceName

The name of the gslb service.

newName

The new name of the gslb service.

Example

rename gslb service gsl_svc gslb_svc_new

Top

gslb vserver

[add | rm | set | unset | bind | unbind | enable | disable | show | stat | rename]

add gslb vserver

Synopsis

add gslb vserver <name> <serviceType> [-dnsRecordType <dnsRecordType>] [-lbMethod <lbMethod>] [-backupLBMethod <backupLBMethod>] [-netmask <netmask>] [-v6netmasklen <positive_integer>] [-tolerance <positive_integer>] [-persistenceType (SOURCEIP | NONE)] [-persistenceId <positive_integer>] [-persistMask <netmask>] [-v6persistmasklen <positive_integer>] [-timeout <mins>] [-EDR (ENABLED | DISABLED)] [-MIR (ENABLED | DISABLED)] [-disablePrimaryOnDown (ENABLED | DISABLED)] [-dynamicWeight <dynamicWeight>] [-state (ENABLED | DISABLED)] [-considerEffectiveState (NONE | STATE_ONLY)] [-comment <string>] [-soMethod <soMethod>] [-soPersistence (ENABLED | DISABLED)] [-soPersistenceTimeOut <positive_integer>] [-soThreshold <positive_integer>] [-appflowLog (ENABLED | DISABLED)]

Description

Add a GSLB vserver in the system.

Parameters

name

The virtual server name.

serviceType

The service type of the virtual server Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, RADIUS, RDP, RTSP, MYSQL, MSSQL

ipType

The IP type for this GSLB vserver. Possible values: IPV4, IPV6 Default value: NSGSLB_IPV4

dnsRecordType

Record type for GSLB vserver. Possible values: A, AAAA, CNAME Default value: NSGSLB_A

lbMethod

The load balancing method for the virtual server.The valid options for this parameter are: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT , CUSTOMLOAD Possible

values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD Default value: PEMGMT_LB_LEASTCONNS

backupSessionTimeout

A non zero value enables the feature whose minimum value is 2 minutes. The feature can be disabled by setting the value to zero. The created session is in effect for a specific client per domain. Maximum value: 1440

backupLBMethod

The load balancing method for the virtual server, in case the primary lb method fails on impossible to perform. The valid options for this parameter are: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT , CUSTOMLOAD. Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD

netmask

The netmask to be used in the SOURCEIPHASH policy. The default is 255.255.255.255 Default value: 0xFFFFFFFF

v6netmasklen

The Network mask. Use this parameter if you are setting the DESTINATIONIPHASH or SOURCEIPHASH policy. Enter the netmask to be used in modifying the destination or source IP address or network. Default value: 128 Minimum value: 1 Maximum value: 128

tolerance

The Site selection tolerance is the maximum deviation (in milliseconds) in the RTT value, which the system can tolerate, while deciding the best site for a domain. This value enables the system to implement the Round Robin method of GSLB between sites that have RTT values within this permissible limit. The tolerance value is required only if the LB method is RTT. The default tolerance value is 0 Maximum value: 100

persistenceType

The persistence type for the virtual server. This has 2 options: SOURCEIP and NONE Possible values: SOURCEIP, NONE

persistenceId

The Persistence Id. This parameter is a positive integer which is used to identify the GSLB VIP on all sites. This is a required argument if SOURCEIP based persistency is enabled. Maximum value: 65535

persistMask

The netmask to be used while SOURCEIP based persistency is ENABLED.This is an optional argument. Default value: 0xFFFFFFFF

v6persistmasklen

The persistence mask. Use this parameter if you are using IP based persistence type on a ipv6 vserver. Default value: 128 Minimum value: 1 Maximum value: 128

timeout

The idle time out in minutes for the persistence entries Default value: 2 Minimum value: 2 Maximum value: 1440

EDR

Use this parameter to specify whether System will send empty DNS response when all the sites participating in GSLB are down Possible values: ENABLED, DISABLED Default value: DISABLED

MIR

Use this parameter to specify whether System can send Multiple IP addresses in the DNS response or not. Possible values: ENABLED, DISABLED Default value: DISABLED

disablePrimaryOnDown

When this feature is enabled we will continue to direct traffic to the backup chain even after the primary comes UP. Ideally one should use backup persistence if they want to stick to the same vserver in the chain. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicWeight

Specifies whether we want to consider the svc count or the svc weights or ignore both Possible values: SERVICECOUNT, SERVICEWEIGHT, DISABLED Default value: DISABLED

state

State of the virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

considerEffectiveState

Specifies which backup to consider when the primary state of all gslb services bound to the vip are down. By specifying NONE we will not consider the effective state of the gslb service to determine the state of the gslb vip. If STATE_ONLY is chosen we will consider the effective state obtained via MEP to determine the state of the gslb vip Possible values: NONE, STATE_ONLY Default value: NS_GSLB_DONOT_CONSIDER_BKPS

comment

Comments associated with this virtual server.

soMethod

The spillover factor based on which the traffic will be given to the backupvserver once the main virtual server reaches the spillover threshold. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence

The state of the spillover persistence. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut

The spillover persistency entry timeout. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold

In case of CONNECTION (or) DYNAMICCONNECTION type spillover method this value is treated as Maximum number of connections a lb vserver will handle before spillover takes place. In case of BANDWIDTH type spillover method this value is treated as the amount of incoming and outgoing traffic (in Kbps) a Vserver will handle before spillover takes place. In case of HEALTH type spillover method if the percentage of active services (by weight) becomes lower than this value, spillover takes place Minimum value: 1 Maximum value: 4294967287

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

Example

add gslb vserver gvip http

Top

rm gslb vserver

Synopsis

rm gslb vserver <name>

Description

Remove a GSLB vserver configured in system.

Parameters

name

The name of the GSLB virtual server to be removed

Example

rm gslb vserver gvip

Top

set gslb vserver

Synopsis

set gslb vserver <name> [-dnsRecordType <dnsRecordType>] [-backupVServer <string>] [-lbMethod <lbMethod>] [-backupLBMethod <backupLBMethod>] [-netmask <netmask>] [-v6netmasklen <positive_integer>] [-tolerance <positive_integer>] [-persistenceType (SOURCEIP | NONE)] [-persistenceId <positive_integer>] [-persistMask <netmask>] [-v6persistmasklen <positive_integer>] [-timeout <mins>] [-EDR (ENABLED | DISABLED)] [-MIR (ENABLED | DISABLED)] [-disablePrimaryOnDown (ENABLED | DISABLED)] [-dynamicWeight <dynamicWeight>] [-considerEffectiveState (NONE | STATE_ONLY)] [-soMethod <soMethod>] [-soPersistence (ENABLED | DISABLED)] [-soPersistenceTimeOut <positive_integer>] [-soThreshold <positive_integer>] [-serviceName <string> -weight <positive_integer>] [-domainName <string> [-TTL <secs>] [-backupIP <ip_addr|ipv6_addr|*>] [-cookieDomain <string>] [-cookieTimeout <mins>] [-sitedomainTTL <secs>]] [-comment <string>] [-appflowLog (ENABLED | DISABLED)]

Description

Specify different settings on GSLB vserver

Parameters

name

The virtual server name.

ipType

The IP type for this GSLB vserver. Possible values: IPV4, IPV6 Default value: NSGSLB_IPV4

dnsRecordType

Record type for GSLB vserver. Possible values: A, AAAA, CNAME Default value: NSGSLB_A

backupVServer

Backup server.

backupSessionTimeout

A non zero value enables the feature whose minimum value is 2 minutes. The feature can be disabled by setting the value to zero. The created session is in effect for a specific client per domain. Maximum value: 1440

lbMethod

The load balancing method for the virtual server. Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD Default value: PEMGMT_LB_LEASTCONNS

netmask

The netmask to be used in the SOURCEIPHASH policy. Default value: 0xFFFFFFFF

v6netmasklen

The Network mask. Use this parameter if you are setting the DESTINATIONIPHASH or SOURCEIPHASH policy. Enter the v6 prefix length to be used in modifying the destination or source IPv6 address or network. Default value: 128 Minimum value: 1 Maximum value: 128

tolerance

The Site selectionn tolerance. Site selection tolerance is the maximum deviation (in milliseconds) in the RTT value, which the System system can tolerate, while deciding the best site for a domain. This value enables the system to implement the Round Robin method of GSLB between sites that have RTT values within this permissible limit. The tolerance value is required only if the LB method is RTT. Maximum value: 100

persistenceType

The persistence type for the virtual server. Possible values: SOURCEIP, NONE

persistenceId

The Persistence Id. This parameter is a positive integer which is used to identify the GSLB VIP on all sites Maximum value: 65535

persistMask

The netmask to be used while SOURCEIP based persistency is ENABLED.This is an optional argument. Default is 255.255.255.255 Default value: 0xFFFFFFFF

v6persistmasklen

The netmask to be useed for ipv6 traffic when the persistency type is SOURCEIP. Default value: 128 Minimum value: 1 Maximum value: 128

timeout

The idle time out in minutes for the persistence entries Default value: 2 Minimum value: 2 Maximum value: 1440

EDR

The state of the System in sending empty DNS response when all the sites participating in GSLB are down. Possible values: ENABLED, DISABLED Default value: DISABLED

MIR

The state of the System in sending Multiple IP addresses in the DNS response. Possible values: ENABLED, DISABLED Default value: DISABLED

disablePrimaryOnDown

When this feature is enabled we will continue to direct traffic to the backup chain even after the primary comes UP. Ideally one should use backup persistence if they want to stick to the same vserver in the chain. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicWeight

The state to consider the svc count or the svc weights or ignore both. Possible values: SERVICECOUNT, SERVICEWEIGHT, DISABLED Default value: DISABLED

considerEffectiveState

Specifies which backup to consider when the primary state of all gslb services bound to the vip are down. By specifying NONE we will not consider the effective state of the gslb service to determine the state of the gslb vip. If STATE_ONLY is chosen we will consider the effective state obtained via MEP to determine the state of the gslb vip Possible values: NONE, STATE_ONLY Default value: NS_GSLB_DONOT_CONSIDER_BKPS

soMethod

The spillover factor based on which the traffic will be given to the backupvserver once the main virtual server reaches the spillover threshold. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence

The state of the spillover persistence. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut

The spillover persistency entry timeout. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold

In case of CONNECTION (or) DYNAMICCONNECTION type spillover method this value is treated as Maximum number of connections a lb vserver will handle before spillover takes place. In case of BANDWIDTH type spillover method this value is treated as the amount of incoming and outgoing traffic (in Kbps) a Vserver will handle before spillover takes place. In case of HEALTH type spillover method if the percentage of active services (by weight) becomes lower than this value, spillover takes place Minimum value: 1 Maximum value: 4294967287

serviceName

The service for which the weight needs to be changed.

domainName

The name of the domain for which TTL and/or backupIP has to be changed.

comment

Comments associated with this virtual server.

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set gslb vserver gvip -persistenceType SOURCEIP

Top

unset gslb vserver

Synopsis

unset gslb vserver <name>@ [-backupVServer] [-dnsRecordType] [-lbMethod] [-backupLBMethod] [-netmask] [-v6netmasklen] [-tolerance] [-persistenceType] [-persistenceId] [-persistMask] [-v6persistmasklen] [-timeout] [-EDR] [-MIR] [-disablePrimaryOnDown] [-dynamicWeight] [-considerEffectiveState] [-soMethod] [-soPersistence] [-soPersistenceTimeOut] [-serviceName] [-weight] [-comment] [-appflowLog]

Description

Unset the backup virtual server or redirectURL set on the virtual server..Refer to the set gslb vserver command for meanings of the arguments.

Example

unset gslb vserver lb_vip -backupVServer
For multiple gslb vservers the command is:
unset gslb vserver lb_vip[1-3] -backupVServer

Top

bind gslb vserver

Synopsis

bind gslb vserver <name> [(-serviceName <string> [-weight <positive_integer>]) | (-domainName <string> [-TTL <secs>] [-backupIP <ip_addr|ipv6_addr|*>] [-cookieDomain <string>] [-cookieTimeout <mins>] [-sitedomainTTL <secs>])]

Description

Bind a domain or service to a GSLB vserver

Parameters

name

The vserver for which the binding operation is to be done

serviceName

The name of the service to be bound with the gslb vserver

domainName

The domain to be bound with this vserver

Example

bind gslb vserver gvip -domainName www.mynw.com

Top

unbind gslb vserver

Synopsis

unbind gslb vserver <name> [-serviceName <string> | (-domainName <string> [-backupIP] [-cookieDomain])]

Description

Unbind the domain or service from the gslb vserver

Parameters

name

The vserver for which the unbinding operation is to be performed

serviceName

The service to be unbound from the gslb vserver

domainName

The domain to be unbound from this vserver

Example

unbind gslb vserver gvip -domainName www.mynw.com

Top

enable gslb vserver

Synopsis

enable gslb vserver <name>@

Description

Enable a virtual server. Note: Virtual servers, when added, are enabled by default.

Parameters

name

The name of the virtual server to be enabled.

Example

enable gslb vserver gslb_vip
To enable multiple gslb vservers use the following command:
enable gslb vserver gslb_vip[1-3]

Top

disable gslb vserver

Synopsis

disable gslb vserver <name>@

Description

Disable (makes out of service) a virtual server.

Parameters

name

The name of the virtual server to be disabled. Notes: 1. The system still responds to ARP and/or ping requests for the IP address of this virtual server. 2. As the virtual server is still configured in the system, you can enable the virtual server using enable vserver CLI command.

Example

disable gslb vserver gslb_vip
To disable multiple gslb vservers use the following command:
disable gslb vserver gslb_vip[1-3]

Top

show gslb vserver

Synopsis

show gslb vserver [<name>] show gslb vserver stats - alias for 'stat gslb vserver'

Description

Display the GSLB virtual server attributes

Parameters

name

The name of the GSLB virtual server.

Example

show gslb vserver gvip

Top

stat gslb vserver

Synopsis

stat gslb vserver [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of a gslb vserver.

Parameters

name

The name of the gslb vserver for which statistics will be displayed. If not given statistics are shown for all gslb vservers.

Top

rename gslb vserver

Synopsis

rename gslb vserver <name>@ <newName>@

Description

Rename a global load balancing virtual server.

Parameters

name

The name of the global load balancing virtual server.

newName

The new name of the virtual server.

Example

rename gslb vserver gsl_vsvr gslb_vsvr_new

Top

gslb runningConfig

show gslb runningConfig

Synopsis

show gslb runningConfig

Description

Display the information pertaining to all the configuration that has been applied to the system, including settings that have not yet been saved to the system's ns.conf file using the save config command.

gslb domain

stat gslb domain

Synopsis

stat gslb domain [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of a gslb domain.

Parameters

name

The name of the gslb domain for which statistics will be displayed. If not given statistics are shown for all gslb domain.

gslb ldnsentries

[clear | show]

clear gslb ldnsentries

Synopsis

clear gslb ldnsentries

Description

Use this command to clear the ldns entries.

Top

show gslb ldnsentries

Synopsis

show gslb ldnsentries

Description

Displays the LDNS entries.

Example

show gslb ldnsentries

Top

gslb parameter

[set | unset | show]

set gslb parameter

Synopsis

set gslb parameter [-ldnsEntryTimeout <secs>] [-RTTTolerance <msecs>] [-ldnsMask <netmask>] [-v6ldnsmasklen <positive_integer>] [-ldnsProbeOrder <ldnsProbeOrder> ...] [-dropLdnsReq (ENABLED | DISABLED)]

Description

Set different GSLB parameters

Parameters

ldnsEntryTimeout

The idle timeout in seconds of the learnt LDNS entry. If no new DNS request is made within this interval, then the LDNS entry is aged out. Default value: 180 Maximum value: 65534

RTTTolerance

The RTT Tolerance in milli seconds. When the RTT is calculated for an LDNS entry, and if the difference between the old RTT and the newly computed one is less than or equal to the RTT Tolerance value, the network metric table is not updated with the new value for this LDNS entry. This is done to prevent exchange of metric when there is small variation in RTT. Default value: 5 Minimum value: 1 Maximum value: 100

ldnsMask

The Netmask. The Netmask specified here is used to store the LDNS IP addresses in the hash table and these are used in dynamic proximity-based GSLB Default value: 0xFFFFFFFF

v6ldnsmasklen

The V6 ldns mask prefix length. Default value: 128 Minimum value: 1 Maximum value: 128

ldnsProbeOrder

The order in which monitors should be initiated to calculate RTT. Possible values: PING, DNS, TCP Default value: ARRAY(0x99d8494)

dropLdnsReq

Drop LDNS requests if no RTT info available.Effective state will be not be considered when services are down or saturated too. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set gslb parameter -ldnsMask 255.255.0.0

Top

unset gslb parameter

Synopsis

unset gslb parameter [-ldnsEntryTimeout] [-RTTTolerance] [-ldnsMask] [-v6ldnsmasklen] [-ldnsProbeOrder] [-dropLdnsReq]

Description

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

Top

show gslb parameter

Synopsis

show gslb parameter

Description

Display the GSLB parameters

Example

show gslb parameter

Top

gslb ldnsentry

rm gslb ldnsentry

Synopsis

rm gslb ldnsentry <IPAddress>

Description

Removes the LDNS entry corresponding to the IP address given

Parameters

IPAddress

IP address of the LDNS server

Example

rm gslb ldnsentry 10.102.27.226

gslb config

sync gslb config

Synopsis

sync gslb config [-preview | -forceSync <string> | -command <string> | -nowarn | -saveconfig] [-debug]

Description

Synchronize the GSLB running configuration on all NetScalers participating in GSLB. The NetScaler on which this command is run is considered the "master node". All GSLB sites configured on the master, which do not have a parent, will be brought in sync with the master node.

Parameters

preview

Preview of the commands that are applied on the slave node. This won't initiate the gslb auto sync.

debug

A more verbose output of gslb auto sync.

forceSync

Forcibly sync the config from master to slave. The slave is identified with the sitename supplied as part of the argument. If the supplied argument is "all-sites", the config will be pushed to all slave nodes.

nowarn

Suppresses warning and confirmation prompt

saveconfig

Executes saveconfig on master prior to sync and after successful sync on slaves

command

Execute the command on master and then on all the slaves

Example

sync gslb config

gslb syncStatus

show gslb syncStatus

Synopsis

show gslb syncStatus

Description

Shows the status of the master and slave nodes configured for GSLB Auto Sync.

Parameters

response

gslb sync status as text blob

HA Commands

This group of commands can be used to perform operations on the following entities:

- HA node
- HA sync
- HA files
- HA failover

HA node

[add | rm | set | unset | bind | unbind | show | stat]

add HA node

Synopsis

add HA node <id> <IPAddress> [-inc (ENABLED | DISABLED)]

Description

Adds a peer node to a HA configuration. Each node must add the other as a peer. An algorithm determines which node becomes primary and which becomes secondary.

Parameters

id

A number that uniquely identifies the peer node. Minimum value: 1 Maximum value: 64

IPAddress

The NSIP or NSIP6 address of the node to be added for an HA configuration.

inc

When this mode is enabled, the following independent network entities and configurations are not propagated to the other node: MIPs, SNIPs, VLANs, routes (except LLB routes), route monitors, RNAT rules (except any RNAT rule with VIP as the NAT IP), dynamic routing configurations. Each node has its own. This option is required if the HA nodes reside on different networks. Possible values: ENABLED, DISABLED Default value: DISABLED

Top

rm HA node

Synopsis

rm HA node <id>

Description

Removes the peer node from the HA configuration. To completely remove both the nodes from the HA configuration, you have to log on to each node and remove its peer node.

Parameters

id

A number that uniquely identifies the peer node. To learn the ID of the peer node, you can run the show HA node command on the local node. Maximum value: 64

Top

set HA node

Synopsis

set HA node [-haStatus <haStatus>] [-haSync (ENABLED | DISABLED)] [-haProp (ENABLED | DISABLED)] [-helloInterval <msecs>] [-deadInterval <secs>] [-failSafe (ON | OFF)]

Description

Sets the specified parameters for the node. The settings are not shared with the other HA node.

Parameters

id

A number that uniquely identifies the peer node. Maximum value: 64

haStatus

The HA status of the node. The HA status STAYSECONDARY is used to force the secondary device stay as secondary independent of the state of the Primary device. For example, in an existing HA setup, the Primary node has to be upgraded and this process would take few seconds. During the upgradation, it is possible that the Primary node may suffer from a downtime for a few seconds. However, the Secondary should not take over as the Primary node. Thus, the Secondary node should remain as Secondary even if there is a failure in the Primary node. STAYPRIMARY configuration keeps the node in primary state in case if it is healthy, even if the peer node was the primary node initially. If the node with STAYPRIMARY setting (and no peer node) is added to a primary node (which has this node as the peer) then this node takes over as the new primary and the older node becomes secondary. ENABLED state means normal HA operation without any constraints/preferences. DISABLED state disables the normal HA operation of the node. Possible values: ENABLED, STAYSECONDARY, DISABLED, STAYPRIMARY

haSync

Automatically maintain synchronization by duplicating the configuration of the primary node on the secondary node. This setting is not propagated. Automatic synchronization requires this setting be enabled (the default) on each node. Synchronization uses port 3010. Possible values: ENABLED, DISABLED Default value: ENABLED

haProp

Automatically propagate all commands from the primary to the secondary node, except the following: All HA configuration related commands. For example, add ha node, set ha node, and bind ha node. All Interface related commands. For example, set interface and unset interface. All channels related commands. For example, add channel, set channel, and bind channel. The propagated command is executed on the secondary node before it is executed on the primary. If command propagation fails, or if command execution fails on the secondary, the primary node executes the command and logs an error. Command propagation uses port 3010. Note: After reenabling propagation, remember to run force synchronization on either node. Possible values: ENABLED, DISABLED Default value: ENABLED

helloInterval

The interval, in milliseconds, between heartbeat messages sent to the peer node.The heartbeat messages are UDP packets sent to port 3003 of the peer node. Default value: 200 Minimum value: 200 Maximum value: 1000

deadInterval

The number of seconds after which a peer node is marked DOWN if heartbeat messages are not received from the peer node. Default value: 3 Minimum value: 3 Maximum value: 60

failSafe

Keep one node primary if both nodes fail the health check,so that a partially available node can back up data and handle traffic as well as possible. This mode is set independently on each node. Possible values: ON, OFF Default value: OFF

Top

unset HA node

Synopsis

unset HA node [-haStatus] [-haSync] [-haProp] [-helloInterval] [-deadInterval] [-failSafe]

Description

Use this command to remove HA node settings.Refer to the set HA node command for meanings of the arguments.

Top

bind HA node

Synopsis

bind HA node [<id>] (-routeMonitor <ip_addr|ipv6_addr|*> [<netmask>])

Description

Adds a route monitor to the local node. When a NetScaler appliance has only static routes for reaching a network, and you want to create a route monitor for the network, you must enable monitored static routes (MSR) for the static routes. Route Monitors are supported both in non-INC and INC mode.

Parameters

id

A number that uniquely identifies the local node. The ID of the local node is always 0. Maximum value: 64

routeMonitor

Route Monitor

Top

unbind HA node

Synopsis

unbind HA node [<id>] (-routeMonitor <ip_addr|ipv6_addr|*> [<netmask>])

Description

Removes a route monitor entry from the local node. The NetScaler appliance stops monitoring the route in its internal routing table.

Parameters

id

A number that uniquely identifies the local node. The ID of the local node is always 0. Maximum value: 64

routeMonitor

The route specified in the route monitor entry that you want to remove from the NetScaler appliance. It can be an IPv4 address or network, or an IPv6 address or network

prefix.

Top

show HA node

Synopsis

show HA node [<id>]

Description

Displays the HA settings of both nodes or, if you specify a node, just the specified node.

Parameters

id

The ID of the node whose HA settings you want to display. (The ID of the local node is always 0.) Maximum value: 64

Example

An example of the command's output is as follows:
2 configured nodes:
1) Node ID: 0 IP: 192.168.100.5 Primary node
2) Node ID: 2 IP: 192.168.100.112 Secondary node

Top

stat HA node

Synopsis

stat HA node [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display the statistics related to HA configuration.

Top

HA sync

force HA sync

Synopsis

force HA sync [-force [-save (YES | NO)]]

Description

Forces duplication of the primary node's configurationon the secondary node. Can be initiated from either node. Note: This command fails if synchronization is already in progress, the secondary node is disabled, synchronization is disabled on either node, or you enter the command on a standalone appliance.

Parameters

force

Force synchronization regardless of the state of HA propagation and HA synchronization on either node.

save

After synchronization, automatically save the configuration in the secondary node's configuration file (ns.conf) without prompting for confirmation. Possible values: YES, NO Default value: VAL_NOT_SET

Example

Can be used in following formats:

>force sync <cr>
>force sync -force <cr>
>force sync -force -save [yes|no]<cr>

HA files

sync HA files

Synopsis

sync HA files [<Mode> ...]

Description

Synchronize various configuration files from the primary node to the secondary. You can run this command from either node.Files that are present on only the secondary and are specific to the secondary are not deleted. This command fails on a standalone system or with the secondary node disabled.

Parameters

Mode

Specify one of the following modes of synchronization. all. Synchronize files related to system configuration, Access GatewaySpecify one of the following modes of synchronization. all. Synchronize files related to system configuration, Access Gateway bookmarks, SSL certificates, SSL CRL lists, HTML injection scripts, and Application Firewall XML objects. bookmarks. Synchronize all Access GatewaySpecify one of the following modes of synchronization. all. Synchronize files related to system configuration, Access Gateway bookmarks, SSL certificates, SSL CRL lists, HTML injection scripts, and Application Firewall XML objects. bookmarks. Synchronize all Access Gateway bookmarks. ssl. Synchronize all certificates, keys, and CRLs for the SSL feature. htmlinjection. Synchronize all scripts configured for the HTML injection feature. imports. Synchronize all XML objects (for example, WSDLs, schemas, error pages) configured for the Application Firewall. misc. Synchronize all license files and the rc.conf file. all_plus_misc. Synchronize files related to system configuration, Access Gateway bookmarks, SSL certificates, SSL CRL lists, HTML injection scripts, Application Firewall XML objects, licenses, and the rc.conf file.

Example

sync files all

HA failover

force HA failover

Synopsis

force HA failover [-force]

Description

Forces an HA failover. Can be initiated from either node. A forced failover is not propagated or synchronized. This commandfails if the secondary is disabled or configured to remain secondary, the primary is configured to remain primary, the state of the peer node is unknown, or you run the command on a standalone appliance.

Parameters

force

Force a failover without prompting for confirmation.

IPSec Commands

This group of commands can be used to perform operations on the following entities:

- ipsec profile
- ipsec parameter
- ipsec counters

ipsec profile

[add | show | rm]

add ipsec profile

Synopsis

add ipsec profile <name> [-encAlgo (AES | 3DES) ...] [-hashAlgo <hashAlgo> ...] [-lifetime <positive_integer>] (-psk | (-publickey <string> -privatekey <string> -peerPublicKey <string>)) [-livenessCheckInterval <positive_integer>] [-retransmissiontime <positive_integer>]

Description

Add an ipsec profile.

Parameters

name

The name of the ipsec profile

encAlgo

Type of encryption algorithm

hashAlgo

Type of hashing algorithm

lifetime

Lifetime of SA in seconds Minimum value: 60 Maximum value: 31536000

psk

Pre shared key value

publickey

Public key file path

livenessCheckInterval

Number of seconds after which a notify payload is sent to check the liveliness of the peer. Additional retries are done as per retransmit interval setting. Zero value disables

liveliness checks. Maximum value: 64999

retransmissiontime

The interval in seconds to retry sending the IKE messages to peer, three consecutive attempts are done with doubled interval after every failure. Minimum value: 1 Maximum value: 99

Top

show ipsec profile

Synopsis

show ipsec profile [<name>]

Description

Display all of the configured ipsec peers

Parameters

name

The name of the ipsec profile

Example

show ipsec profile

Top

rm ipsec profile

Synopsis

rm ipsec profile <name>

Description

Remove an ipsec peer

Parameters

name

The name of the ipsec profile.

Example

rm ipsec profile

Top

ipsec parameter

[set | unset | show]

set ipsec parameter

Synopsis

set ipsec parameter [-encAlgo (AES | 3DES) ...] [-hashAlgo <hashAlgo> ...] [-lifetime <positive_integer>] [-livenessCheckInterval <positive_integer>] [-retransmissiontime <positive_integer>]

Description

Set global parameters for IPSEC

Parameters

encAlgo

Type of encryption algorithm Default value: ENC_AES

hashAlgo

Type of hashing algorithm Default value: HMAC_SHA256

lifetime

Lifetime of SA in seconds Minimum value: 60 Maximum value: 31536000

livenessCheckInterval

Number of seconds after which a notify payload is sent to check the liveliness of the peer. Additional retries are done as per retransmit interval setting. Zero value disables liveliness checks. Maximum value: 64999

retransmissiontime

The interval in seconds to retry sending the IKE messages to peer, three consecutive attempts are done with doubled interval after every failure., increases for every retransmit till 6 retransmits. Minimum value: 1 Maximum value: 99

Top

unset ipsec parameter

Synopsis

unset ipsec parameter [-encAlgo] [-hashAlgo] [-lifetime] [-livenessCheckInterval] [-retransmissiontime]

Description

Set global parameters for IPSEC.Refer to the set ipsec parameter command for meanings of the arguments.

Top

show ipsec parameter

Synopsis

show ipsec parameter

Description

Show global parameters for IPSEC

Top

ipsec counters

stat ipsec counters

Synopsis

stat ipsec counters [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics for secure tunnel sessions.

Example

stat ipsec

LB Commands

This group of commands can be used to perform operations on the following entities:

- lb monitor
- lb route
- lb route6
- lb vserver
- lb metricTable
- lb monbindings
- lb persistentSessions
- lb group
- lb sipParameters
- lb parameter

lb monitor

[add | rm | set | unset | enable | disable | bind | unbind | show]

add lb monitor

Synopsis

add lb monitor <monitorName> <type> [-action <action>] [-respCode <int[-int]> ...] [-httpRequest <string>] [-rtspRequest <string>] [-customHeaders <string>] [-maxForwards <positive_integer>] [-sipMethod <sipMethod>] [-sipURI <string>] [-sipregURI <string>] [-send <string>] [-recv <string>] [-query <string>] [-queryType <queryType>] [-scriptName <string>] [-scriptArgs <string>] [-dispatcherIP <ip_addr>] [-dispatcherPort <port>] [-userName <string>] {-password } {-secondaryPassword } [-logonpointName <string>] [-lasVersion <string>] {-radKey } [-radNASid <string>] [-radNASip <ip_addr>] [-LRTM (ENABLED | DISABLED)] [-deviation <positive_integer> [<units>]] [-interval <integer> [<units>]] [-resptimeout <integer> [<units>]] [-resptimeoutThresh <positive_integer>] [-retries <integer>] [-failureRetries <integer>] [-alertRetries <integer>] [-successRetries <integer>] [-downTime <integer> [<units>]] [-destIP <ip_addr|ipv6_addr>] [-destPort <port>] [-state (ENABLED | DISABLED)] [-reverse (YES | NO)] [-transparent (YES | NO)] [-ipTunnel (YES | NO)] [-tos (YES | NO)] [-tosId <positive_integer>] [-secure (YES | NO)] [-validateCred (YES | NO)] [-domain <string>] [-IPAddress <ip_addr|ipv6_addr|*> ...] [-group <string>] [-fileName <string>] [-baseDN <string>] [-bindDN <string>] [-filter <string>] [-attribute <string>] [-database <string>] [-sqlQuery <text>] [-evalRule <expression>] [-mssqlProtocolVersion <mssqlProtocolVersion>] [-snmpOID <string>] [-snmpCommunity <string>] [-snmpThreshold <string>] [-snmpVersion (V1 | V2)] [-metricTable <string>] [-application <string>] [-sitePath <string>] [-netProfile <string>] [-originHost <string>] [-originRealm <string>] [-hostIPAddress <ip_addr|ipv6_addr|*>] [-vendorId <positive_integer>] [-productName <string>] [-firmwareRevision <positive_integer>] [-authApplicationId <positive_integer> ...] [-acctApplicationId <positive_integer> ...] [-inbandSecurityId (NO_INBAND_SECURITY | TLS)] [-supportedVendorIds <positive_integer> ...] [-vendorSpecificVendorId <positive_integer> [-vendorSpecificAuthApplicationIds <positive_integer> ...] [-vendorSpecificAcctApplicationIds <positive_integer> ...]]

Description

Add a monitor to the system.

Parameters

monitorName

The name of the monitor.

type

The type of monitor. Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, MYSQL-ECV, MSSQL-ECV, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, CITRIX-WI-EXTENDED, DIAMETER

action

The action to be taken in INLINE monitors. Possible values: NONE, LOG, DOWN Default value: SM_DOWN

respCode

The response codes. For the probe to succeed, the HTTP/RADIUS response from the server must be of one of the types specified.

httpRequest

The HTTP request that is sent to the server (for example, "HEAD /file.html").

rtspRequest

The RTSP request that is sent to the server (for example, "OPTIONS *").

customHeaders

The custom header string, attached to the monitoring probes.

maxForwards

SIP packet max-forwards Default value: 1 Maximum value: 255

sipMethod

SIP method to be used for the query Possible values: OPTIONS, INVITE, REGISTER

sipURI

SIP method string, sent to the server. For example "OPTIONS sip:sip.test".

sipregURI

SIP user to be registered

send

The string that is sent to the service. Applicable to TCP-ECV, HTTP-ECV, and UDP-ECV monitor types.

recv

The string that is expected from the server to mark the server as UP. Applicable to TCP-ECV, HTTP-ECV, and UDP-ECV monitor types.

query

The DNS query (domain name) sent to the DNS service that is being monitored.

queryType

The type of DNS query that is sent. Possible values: Address, Zone, AAAA

scriptName

The path and name of the script to execute.

scriptArgs

The string that are put in the POST data - they are copied to the request verbatim.

dispatcherIP

The IP Address of the dispatcher to which the probe is sent.

dispatcherPort

The port of the dispatcher to which the probe is sent.

userName

Username on the RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/MSSQL/POP3/CITRIX-AG/CITRIX-XD-DDC/CITRIX-WI-EXTENDED server. This user name is used in the probe.

password

Password used in RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/LDAP/CITRIX-AG/CITRIX-XD-DDC/CITRIX-WI-EXTENDED server monitoring.

secondaryPassword

Secondary password used in Access Gateway server monitoring.

logonpointName

Logonpoint name used in Citrix AAC login page and logon agent service monitoring.

lasVersion

The version of the Citrix AAC logon agent service required by CITRIX-AAC-LAS monitor.

radKey

The radius key.

radNASid

The NAS ID to be used in Radius monitoring.

radNASip

The NAS IP to be used in Radius monitoring.

LRTM

The state of response time calculation of probes. Possible values: ENABLED, DISABLED

deviation

Deviation from the learnt response time for Dynamic Response Time monitoring. The maximum value is 20939000 in milliseconds , 20939 in seconds and 348 in minutes. Maximum value: 20939000

interval

The frequency at which the probe is sent to a service.The interval should be greater than the response timeout. The minimum value is 20 msec.The maximum value is 20940000 in milliseconds , 20940 in seconds and 349 in minutes Default value: 5 Minimum value: 1 Maximum value: 20940000

resptimeout

The interval for which the system waits before it marks the probe as FAILED. The response timeout should be less than the value specified in -interval parameter. The UDP-ECV monitor type does not decide the probe failure by the response timeout. System considers the probe successful for UDP-ECV monitor type, when the server response matches the criteria set by the -send and -recv options or if the response is not received from the server (unless the -reverse option is set to yes). Note: The -send option specifies what data is to be sent to the server in the probe and -recv specifies the server response criteria for the probe to succeed. The probe failure is caused by the ICMP port unreachable error from the service. The minimum value is 10 msec. The maximum value is 20939000 in milliseconds , 20939 in seconds and 348 in minutes Default value: 2 Minimum value: 1 Maximum value: 20939000

resptimeoutThresh

Monitor response timeout threshold , a trap will be sent if the response time for the monitoring probes exceeds the thereshold. It is given in percentage. Maximum value: 100

retries

The maximum number of most recent probes considered to decide whether to mark the service as DOWN. Minimum value of retries is 1. Default value: 3 Minimum value: 1 Maximum value: 127

failureRetries

The number of failed probes out of most recent "retries" number of probes required to mark the service as DOWN. By default, the system requires "retries" number of consecutive probe failures to mark the service as DOWN. Maximum value: 32

alertRetries

The number of probes failures after which the system generates a snmp trap. Maximum value: 32

successRetries

The number of consecutive sucessful probes required to mark the service as UP. Default value: 1 Minimum value: 1 Maximum value: 32

downTime

The duration for which the system waits to make the next probe once the service is marked as DOWN. The minimum value is 10 msec. The maximum value is 20939000 in milliseconds , 20939 in seconds and 348 in minutes Default value: 30 Minimum value: 1 Maximum value: 20939000

destIP

The IP address to which the probe is sent. If the destination IP address is set to 0, the destination IP address is that of the server to which the monitor is bound.

destPort

The TCP/UDP port to which the probe is sent. If the destination port is set to 0, the destination port is of the service to which the monitor is bound. For a USER monitor, however, this will be the port sent in the HTTP request to the dispatcher. This option is ignored if the monitor is of the PING type.

state

The state of the monitor. If the monitor is disabled, this monitor-type probe is not sent for all services. If the monitor is bound, the state of this monitor is not taken into account when the service of this state is determined. Possible values: ENABLED, DISABLED Default value: ENABLED

reverse

The state of reverse probe's criterion check. Possible values: YES, NO Default value: NO

transparent

The state of the monitor for transparent devices, such as firewalls, based on the responsiveness of the services behind them. If the monitoring of transparent devices is enabled, the destination IP address should be specified. The probe is sent to the specified destination IP address using the MAC address of the transparent device. Possible values: YES, NO Default value: NO

ipTunnel

The state of the monitor for tunneled devices. If the monitoring of tunneled devices is enabled, the destination IP address should be specified. The probe is sent to the specified destination IP address by tunneling it to the device. Possible values: YES, NO Default value: NO

tos

If enabled, the probe is sent to the service by encoding the specified destination IP address in the IP TOS (6)bits. Possible values: YES, NO

tosId

Use this parameter to specify the TOS ID of the specified destination IP. Applicable only when the -tos is enabled Minimum value: 1 Maximum value: 63

secure

The state of the secure monitoring of services. SSL handshake will be done on the TCP connection established. Applicable only for TCP based monitors. This option can't be used in conjuction with CITRIX-AG monitor as this monitor is a secure monitor by default. Possible values: YES, NO Default value: NO

validateCred

Setting this field causes the monitor to send probe which validate the credentials of the Xen Desktop DDC. Possible values: YES, NO Default value: NO

domain

Domain name required by the monitors. This is for the Xen Desktop DDC monitor to validate the credentials and CITRIX-WI-EXTENDED monitor for logon process.

IPAddress

List of IP address to be checked against the response to the DNS monitoring probe. Applicable only to the DNS monitors.

group

Group name to be queried for NNTP monitor.

fileName

File name to be used for FTP-EXTENDED monitor.

baseDN

Base name for the LDAP monitor.

bindDN

BDN name for the LDAP monitor.

filter

Filter for the LDAP monitor.

attribute

Attribute for the LDAP monitor.

database

Database to be used for the MYSQL/MSSQL monitor.

sqlQuery

SQL query to be used for the MYSQL/MSSQL monitor.

evalRule

Rule evaluated to determine the state of MYSQL/MSSQL monitor.

mssqlProtocolVersion

Protocol Version used by MSSQL monitor Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2 Default value: TDS_PROT_70

snmpOID

OID to be used for the SNMP monitor.

snmpCommunity

Community to be used for the SNMP monitor.

snmpThreshold

Threshold to be used for the SNMP monitor.

snmpVersion

SNMP version to be used for LOAD monitoring. Possible values: V1, V2

metricTable

Metric table to use for the metrics that are going to be bound.

application

Name of the application that has to be executed to check the state of the service

sitePath

URL of the logon page. To get the dynamic page under sitepath, this sitepath must be specified ending with "/".

netProfile

The name of the network profile.

originHost

Origin Host to be put in CER message.

originRealm

Origin realm to be put in CER message.

hostIPAddress

Host IP Address to be put in CER message.

vendorId

Vendor ID to be put in CER message.

productName

Product Name to be put in CER message.

firmwareRevision

FIRMWARE-REVISION to be put in CER message.

authApplicationId

list of Auth-Application-Ids to be put in CER message. maximum 8 such auth application id are supported in monitoring message. Maximum value: 4294967295

acctApplicationId

list of ACCT-APPLICATION-IDs to be put in CER message. maximum 8 such acct application id are supported in monitoring message. Maximum value: 4294967295

inbandSecurityId

INBAND-SECURITY-ID to be put in CER message. Possible values: NO_INBAND_SECURITY, TLS

supportedVendorIds

list of SUPPORTED-VENDOR-ID to be put in CER message. maximum 8 such supported Vendor id are supported in monitoring message. Minimum value: 1 Maximum value: 4294967295

vendorSpecificVendorId

Vendor Id to be used in Vendor-Specific-Application-Id in monitoring CER message. Only 1 such vendor id is supported. Minimum value: 1

Example

add monitor http_mon http

Top

rm lb monitor

Synopsis

rm lb monitor <monitorName> <type> [-respCode <int[-int]> ...]

Description

Remove either a specified monitor or response code for the HTTP monitor. While the response codes for a specified monitor are removed, the monitor itself is not removed. Built-in monitors can not be removed.

Parameters

monitorName

The name of the monitor.

type

The type of monitor. Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, MYSQL-ECV, MSSQL-ECV, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, CITRIX-WI-EXTENDED, DIAMETER

respCode

The response codes to be deleted from the response codes list of the HTTP monitor.

Example

rm monitor http_mon http

Top

set lb monitor

Synopsis

set lb monitor <monitorName> <type> [-action <action>] [-respCode <int[-int]> ...] [-httpRequest <string>] [-rtspRequest <string>] [-customHeaders <string>] [-maxForwards <positive_integer>] [-sipMethod <sipMethod>] [-sipregURI <string>] [-sipURI <string>] [-send <string>] [-recv <string>] [-query <string>] [-queryType <queryType>] [-userName <string>] {-password } {-secondaryPassword } [-logonpointName <string>] [-lasVersion <string>] {-radKey } [-radNASid <string>] [-radNASip <ip_addr>] [-LRTM (ENABLED | DISABLED)] [-deviation <positive_integer> [<units>]] [-scriptName <string>] [-scriptArgs <string>] [-validateCred (YES | NO)] [-domain <string>] [-dispatcherIP <ip_addr>] [-dispatcherPort <port>] [-interval <integer> [<units>]] [-resptimeout <integer> [<units>]] [-resptimeoutThresh <positive_integer>] [-retries <integer>] [-failureRetries <integer>] [-alertRetries <integer>] [-successRetries <integer>] [-downTime <integer> [<units>]] [-destIP <ip_addr|ipv6_addr>] [-destPort <port>] [-state (ENABLED | DISABLED)] [-reverse (YES | NO)] [-transparent (YES | NO)] [-ipTunnel (YES | NO)] [-tos (YES | NO)] [-tosId <positive_integer>] [-secure (YES | NO)] [-IPAddress <ip_addr|ipv6_addr|*> ...] [-group <string>] [-fileName <string>] [-baseDN <string>] [-bindDN <string>] [-filter <string>] [-attribute <string>] [-database <string>] [-sqlQuery <text>] [-evalRule <expression>] [-snmpOID <string>] [-snmpCommunity <string>] [-snmpThreshold <string>] [-snmpVersion (V1 | V2)] [-metricTable <string>] [-metric <string> [-metricThreshold <positive_integer>] [-metricWeight <positive_integer>]] [-application <string>] [-sitePath <string>] [-netProfile <string>] [-mssqlProtocolVersion <mssqlProtocolVersion>] [-originHost <string>] [-originRealm <string>] [-hostIPAddress <ip_addr|ipv6_addr|*>] [-vendorId <positive_integer>] [-productName <string>] [-firmwareRevision <positive_integer>] [-authApplicationId <positive_integer> ...] [-acctApplicationId <positive_integer> ...] [-inbandSecurityId (NO_INBAND_SECURITY | TLS)] [-supportedVendorIds <positive_integer> ...] [-vendorSpecificVendorId <positive_integer> [-vendorSpecificAuthApplicationIds <positive_integer> ...] [-vendorSpecificAcctApplicationIds <positive_integer> ...]]

Description

Use this command to modify the parameters of a specific monitor.

Parameters

monitorName

The name of the monitor that is being set.

type

The type of monitor. Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, MYSQL-ECV, MSSQL-ECV, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, CITRIX-WI-EXTENDED, DIAMETER

action

The action to be taken in INLINE monitors. Possible values: NONE, LOG, DOWN Default value: SM_DOWN

respCode

The response codes.

httpRequest

The HTTP request that is sent to the server.

rtspRequest

The RTSP request that is sent to the server (for example, "OPTIONS *").

customHeaders

The string that is sent to the service. Applicable to HTTP and HTTP-ECV monitor types.

maxForwards

SIP packet max-forwards Default value: 1 Maximum value: 255

sipMethod

SIP method to be used for the query Possible values: OPTIONS, INVITE, REGISTER

sipURI

SIP uri string, sent to the server. For example "sip:sip.test".

send

The string that is sent to the service.

recv

The string that is expected from the server to mark the server as UP.

query

The DNS query (domain name) sent to the DNS service that is being monitored.

queryType

The type of DNS query that is sent. Possible values: Address, Zone, AAAA

userName

Username on the RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/MSSQL/POP3/CITRIX-AG/CITRIX-XD-DDC/CITRIX-WI-EXTENDED server. This user name is used in the probe.

password

Password used in RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/LDAP/CITRIX-AG/CITRIX-XD-DDC/CITRIX-WI-EXTENDED server monitoring.

secondaryPassword

Secondary password used in Access Gateway server monitoring.

logonpointName

Logonpoint name used in Citrix AAC login page and logon agent service monitoring.

lasVersion

The version of the Citrix AAC logon agent service required by CITRIX-AAC-LAS monitor.

radKey

The radius key.

radNASid

The NAS ID to be used in Radius monitoring.

radNASip

The NAS IP to be used in Radius monitoring.

LRTM

The state of response time calculation of probes. Possible values: ENABLED, DISABLED

deviation

Deviation from the learnt response time for Dynamic Response Time monitoring. The maximum value is 20939000 in milliseconds , 20939 in seconds and 348 in minutes. Maximum value: 20939000

scriptName

The path and name of the script to execute.

scriptArgs

The string that are put in the POST data - they are copied to the request verbatim.

validateCred

Setting this field triggers the monitor to send probe which validate the credentials of the Xen Desktop DDC. Possible values: YES, NO Default value: NO

domain

Domain name required by the monitors. This is for the Xen Desktop DDC monitor to validate the credentials and CITRIX-WI-EXTENDED monitor for logon process.

dispatcherIP

The IP Address of the dispatcher to which the probe is sent.

dispatcherPort

The port of the dispatcher to which the probe is sent.

interval

The frequency at which the probe is sent to the service.The minimum value is 20 msec.The maximum value is 20940000 in milliseconds , 20940 in seconds and 349 in minutes Default value: 5 Minimum value: 1 Maximum value: 20940000

resptimeout

The interval for which the system waits before it marks the probe as FAILED. The minimum value is 10 msec. The maximum value is 20939000 in milliseconds , 20939 in seconds and 348 in minutes. Default value: 2 Minimum value: 1 Maximum value: 20939000

resptimeoutThresh

Monitor response timeout threshold , a trap will be sent if the response time for the monitoring probes exceeds the thereshold. It is given in percentage. Maximum value: 100

retries

The maximum number of most recent probes considered to decide whether to mark the service as DOWN. Minimum value of retries is 1. Default value: 3 Minimum value: 1 Maximum value: 127

failureRetries

The number of failed probes out of most recent "retries" number of probes required to mark the service as DOWN. By default, the system requires "retries" number of consecutive probe failures to mark the service as DOWN. Maximum value: 32

alertRetries

The number of probes failures after which the system generates a snmp trap. Maximum value: 32

successRetries

The number of consecutive sucessful probes required to mark the service as UP. Default value: 1 Minimum value: 1 Maximum value: 32

downTime

The duration for which the system waits to make the next probe once the service is marked as DOWN. The minimum value is 10 msec. The maximum value is 20939000 in milliseconds , 20939 in seconds and 348 in minutes Default value: 30 Minimum value: 1 Maximum value: 20939000

destIP

The IP address to which the probe is sent.

destPort

The TCP/UDP port to which the probe is sent.

state

The state of the monitor. Possible values: ENABLED, DISABLED Default value: ENABLED

reverse

The state of reverse probe's criterion check. Possible values: YES, NO Default value: NO

transparent

The state of the monitor for transparent devices. Possible values: YES, NO Default value: NO

ipTunnel

The state of the monitor for tunneled devices. Possible values: YES, NO Default value: NO

tos

If enabled, the probe is sent to the service by encoding the specified destination IP address in the IP TOS (6)bits. Possible values: YES, NO

tosId

Use this parameter to specify the TOS ID of the specified destination IP. Applicable only when the -tos is enabled Minimum value: 1 Maximum value: 63

secure

The state of the secure monitoring of services. Possible values: YES, NO Default value: NO

IPAddress

List of IP address to be checked against the response to the DNS monitoring probe. Applicable only to the DNS monitors.

group

Group name to be queried for NNTP monitor.

fileName

File name to be used for FTP-EXTENDED monitor.

baseDN

Base name for the LDAP monitor.

bindDN

BDN name for the LDAP monitor.

filter

Filter for the LDAP monitor.

attribute

Attribute for the LDAP monitor.

database

Database to be used for the MYSQL/MSSQL monitor.

sqlQuery

SQL query to be used for the MYSQL/MSSQL monitor.

evalRule

Rule evaluated to determine the state of MYSQL/MSSQL monitor.

snmpOID

OID to be used for the SNMP monitor.

snmpCommunity

Community to be used for the SNMP monitor.

snmpThreshold

Threshold to be used for the SNMP monitor.

snmpVersion

SNMP version to be used for SNMP monitoring. Possible values: V1, V2

metricTable

Metric table to use for the metrics that are going to be bound.

metric

Metric name in the metric table, whose setting is changed. A value zero disables the metric and it will not be used for load calculation

application

Name of the application that has to be executed to check the state of the service

sitePath

URL of the logon page. To get the dynamic page under sitepath, this sitepath must be specified ending with "/".

netProfile

The name of the network profile.

mssqlProtocolVersion

Protocol Version used by MSSQL monitor Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2 Default value: TDS_PROT_70

originHost

Origin Host to be put in CER message.

originRealm

Origin realm to be put in CER message.

hostIPAddress

Host IP Address to be put in CER message.

vendorId

Vendor ID to be put in CER message.

productName

Product Name to be put in CER message.

firmwareRevision

FIRMWARE-REVISION to be put in CER message.

authApplicationId

list of Auth-Application-Ids to be put in CER message. maximum 8 such auth application id are supported in monitoring message. Maximum value: 4294967295

acctApplicationId

list of ACCT-APPLICATION-IDs to be put in CER message. maximum 8 such acct application id are supported in monitoring message. Maximum value: 4294967295

inbandSecurityId

INBAND-SECURITY-ID to be put in CER message. Possible values: NO_INBAND_SECURITY, TLS

supportedVendorIds

list of SUPPORTED-VENDOR-ID to be put in CER message. maximum 8 such supported Vendor id are supported in monitoring message. Minimum value: 1 Maximum value: 4294967295

vendorSpecificVendorId

Vendor Id to be used in Vendor-Specific-Application-Id in monitoring CER message. Only 1 such vendor id is supported. Minimum value: 1

Example

set monitor http_mon http -respcode 100

Top

unset lb monitor

Synopsis

unset lb monitor <monitorName> <type> [-IPAddress <ip_addr|ipv6_addr|*> ...] [-scriptName] [-destPort] [-netProfile] [-action] [-respCode] [-httpRequest] [-rtspRequest] [-customHeaders] [-maxForwards] [-sipMethod] [-sipregURI] [-send] [-recv] [-query] [-queryType] [-userName] [-password] [-secondaryPassword] [-logonpointName] [-lasVersion] [-radKey] [-radNASid] [-radNASip] [-LRTM] [-deviation] [-scriptArgs] [-validateCred] [-domain] [-dispatcherIP] [-dispatcherPort] [-interval] [-resptimeout] [-resptimeoutThresh] [-retries] [-failureRetries] [-alertRetries] [-successRetries] [-downTime] [-destIP] [-state] [-reverse] [-transparent] [-ipTunnel] [-tos] [-tosId] [-secure] [-group] [-fileName] [-baseDN] [-bindDN] [-filter] [-attribute] [-database] [-sqlQuery] [-evalRule] [-snmpOID] [-snmpCommunity] [-snmpThreshold] [-snmpVersion] [-metricTable] [-mssqlProtocolVersion] [-originHost] [-originRealm] [-hostIPAddress] [-vendorId] [-productName] [-firmwareRevision] [-authApplicationId] [-acctApplicationId] [-inbandSecurityId] [-supportedVendorIds] [-vendorSpecificVendorId] [-vendorSpecificAuthApplicationIds] [-vendorSpecificAcctApplicationIds]

Description

Use this command to modify the parameters of a specific monitor..Refer to the set lb monitor command for meanings of the arguments.

Example

set monitor dns_mon dns -ipaddress 10.102.27.230

Top

enable lb monitor

Synopsis

enable lb monitor (<serviceName>@ | <serviceGroupName>@) [<monitorName>]

Description

Enable the monitor that is bound to a specific service. If no monitor name is specified, all monitors bound to the service are enabled.

Parameters

serviceName

The name of the service to which the monitor is bound.

serviceGroupName

The name of the service group to which the monitor is to be bound.

monitorName

The name of the monitor.

Example

enable monitor http_svc http_mon
To enable monitor for multiple services use the following command:
enable monitor http_svc[1-3] http_mon

Top

disable lb monitor

Synopsis

disable lb monitor (<serviceName>@ | <serviceGroupName>@) [<monitorName>]

Description

Disable the monitor for a service. If the monitor name is not specified, all monitors bound to the service are disabled.

Parameters

serviceName

The name of the service being monitored.

serviceGroupName

The name of the service group being monitored.

monitorName

The name of the monitor.

Example

disable monitor http_svc http_mon
To disable a monitor on multiple services use the following command:
disable monitor http_svc[1-3] http_mon

Top

bind lb monitor

Synopsis

bind lb monitor <monitorName> [-state (ENABLED | DISABLED)] [-weight <positive_integer>] [-state (ENABLED | DISABLED)] [-weight <positive_integer>] [-metric <string> -metricThreshold <positive_integer> [-metricWeight <positive_integer>]]

Description

Use this command to bind a monitor to a service. Multiple monitors can be bound to the service. The server's state is determined by the state of all the bound monitors using the AND condition. All monitor's probes have to succeed for the service to be in the UP state.

Parameters

monitorName

The name of the monitor to be bound.

serviceName

The name of the service or a service group to which the monitor is to be bound.

serviceGroupName

The name of the service group to which the monitor is to be bound.

metric

The name of the metric from the table to be used for this monitor.

Example

bind monitor http_mon http_svc
To bind a monitor to multiple services use the following command:
bind monitor http_mon http_svc[1-3]

Top

unbind lb monitor

Synopsis

unbind lb monitor <monitorName> -metric <string>

Description

Use this command to unbind a specified monitor from the service.

Parameters

monitorName

The name of the monitor to be unbound.

serviceName

The service name from which the monitor is to be unbound.

serviceGroupName

The service group name from which the monitor is to be unbound.

metric

The name of the metric from the table to be used for this monitor.

Example

unbind monitor http_mon http_svc
To unbind a monitor to multiple services use the following command:
unbind monitor http_mon http_svc[1-3]

Top

show lb monitor

Synopsis

show lb monitor [<monitorName>] [<type>] show lb monitor bindings - alias for 'show lb monbindings'

Description

Display the parameters for the specified monitor. If the monitor_name argument is not specified, a list of all existing monitors is returned.

Parameters

monitorName

The name of the monitor.

type

The type of monitor. Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, MYSQL-ECV, MSSQL-ECV, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, CITRIX-WI-EXTENDED, DIAMETER

Example

An example of the show monitor command output is as follows:

```
8 configured monitors:
1)  Name.......:         ping  Type......:     PING   State....ENABLED
2)  Name.......:          tcp  Type......:      TCP   State....ENABLED
3)  Name.......:         http  Type......:     HTTP   State....ENABLED
4)  Name.......:      tcp-ecv  Type......:   TCP-ECV   State....ENABLED
5)  Name.......:     http-ecv  Type......:  HTTP-ECV   State....ENABLED
6)  Name.......:      udp-ecv  Type......:   UDP-ECV   State....ENABLED
7)  Name.......:          dns  Type......:      DNS   State....ENABLED
8)  Name.......:          ftp  Type......:      FTP   State....ENABLED
```

Top

lb route

[add | rm | show]

add lb route

Synopsis

add lb route <network> <netmask> <gatewayName>

Description

Bind the route VIP to the route structure.

Parameters

network

The IP address of the network to which the route belongs.

netmask

The netmask to which the route belongs.

gatewayName

The name of the route.

Top

rm lb route

Synopsis

rm lb route <network> <netmask>

Description

Remove the route VIP from the route structure.

Parameters

network

The IP address of the network to which the route VIP belongs.

netmask

The netmask of the destination network.

Top

show lb route

Synopsis

show lb route [<network> <netmask>]

Description

Display the names of the routes associated to the route structure using the ###add lb route### command.

Parameters

network

The destination network or host.

Top

lb route6

[add | rm | show]

add lb route6

Synopsis

add lb route6 <network> <gatewayName>

Description

Bind the route VIP to the route structure.

Parameters

network

The destination network.

gatewayName

The name of the route.

Top

rm lb route6

Synopsis

rm lb route6 <network>

Description

Remove the route VIP from the route structure.

Parameters

network

The IP address of the network to which the route VIP belongs.

Top

show lb route6

Synopsis

show lb route6 [<network>]

Description

Display the names of the routes associated to the route structure using the ###add lb route6### command.

Parameters

network

The destination network or host.

Top

lb vserver

[add | rm | set | unset | bind | unbind | enable | disable | show | stat | rename]

add lb vserver

Synopsis

add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port> [-range <positive_integer>]) | (-IPPattern <ippat> -IPMask <ipmask>)] [-persistenceType <persistenceType>] [-timeout <mins>] [-persistenceBackup (SOURCEIP | NONE)] [-ownerNode <positive_integer> [-backupNode <positive_integer>]] [-backupPersistenceTimeout <mins>] [-lbMethod <lbMethod> [-hashLength <positive_integer>] [-netmask <netmask>] [-v6netmasklen <positive_integer>]] [-rule <expression>] [-Listenpolicy <expression> [-Listenpriority <positive_integer>]] [-resRule <expression>] [-persistMask <netmask>] [-v6persistmasklen <positive_integer>] [-pq (ON | OFF)] [-sc (ON | OFF)] [-rtspNat (ON | OFF)] [-m <m>] [-tosId <positive_integer>] [-dataLength <positive_integer>] [-dataOffset <positive_integer>] [-sessionless (ENABLED | DISABLED)] [-state (ENABLED | DISABLED)] [-connfailover <connfailover>] [-redirectURL <URL>] [-cacheable (YES | NO)] [-cltTimeout <secs>] [-soMethod <soMethod>] [-soPersistence (ENABLED | DISABLED)] [-soPersistenceTimeOut <positive_integer>] [-soThreshold <positive_integer>] [-redirectPortRewrite (ENABLED | DISABLED)] [-downStateFlush (ENABLED | DISABLED)] [-backupVServer <string>] [-disablePrimaryOnDown (ENABLED | DISABLED)] [-insertVserverIPPort <insertVserverIPPort> [<vipHeader>]] [-AuthenticationHost <string>] [-Authentication (ON | OFF)] [-authn401 (ON | OFF)] [-authnVsName <string>] [-push (ENABLED | DISABLED)] [-pushVserver <string>] [-pushLabel <expression>] [-pushMultiClients (YES | NO)] [-tcpProfileName <string>] [-httpProfileName <string>] [-comment <string>] [-l2Conn (ON | OFF)] [-mssqlServerVersion <mssqlServerVersion>] [-mysqlProtocolVersion <positive_integer>] [-mysqlServerVersion <string>] [-mysqlCharacterSet <positive_integer>] [-mysqlServerCapabilities <positive_integer>] [-appflowLog (ENABLED | DISABLED)] [-netProfile <string>] [-icmpVsrResponse (PASSIVE | ACTIVE)] [-newServiceRequest <positive_integer> [<newServiceRequestUnit>]] [-newServiceRequestIncrementInterval <positive_integer>] [-persistAVPno <positive_integer> ...]

Description

Add a load balancing virtual server.

Parameters

name

The name of the load balancing virtual server being added.

serviceType

The service type. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER

IPAddress

The IP address of the virtual server.

IPPattern

The IP Pattern of the virtual server.

port

A port number for the virtual server.

range

The IP range for the network vserver. Default value: 1 Minimum value: 1 Maximum value: 254

persistenceType

Persistence type for the virtual server. Note: The <persistenceType> parameter can take one of the following options: SOURCEIP - When configured, the system selects a physical service based on the Load Balancing method, and then directs all the subsequent requests arriving from the same IP as the first request to the same physical service. COOKIEINSERT - When configured, the system inserts an HTTP cookie into the client responses. The cookie is inserted into the "Cookie" header field of the HTTP response. The client stores the cookie (if enabled) and includes it in all the subsequent requests, which then match the cookie criteria. The cookie contains information about the service where the requests have to be sent. SSLSESSION ID - When configured, the system creates a persistence that is session based on the arriving SSL Session ID, which is part of the SSL handshake process. All requests with the same SSL session ID are directed to the initially selected physical service. CUSTOM SERVER ID -This mode of Persistence requires the server to provide its Server-ID in such a way that it can be extracted from subsequent requests. The system extracts the Server-ID from subsequent client requests and uses it to select a server. The server embeds the Server-ID into the URL query of the HTML links, accessible from the initial page that has to generate persistent HTTP requests. RULE - When configured, the system maintains persistence based on the contents of the matched rule. This persistence requires an expression to be configured. The expression is created using the add expression CLI command and is configured on a virtual server, using the -rule option of the add lb vserver or set lb vserver CLI command.After successful evaluation of the expression, a persistence session is created and all subsequent matching client requests are directed to the previously selected server. URLPASSIVE - This mode of Persistence requires the server to provide its Server-ID in such a way that it can be extracted from subsequent requests.The system extracts the Server-ID from subsequent client requests and uses it to select a server. The servers which require persistence, embed the Server-ID into the URL query of the HTML links, accessible from the initial page. The Server-ID is its IP address and port specified as a hexadecimal number.URL Passive persistence type requires an expression to be configured that specifies the location of the Server-ID in the client's requests. The expression is created using the CLI command add expression. This expression is configured on a virtual server, using option -rule of the add lb vserver or set lb vserver CLI command. DESTIP -When configured, the system selects a physical service based on the Load Balancing method, and then directs all the subsequent requests with the same

destination as the first packet to the same physical service. This will be used in LLB deployment scenarios. SRCIPDESTIP - When configured, the system selects a physical service based on the Load Balancing method, and then directs all the subsequent requests with the same Source IP and Destination IP as the first packet to the same physical service. This will be used in IDS LB depolyments. CALLID - When configured, the system maintains persistence based on CALLID used in the SIP transactions. All the SIP transactions with same CALLID are directed to the same server. RTSPSID - When configured, the system maintains persistence based on RTSP sessionID provided by the server. The client also sends the same RTSP sessionID in the subsequent requests which are then directed to the same server. DIAMETER - When configured, the system mantains persistence based on an AVP code value found in Diameter Message. This persistence requires an AVP code to be configured as persist AVP code. This persist Avp Code is configured in cli using using option -persistAVPno. After successfully finding persist AVP code in diameter request, a persistence session is created with AVP contents and all subsequent matching Diameter messages are directed to the previously selected server. Possible values: SOURCEIP, COOKIEINSERT, SSLSESSION, RULE, URLPASSIVE, CUSTOMSERVERID, DESTIP, SRCIPDESTIP, CALLID, RTSPSID, DIAMETER, NONE

timeout

The time period for which the persistence is in effect for a specific client. The value ranges from 2 to 1440 minutes. Default value: 2 Maximum value: 1440

persistenceBackup

Use this parameter to specify a backup persistence type for the virtual server. The Backup persistence option is used when the primary configured persistence mechanism on virtual server fails. The <persistenceBacup> parameter can take one of the following options: SOURCEIP NONE Possible values: SOURCEIP, NONE

ownerNode

The owner node. Maximum value: 31

backupPersistenceTimeout

The maximum time backup persistence is in effect for a specific client. Default value: 2 Minimum value: 2 Maximum value: 1440

lbMethod

The load balancing method for the virtual server. The valid options for this parameter are: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, URLHASH, DOMAINHASH, DESTINATIONIPHASH, SOURCEIPHASH, SRCIPDESTIPHASH,LEASTBANDWIDTH, LEASTPACKETS, TOKEN, SRCIPDESTIPHASH, CUSTOMLOAD, SRCIPSRCPORTHASH, LRTM, CALLIDHASSH. When the load balancing policy is configured as: ROUNDROBIN - When configured, the system distributes incoming requests to each server in rotation, regardless of the load. When different weights are assigned to services then weighted round robin occurs and requests go to services according to how much weighting has been set. LEASTCONNECTION (default value)- When configured, the system selects the service that has the least number of connections. For TCP, HTTP, HTTPS and SSL_TCP services the least number of connections includes: Established, active connections to a service. Connection reuse applies to HTTP and HTTPS. Hence the count includes only those connections which have outstanding HTTP or HTTPS requests, and does not include inactive, reusable connections. Connections to a service waiting in the Surge Queue, which exists only if the Surge Protection feature is enabled. For UDP services the least

number of connections includes: The number of sessions between client and a physical service. These sessions are the logical, time-based entities, created on first arriving UDP packet. If configured, weights are taken into account when server selection is performed. LEASTRESPONSETIME - When configured, the system selects the service with the minimum average response time. The response time is the time interval taken when a request is sent to a service and first response packet comes back from the service, that is Time to First Byte (TTFB). URLHASH - The system selects the service based on the hashed value of the incoming URL.To specify the number of bytes of the URL that is used to calculate the hash value use the optional argument [-hashLength <positive_integer>] in either the add lb vserver or set lb vserver CLI command. The default value is 80. DOMAINHASH - When configured with this load balancing method, the system selects the service based on the hashed value of the domain name in the HTTP request. The domain name is taken either from the incoming URL or from the Host header of the HTTP request. Note: The system defaults to LEASTCONNECTION if the request does not contain a domain name. If the domain name appears in both the URL and the host header, the system gives preference to the URL domain. DESTINATIONIPHASH - The system selects the service based on the hashed value of the destination IP address in the TCP IP header. SOURCEIPHASH - The system selects the service based on the hashed value of the client's IP address in the IP header. LEASTBANDWIDTH - The system selects the service that is currently serving the least traffic, measured in megabits per second. LEASTPACKETS - The system selects the service that is currently serving the lowest number of packets per second. Token -The system selects the service based on the value, calculated from a token, extracted from the client's request (location and size of the token is configurable or by evaluating the rule configured). For subsequent requests with the same token, the systems will select the same physical server. SRCIPDESTIPHASH - The system selects the service based on the hashed value of the client's SOURCE IP and DESTINATION IP address in the TCP IP header. CUSTOMLOAD - The system selects the service based on the it load which was determined by the LOAD monitors bound to the service. SRCIPSRCPORTHASH - The system selects the service based on the hashed value of the client's SOURCE IP and SOURCE PORT in the TCP/UDP+IP header. LRTM - When configured, the system selects the service with least response time learned through probing(number of active connections taken into account in addition to the response time). CALLIDHASSH - The system selects the service based on the hashed value of SIP callid. Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, URLHASH, DOMAINHASH, DESTINATIONIPHASH, SOURCEIPHASH, SRCIPDESTIPHASH, LEASTBANDWIDTH, LEASTPACKETS, TOKEN, SRCIPSRCPORTHASH, LRTM, CALLIDHASH, CUSTOMLOAD, LEASTREQUEST Default value: PEMGMT_LB_LEASTCONNS

rule

Use this parameter to specify the string value used to set the RULE persistence type. The string can be either an existing rule name (configured using add expression command) or else it can be an in-line expression with a maximum of 1499 characters. Default value: "none"

Listenpolicy

Use this parameter to specify the listen policy for LB Vserver. The string can be either an existing expression name (configured using add policy expression command) or else it can be an in-line expression with a maximum of 1499 characters. Default value: "none"

Listenpriority

Use this parameter to specify the priority for listen policy of LB Vserver. Default value: 101 Maximum value: 101

resRule

Use this parameter to specify the expression to be used in response for RULE persistence type. The string is an in-line expression with a maximum of 1499 characters. Default value: "none"

persistMask

Use this parameter to specify if the persistency is IP based. This parameter is Optional. Default value: 0xFFFFFFFF

v6persistmasklen

The persistence mask. Use this parameter if you are using IP based persistence type on a ipv6 vserver. Default value: 128 Minimum value: 1 Maximum value: 128

pq

Use this parameter to enable priority queuing on the specified virtual server. Possible values: ON, OFF Default value: OFF

sc

Use this parameter to enable SureConnect on the specified virtual server. Possible values: ON, OFF Default value: OFF

rtspNat

Use this parameter to enable natting for RTSP data connection. Possible values: ON, OFF Default value: OFF

m

Use this parameter to specify the LB mode. If the value is specified as IP then the traffic is sent to the physical servers by changing the destination IP address to that of the physical server. If the value is MAC then the traffic is sent to the physical servers , by changing the destination MAC address to that of one of the physical servers, the destination IP is not changed. MAC mode is used mostly in Firewall Load Balancing scenario. Possible values: IP, MAC, IPTUNNEL, TOS Default value: NSFWD_IP

tosId

Use this parameter to specify the TOS ID of this vserver. Applicable only when the LB mode is TOS Minimum value: 1 Maximum value: 63

dataLength

Use this parameter to specify the length of the token in bytes. Applicable to TCP virtual servers, when Token Load Balancing method is selected. The datalength should not be more than 24k. Maximum value: 100

dataOffset

Use this parameter to specifies offset of the data to be taken as token. Applicable to the TCP type virtual servers, when Token load balancing method is used. Must be within the first 24k of the client TCP data. Maximum value: 25400

sessionless

Use this parameter to enable sessionless load balancing. Possible values: ENABLED, DISABLED Default value: DISABLED

state

The state of the load balancing virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

connfailover

Specifies the connection failover mode of the virtual server Possible values: DISABLED, STATEFUL, STATELESS Default value: DISABLED

redirectURL

The URL where traffic is redirected if the virtual server in the system becomes unavailable. You can enter up to 127 characters as the URL argument. WARNING! Make sure that the domain you specify in the URL does not match the domain specified in the -d domainName argument of the add cs policy CLI command. If the same domain is specified in both arguments, the request will be continuously redirected to the same unavailable virtual server in the system - then the user may not get the requested content.

cacheable

Use this option to specify whether a virtual server, used for load balancing or content switching, routes requests to the cache redirection virtual server before sending it to the configured servers. Possible values: YES, NO Default value: NO

cltTimeout

The timeout value in seconds for idle client connection Default value: VAL_NOT_SET Maximum value: 31536000

soMethod

The spillover factor based on which the traffic will be given to the backupvserver once the main virtual server reaches the spillover threshold. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence

The state of the spillover persistence. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut

The spillover persistency entry timeout. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold

In case of CONNECTION (or) DYNAMICCONNECTION type spillover method this value is treated as Maximum number of connections an lb vserver will handle before spillover

takes place. In case of BANDWIDTH type spillover method this value is treated as the amount of incoming and outgoing traffic (in Kbps) a Vserver will handle before spillover takes place. In case of HEALTH type spillover method if the percentage of active services (by weight) becomes lower than this value, spillover takes place Minimum value: 1 Maximum value: 4294967287

redirectPortRewrite

The state of port rewrite while performing HTTP redirect. Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush

Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

backupVServer

The Backup Virtual Server.

disablePrimaryOnDown

When this argument is enabled, traffic will continue reaching backup vservers even after primary comes UP from DOWN state. Possible values: ENABLED, DISABLED Default value: DISABLED

insertVserverIPPort

The virtual IP and port header insertion option for the vserver. VIPADDR - Header contains the vserver's IP address and port number without any translation. OFF - The virtual IP and port header insertion option is disabled. V6TOV4MAPPING - Header contains the mapped IPv4 address corresponding to the IPv6 address of the vserver and the port number. An IPv6 address can be mapped to a user-specified IPv4 address using the set ns ip6 command. Possible values: OFF, VIPADDR, V6TOV4MAPPING

AuthenticationHost

FQDN of authentication vserver

Authentication

This option toggles on or off the application of authentication of incoming users to the vserver. Possible values: ON, OFF Default value: OFF

authn401

This option toggles on or off the HTTP 401 response based authentication. Possible values: ON, OFF Default value: OFF

authnVsName

Name of authentication vserver

push

Process traffic on bound Push vserver. Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver

The lb vserver of type PUSH/SSL_PUSH to which server pushes the updates received on the client facing non-push lb vserver.

pushLabel

Use this parameter to specify the expression to extract the label in response from server. The string can be either a named expression (configured using add policy expression command) or else it can be an in-line expression with a maximum of 63 characters. Default value: "none"

pushMultiClients

Specify if multiple web 2.0 connections from the same client can connect to this vserver and expect updates. Possible values: YES, NO Default value: NO

tcpProfileName

The name of the TCP profile.

httpProfileName

Name of the HTTP profile.

comment

Comments associated with this virtual server.

l2Conn

Use L2 Parameters to identify a connection Possible values: ON, OFF

mssqlServerVersion

The version of the MSSQL server Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2 Default value: TDS_PROT_2008B

mysqlProtocolVersion

The protocol version returned by the mysql vserver. Default value: NSA_MYSQL_PROTOCOL_VER_DEFAULT

mysqlServerVersion

The server version string returned by the mysql vserver. Default value: NSA_MYSQL_SERVER_VER_DEFAULT

mysqlCharacterSet

The character set returned by the mysql vserver. Default value: NSA_MYSQL_CHAR_SET_DEFAULT

mysqlServerCapabilities

The server capabilities returned by the mysql vserver. Default value: NSA_MYSQL_SVR_CAPABILITIES_DEFAULT

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

The name of the network profile.

icmpVsrResponse

Can be active or passive Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

newServiceRequest

The number of requests/sec or percentage of requests/sec a new service should receive compared to the existing services. The maximum possible value for requests/sec is 65536 and percentage of requests is 100

newServiceRequestIncrementInterval

The interval in seconds after which the new services requests limit should be automatically increased. Maximum value: 3600

persistAVPno

Persist AVP number for Diameter Persistency. In case this AVP is not defined in Base RFC 3588 and it is nested inside a Grouped AVP, define a sequence of AVP numbers (max 3) in order of parent to child. So say persist AVP number X is nested inside AVP Y which is nested in Z, then define the list as Z Y X Minimum value: 1

Example

add lb vserver http_vsvr http 10.102.1.10 80
To add multiple vservers at once use the following command:
add lb vs http_vsvr[1-4] http 10.102.27.[115-118] 80
This command adds the vserver http_vsvr1 with the IP address 10.102.27.115, http_vsvr2 with 10.102.27.1

Top

rm lb vserver

Synopsis

rm lb vserver <name>@ ...

Description

Remove a virtual server.

Parameters

name

The name of the virtual server to be removed.

Example

rm vserver lb_vip
To remove multiple vservers use the following command:
rm vserver lb_vip[1-3]

Top

set lb vserver

Synopsis

set lb vserver <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@] [-IPPattern <ippat>] [-IPMask <ipmask>] [-weight <positive_integer> <serviceName>@] [-persistenceType <persistenceType>] [-timeout <mins>] [-persistenceBackup (SOURCEIP | NONE)] [-backupPersistenceTimeout <mins>] [-lbMethod <lbMethod> [-hashLength <positive_integer>] [-netmask <netmask>] [-v6netmasklen <positive_integer>]] [-rule <expression>] [-resRule <expression>] [-persistMask <netmask>] [-v6persistmasklen <positive_integer>] [-pq (ON | OFF)] [-sc (ON | OFF)] [-rtspNat (ON | OFF)] [-m <m>] [-tosId <positive_integer>] [-dataLength <positive_integer>] [-dataOffset <positive_integer>] [-sessionless (ENABLED | DISABLED)] [-connfailover <connfailover>] [-backupVServer <string>] [-redirectURL <URL>] [-cacheable (YES | NO)] [-cltTimeout <secs>] [-soMethod <soMethod>] [-soThreshold <positive_integer>] [-soPersistence (ENABLED | DISABLED)] [-soPersistenceTimeOut <positive_integer>] [-redirectPortRewrite (ENABLED | DISABLED)] [-downStateFlush (ENABLED | DISABLED)] [-insertVserverIPPort <insertVserverIPPort> [<vipHeader>]] [-disablePrimaryOnDown (ENABLED | DISABLED)] [-AuthenticationHost <string>] [-Authentication (ON | OFF)] [-authn401 (ON | OFF)] [-authnVsName <string>] [-push (ENABLED | DISABLED)] [-pushVserver <string>] [-pushLabel <expression>] [-pushMultiClients (YES | NO)] [-Listenpolicy <expression>] [-Listenpriority <positive_integer>] [-tcpProfileName <string>] [-httpProfileName <string>] [-comment <string>] [-l2Conn (ON | OFF)] [-mssqlServerVersion <mssqlServerVersion>] [-mysqlProtocolVersion <positive_integer>] [-mysqlServerVersion <string>] [-mysqlCharacterSet <positive_integer>] [-mysqlServerCapabilities <positive_integer>] [-appflowLog (ENABLED | DISABLED)] [-netProfile <string>] [-icmpVsrResponse (PASSIVE | ACTIVE)] [-newServiceRequest <positive_integer>] [<newServiceRequestUnit>] [-newServiceRequestIncrementInterval <positive_integer>] [-persistAVPno <positive_integer> ...]

Description

Set load balancing virtual server attributes.

Parameters

name

The name of the load balancing virtual server.

IPAddress

The new IP address of the virtual server.

IPPattern

The IP Pattern of the virtual server.

IPMask

The IP Mask of the virtual server IP Pattern

weight

The weight for the specified service. Minimum value: 1 Maximum value: 100

persistenceType

Persistence type for the virtual server. Note: The <persistenceType> parameter can take one of the following options: SOURCEIP - When configured, the system selects a physical service based on the Load Balancing method, and then directs all the subsequent requests arriving from the same IP as the first request to the same physical service. COOKIEINSERT - When configured, the system inserts an HTTP cookie into the client responses. The cookie is inserted into the "Cookie" header field of the HTTP response. The client stores the cookie (if enabled) and includes it in all the subsequent requests, which then match the cookie criteria. The cookie contains information about the service where the requests have to be sent. SSLSESSION ID - When configured, the system creates a persistence that is session based on the arriving SSL Session ID, which is part of the SSL handshake process. All requests with the same SSL session ID are directed to the initially selected physical service. CUSTOM SERVER ID -This mode of Persistence requires the server to provide its Server-ID in such a way that it can be extracted from subsequent requests. The system extracts the Server-ID from subsequent client requests and uses it to select a server. The server embeds the Server-ID into the URL query of the HTML links, accessible from the initial page that has to generate persistent HTTP requests. RULE - When configured, the system maintains persistence based on the contents of the matched rule. This persistence requires an expression to be configured. The expression is created using the add expression CLI command and is configured on a virtual server, using the -rule option of the add lb vserver or set lb vserver CLI command.After successful evaluation of the expression, a persistence session is created and all subsequent matching client requests are directed to the previously selected server. URLPASSIVE - This mode of Persistence requires the server to provide its Server-ID in such a way that it can be extracted from subsequent requests.The system extracts the Server-ID from subsequent client requests and uses it to select a server. The servers which require persistence, embed the Server-ID into the URL query of the HTML links, accessible from the initial page. The Server-ID is its IP address and port specified as a hexadecimal number.URL Passive persistence type requires an expression to be configured that specifies the location of the Server-ID in the client's requests. The expression is created using the CLI command add expression. This expression is configured on a virtual server, using option -rule of the add lb vserver or set lb vserver CLI command. DESTIP -When configured, the system selects a physical service based on

the Load Balancing method, and then directs all the subsequent requests with the same destination as the first packet to the same physical service. This will be used in LLB deployment scenarios. SRCIPDESTIP - When configured, the system selects a physical service based on the Load Balancing method, and then directs all the subsequent requests with the same Source IP and Destination IP as the first packet to the same physical service. This will be used in IDS LB depolyments. CALLID - When configured, the system maintains persistence based on CALLID used in the SIP transactions. All the SIP transactions with same CALLID are directed to the same server. RTSPSID - When configured, the system maintains persistence based on RTSP sessionID provided by the server. The client also sends the same RTSP sessionID in the subsequent requests which are then directed to the same server. DIAMETER - When configured, the system mantains persistence based on an AVP code value found in Diameter Message. This persistence requires an AVP code to be configured as persist AVP code. This persist Avp Code is configured in cli using using option -persistAVPno. After successfully finding persist AVP code in diameter request, a persistence session is created with AVP contents and all subsequent matching Diameter messages are directed to the previously selected server. Possible values: SOURCEIP, COOKIEINSERT, SSLSESSION, RULE, URLPASSIVE, CUSTOMSERVERID, DESTIP, SRCIPDESTIP, CALLID, RTSPSID, DIAMETER, NONE

timeout

The maximum time persistence is in effect for a specific client. Default value: 2 Maximum value: 1440

persistenceBackup

The backup persistency to be used when the primary persistency fails. For the backup persistency to be active the primary persistency must be COOKIEINSERT. Possible values: SOURCEIP, NONE

backupPersistenceTimeout

The maximum time backup persistence is in effect for a specific client. Default value: 2 Minimum value: 2 Maximum value: 1440

lbMethod

The load balancing method to be in effect: ROUNDROBIN: When selected, determines the destination of a request based on the performance weight (configured by the -weight argument of the ###set lb vserver### command). LEASTCONNECTION: When selected, determines the destination of a request based on the least number of active connections from the system to each physical service bound to the virtual server. LEASTRESPONSETIME: When selected, determines the destination of a request based on the average response time. URLHASH: When selected, determines the destination of a request by hashing the URL. DOMAINHASH: When selected, determines the destination of a request by hashing the domain name DESTINATIONHASH: When selected, determines the destination of a request by hashing the destination IP address or destination network. SOURCEIPHASH: When selected, determines the destination of a request by hashing the source IP address or source network. LEASTBANDWIDTH: When selected, determines the destination of a request based on the bandwidth utilization. LEASTPACKETS: When selected, determines the destination of a request based on number of packets. Token: When selected, determines the destination of a request based on the value, calculated from a token, extracted from the client's request (location and size of the token is configurable or by evaluating the rule configured). CUSTOMLOAD: The system selects the service based on the it load which w as determined by the LOAD monitors bound to the service. SRCIPSRCPORTHASH - The system selects the service based on the hashed value

of the client's SOURCE IP and SOURCE PORT in the TCP/UDP+IP header. LRTM - When configured, the system selects the service with least response time learned through probing(number of active connections taken into account in addition to the response time). CALLIDHASSH - The system selects the service based on the hashed value of SIP callid. Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, URLHASH, DOMAINHASH, DESTINATIONIPHASH, SOURCEIPHASH, SRCIPDESTIPHASH, LEASTBANDWIDTH, LEASTPACKETS, TOKEN, SRCIPSRCPORTHASH, LRTM, CALLIDHASH, CUSTOMLOAD, LEASTREQUEST Default value: PEMGMT_LB_LEASTCONNS

rule

The RULE persistence type. The string can be either a existing rule name (configured using add expression command)or else it could it be an inline expression with a maximum of 1499 characters. Default value: "none"

resRule

Use this parameter to specify the expression to be used in response for RULE persistence type. The string is an in-line expression with a maximum of 1499 characters. Default value: "none"

persistMask

The persistence mask. Use this parameter if you are using IP based persistence type. Default value: 0xFFFFFFFF

v6persistmasklen

The persistence mask. Use this parameter if you are using IP based persistence type on a ipv6 vserver. Default value: 128 Minimum value: 1 Maximum value: 128

pq

The state of priority queuing on the specified virtual server. Possible values: ON, OFF Default value: OFF

sc

The state of SureConnect the specified virtual server. Possible values: ON, OFF Default value: OFF

rtspNat

Use this parameter to enable natting for RTSP data connection. Possible values: ON, OFF Default value: OFF

m

The LB mode. This option is designed for firewall load balancing and cache redirection. IP - Communicate to the server using server's IP address. MAC - Communicate to the server using server's MAC address. TUNNEL - Communicate to the server through an IP tunnel. TOS - Communicate to server using TOS ID. Possible values: IP, MAC, IPTUNNEL, TOS Default value: NSFWD_IP

tosId

Use this parameter to specify the TOS ID of this vserver. Applicable only when the LB mode is TOS Minimum value: 1 Maximum value: 63

dataLength

The data length when TOKEN load balancing method is selected. Minimum value: 1 Maximum value: 100

dataOffset

The data offset length when TOKEN load balancing method is selected. Maximum value: 25400

sessionless

The state of sessionless load balancing. Possible values: ENABLED, DISABLED Default value: DISABLED

connfailover

Specifies the connection failover mode of the virtual server Possible values: DISABLED, STATEFUL, STATELESS Default value: DISABLED

backupVServer

The Backup Virtual Server.

redirectURL

The redirect URL.

cacheable

The state of caching. Possible values: YES, NO Default value: NO

cltTimeout

The client timeout in seconds. Default value: VAL_NOT_SET Maximum value: 31536000

soMethod

The spillover method to be in effect. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence

State of spillover persistence. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut

The maximum time persistence is in effect for a specific client on a spillover vserver. Default value: 2 Minimum value: 2 Maximum value: 1440

redirectPortRewrite

The state of port rewrite while performing HTTP redirect. Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush

Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

insertVserverIPPort

The virtual IP and port header insertion option for the vserver. VIPADDR - Header contains the vserver's IP address and port number without any translation. OFF - The virtual IP and port header insertion option is disabled. V6TOV4MAPPING - Header contains the mapped IPv4 address corresponding to the IPv6 address of the vserver and the port number. An IPv6 address can be mapped to a user-specified IPv4 address using the set ns ip6 command. Possible values: OFF, VIPADDR, V6TOV4MAPPING

disablePrimaryOnDown

When this argument is enabled, traffic will continue reaching backup vservers even after primary comes UP from DOWN state. Possible values: ENABLED, DISABLED Default value: DISABLED

AuthenticationHost

FQDN of authentication vserver

Authentication

This option toggles on or off the application of authentication of incoming users to the vserver. Possible values: ON, OFF Default value: OFF

authn401

This option toggles on or off the HTTP 401 response based authentication. Possible values: ON, OFF Default value: OFF

authnVsName

Name of authentication vserver

push

Process traffic on bound Push vserver. Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver

The lb vserver of type PUSH/SSL_PUSH to which server pushes the updates received on the client facing non-push lb vserver.

pushLabel

Use this parameter to specify the expression to extract the label in response from server. The string can be either a named expression (configured using add policy expression command) or else it can be an in-line expression with a maximum of 63 characters.

Default value: "none"

pushMultiClients

Specify if multiple web 2.0 connections from the same client can connect to this vserver and expect updates. Possible values: YES, NO Default value: NO

Listenpolicy

Use this parameter to specify the listen policy for LB Vserver. The string can be either an existing expression name (configured using add policy expression command) or else it can be an in-line expression with a maximum of 1499 characters. Default value: "none"

Listenpriority

Use this parameter to specify the priority for listen policy of LB Vserver. Default value: 101 Maximum value: 101

tcpProfileName

The name of the TCP profile.

httpProfileName

Name of the HTTP profile.

comment

Comments associated with this virtual server.

l2Conn

Use L2 Parameters to identify a connection Possible values: ON, OFF

mssqlServerVersion

The version of the MSSQL server Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2 Default value: TDS_PROT_2008B

mysqlProtocolVersion

The protocol version returned by the mysql vserver. Default value: NSA_MYSQL_PROTOCOL_VER_DEFAULT

mysqlServerVersion

The server version string returned by the mysql vserver. Default value: NSA_MYSQL_SERVER_VER_DEFAULT

mysqlCharacterSet

The character set returned by the mysql vserver. Default value: NSA_MYSQL_CHAR_SET_DEFAULT

mysqlServerCapabilities

The server capabilities returned by the mysql vserver. Default value: NSA_MYSQL_SVR_CAPABILITIES_DEFAULT

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

The name of the network profile.

icmpVsrResponse

Can be active or passive Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

newServiceRequest

The number of requests/sec or percentage of requests/sec a new service should receive compared to the existing services. The maximum possible value for requests/sec is 65536 and percentage of requests is 100

newServiceRequestIncrementInterval

The interval in seconds after which the new services requests limit should be automatically increased. Maximum value: 3600

persistAVPno

Persist AVP number for Diameter Persistency. In case this AVP is not defined in Base RFC 3588 and it is nested inside a Grouped AVP, define a sequence of AVP numbers (max 3) in order of parent to child. So say persist AVP number X is nested inside AVP Y which is nested in Z, then define the list as Z Y X Minimum value: 1

Example

set lb vserver http_vip -lbmethod LEASTRESPONSETIME
To set the load balancing method for multiple vserver use the following command:
set lb vserver http_vip[1-3] -lbmethod LEASTRESPONSETIME

Top

unset lb vserver

Synopsis

unset lb vserver <name>@ [-backupVServer] [-cltTimeout] [-redirectURL] [-AuthenticationHost] [-authnVsName] [-pushVserver] [-pushLabel] [-tcpProfileName] [-httpProfileName] [-rule] [-l2Conn] [-mysqlProtocolVersion] [-mysqlServerVersion] [-mysqlCharacterSet] [-mysqlServerCapabilities] [-appflowLog] [-netProfile] [-icmpVsrResponse] [-serviceName] [-persistenceType] [-timeout] [-persistenceBackup] [-backupPersistenceTimeout] [-lbMethod] [-hashLength] [-netmask] [-v6netmasklen] [-resRule] [-persistMask] [-v6persistmasklen] [-pq] [-sc] [-rtspNat] [-m] [-tosId] [-dataLength] [-dataOffset] [-sessionless] [-connfailover] [-cacheable] [-soMethod] [-soPersistence] [-soPersistenceTimeOut] [-redirectPortRewrite] [-downStateFlush] [-insertVserverIPPort] [-vipHeader] [-disablePrimaryOnDown] [-Authentication] [-authn401] [-push] [-pushMultiClients] [-Listenpolicy] [-Listenpriority] [-comment] [-mssqlServerVersion] [-newServiceRequest] [-newServiceRequestUnit] [-newServiceRequestIncrementInterval] [-persistAVPno]

Description

Unset the backup virtual server or redirectURL set on the virtual server..Refer to the set lb vserver command for meanings of the arguments.

Example

unset lb vserver lb_vip -backupVServer

To unset the backup virtual server for multiple vservers use the following command:
unset lb vserver lb_vip[1-3] -backupVServer

Top

bind lb vserver

Synopsis

bind lb vserver <name>@ ((<serviceName>@ [-weight <positive_integer>]) | <serviceGroupName>@ | (-policyName <string>@ [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-type (REQUEST | RESPONSE)] [-invoke (<labelType> <labelName>)]))

Description

Bind a physical service to a virtual server.

Parameters

name

The virtual server name to which the service is bound.

serviceName

The name of the service that is bound.

serviceGroupName

The name of the service group that is bound.

policyName

The SureConnect/priority queuing/Compression/AppSecure/Transform/Filter/Authorization/Rewrite/Responder/Cache/Syslog/Nslog/TMTraffic policy that needs to be bound to the specified load balancing virtual server for SureConnect or priority queuing to be activated on a load balancing virtual server.

Example

bind lb vserver http_vip http_svc
To bind a service to multiple vservers use the following command:
bind lb vs http_vip[1-3] http_svc
To bind multiple services to a vserver use the following command:
bind lb vs http_vip http_svc[1-3]

Top

unbind lb vserver

Synopsis

unbind lb vserver <name>@ (<serviceName>@ | <serviceGroupName>@ | (-policyName <string>@ [-type (REQUEST | RESPONSE)])) [-priority <positive_integer>]

Description

Unbind a service or policy from a virtual server that has been configured for use in system's load balancing.

Parameters

name

The virtual server name from which the service will be unbound.

serviceName

The service name (created with the addService command) that will be unbound.

serviceGroupName

The name of the service group that is unbound.

policyName

The SureConnect or priority queuing policy that has been bound to this load balancing virtual server, using the ###bind lb vserver### command.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind lb vserver http_vip http_svc
To unbind a service from multiple vservers use the following command:
unbind lb vs http_vip[1-3] http_svc
To unbind multiple services from a vserver use the following command:
unbind lb vs http_vip http_svc[1-3]

Top

enable lb vserver

Synopsis

enable lb vserver <name>@

Description

Enable a virtual server. Note: Virtual servers, when added, are enabled by default.

Parameters

name

The name of the virtual server to be enabled.

Example

enable vserver lb_vip
To enable multiple vservers at once use the following command:
enable vserver lb_vip[1-3]

Top

disable lb vserver

Synopsis

disable lb vserver <name>@

Description

Disable (makes out of service) a virtual server.

Parameters

name

The name of the virtual server to be disabled. Notes: 1. The system still responds to ARP and/or ping requests for the IP address of this virtual server. 2. As the virtual server is still configured in the system, you can enable the virtual server using ###enable vserver### command.

Example

disable vserver lb_vip
To disable multiple vservers at once use the following command:
disable vserver lb_vip[1-3]

Top

show lb vserver

Synopsis

show lb vserver [<name>] show lb vserver stats - alias for 'stat lb vserver'

Description

Displays the parameters of all the load balancing virtual servers configured on the appliance, or the parameters of the specified virtual server.

Parameters

name

The name of the load balancing server. If no load balancing virtual server name is entered, a list of all configured load balancing virtual servers is displayed. All the services and priority queuing/SureConnect policies that are bound to this virtual server are also displayed.

Top

stat lb vserver

Synopsis

stat lb vserver [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-sortBy Hits [<sortOrder>]]

Description

Display load-balancing vserver statistics.

Parameters

name

The name of the vserver for which statistics will be displayed. If not given statistics are shown for all vservers.

Top

rename lb vserver

Synopsis

rename lb vserver <name>@ <newName>@

Description

Rename a load balancing virtual server.

Parameters

name

The name of the load balancing virtual server.

newName

The new name of the virtual server.

Example

rename lb vserver http_vsvr http_vsvr_new

Top

lb metricTable

[add | rm | set | bind | unbind | show]

add lb metricTable

Synopsis

add lb metricTable <metricTable>

Description

Use this command to add a metric table.

Parameters

metricTable

The name of the metric table.

Example

add metrictable newtable

Top

rm lb metricTable

Synopsis

rm lb metricTable <metricTable>

Description

Use this command to remove a metric table.

Parameters

metricTable

The name of the metric table.

Example

rm metric table netscaler

Top

set lb metricTable

Synopsis

set lb metricTable <metricTable> <metric> <snmpOID>

Description

Use this command to set a metric table.

Parameters

metricTable

The name of the metric table.

Example

set metrictable table met1 aliasname oidstr

Top

bind lb metricTable

Synopsis

bind lb metricTable <metricTable> <metric> <snmpOID>

Description

Use this command to bind metric and OID to the metrictable.

Parameters

metricTable

The name of the metric table.

metric

metric name of the oid.

Example

bind metrictable tablename aliasname 1.2.3.4

Top

unbind lb metricTable

Synopsis

unbind lb metricTable <metricTable> <metric>

Description

Use this command to unbind metric from the metrictable.

Parameters

metricTable

The name of the metric table.

metric

Metric name from the table that has to be unbound.

Example

unbind metrictable tablename aliasname

Top

show lb metricTable

Synopsis

show lb metricTable [<metricTable>]

Description

Display the parameters for the specified metrictable. If the metrictablename argument is not specified, a list of all existing metrictable is returned.

Parameters

metricTable

The name of the metric table.

Example

An example of the show metrictable command output is as follows:

```
Name : ALTEON                    Type : INTERNAL
Name : CISCO-CSS                 Type : INTERNAL
Name : FOUNDRY                   Type : INTERNAL
Name : NETSCALER                 Type : INTERNAL
Name : F5                      Type : INTERNAL
Name : local                   Type : INTERNAL
```

Top

lb monbindings

show lb monbindings

Synopsis

show lb monbindings <monitorName>

Description

Display the services to which this monitor is bound

Parameters

monitorName

The name of the monitor.

lb persistentSessions

[show | clear]

show lb persistentSessions

Synopsis

show lb persistentSessions [<vServer>]

Description

Get all vserver persistent sessions

Parameters

vServer

The name of the virtual server.

Top

clear lb persistentSessions

Synopsis

clear lb persistentSessions [<vServer>]

Description

Use this command to clear/flush persistent sessions

Parameters

vServer

The name of the LB vserver whose persistence sessions are to be flushed. If not specified, all persistence sessions will be flushed .

Top

lb group

[set | unset | bind | unbind | show | rename]

set lb group

Synopsis

set lb group <name>@ [-persistenceType <persistenceType>] [-persistenceBackup (SOURCEIP | NONE)] [-backupPersistenceTimeout <mins>] [-persistMask <netmask>] [-v6persistmasklen <positive_integer>] [-cookieDomain <string>] [-timeout <mins>] [-rule <expression>]

Description

Set the persistence for the group (used in the system's load balancing feature). Persistence is set for the connections between a client and a server that is being load balanced by the system. The client will be directed to the same server until client's transactions have completed (or until the time period that you have specified has passed). Before using this command, the group must be created. The group is created implicitly when binding a load balancing virtual server to a group using the bind lb group CLI command. Similarly a group is removed when the last load balancing virtual server is unbound from it using the unbind lb group CLI command.

Parameters

name

The name of the group.

persistenceType

The persistence type for the group. Select SOURCEIP - This option is used to maintain persistency based on the client IP. COOKIEINSERT- This option is used to maintain persistency based on the cookie in the client request.This cookie is inserted by the system in the first response to the client. NONE - To disable the persistency. Possible values: SOURCEIP, COOKIEINSERT, RULE, NONE

persistenceBackup

The backup persistence type for the group. Possible values: SOURCEIP, NONE

backupPersistenceTimeout

The maximum time backup persistence is in effect for a specific client. Default value: 2 Minimum value: 2 Maximum value: 1440

persistMask

The netmask to be applied when the persistency type is SOURCEIP. Default value: 0xFFFFFFFF

v6persistmasklen

The persistence mask. Use this parameter if you are using IPv6 based persistence type on an lb group Default value: 128 Minimum value: 1 Maximum value: 128

cookieDomain

The domain attribute of the HTTP cookie.

timeout

The maximum time that persistence is in effect for a specific client. Default value: 2 Maximum value: 1440

rule

The RULE persistence type. The string can be either a existing rule name (configured using ###add rule### command) or else it could it be an inline expression with a maximum of 1500 characters. Default value: "None"

Example

set lb group webgrp -persistenceType COOKIEINSERT
To set the persistence type for multiple groups use the following command:
set lb group webgrp[1-3] -persistenceType COOKIEINSERT

Top

unset lb group

Synopsis

unset lb group <name>@ [-persistenceType] [-persistenceBackup] [-backupPersistenceTimeout] [-persistMask] [-v6persistmasklen] [-cookieDomain] [-timeout] [-rule]

Description

Use this command to remove lb group settings.Refer to the set lb group command for meanings of the arguments.

Top

bind lb group

Synopsis

bind lb group <name>@ <vServerName>@ ...

Description

Create a group of virtual servers in the system. This group supports server persistence. Only address-based (not content-based) virtual servers can be added to a group. Each virtual server can only be assigned to one group. When moving a virtual server from one group to another, the virtual server must be removed from the original group with the unbind lb group command.

Parameters

name

The name of the group. A maximum of 127 characters can be used to specify a new name to a group of virtual servers that you are creating (or to specify an existing group name if you are adding the virtual server to an existing group of virtual servers.

vServerName

The name of the virtual server that will belong to the named group.

Example

bind lb group webgrp http_vip
To bind multiple vservers to a group use the following command:
bind lb group webgrp v[1-4]
To bind vserver v1 to group webgrp1, v2 to webgrp2 and v3 to webgrp3, use the following command:
bind lb group webgrp[1-3] v[1-3]

Top

unbind lb group

Synopsis

unbind lb group <name> <vServerName>@ ...

Description

Unbind the virtual server from a group. When the last vserver is unbound, the group is deleted from system.

Parameters

name

The name of the group.

vServerName

The name of the virtual server to be removed from the group. Multiple names can be specified.

Example

unbind lb group webgroup http_vip
To unbind multiple vservers use the following command:
unbind lb group webgroup v[1-3]

Top

show lb group

Synopsis

show lb group [<name>]

Description

Display the names of the virtual servers associated to the specified group. The virtual servers were created using the ###add vserver### command.

Parameters

name

The name of the group .

Example

show lb group webgrp

Top

rename lb group

Synopsis

rename lb group <name>@ <newName>@

Description

Rename a load balancing virtual server group.

Parameters

name

The name of the load balancing virtual server group.

newName

The new name of the virtual server group.

Example

rename lb group gv1 gv-new1

Top

lb sipParameters

[set | unset | show]

set lb sipParameters

Synopsis

set lb sipParameters [-rnatSrcPort <port>] [-rnatDstPort <port>] [-retryDur <integer>] [-addRportVip (ENABLED | DISABLED)] [-sip503RateThreshold <positive_integer>]

Description

Set different SIP parameters

Parameters

rnatSrcPort

In the rnat path if the sip packet has the src port matching this port configured by the user, we will do SIP processing on it like creating persistence sessions and appending the rport.

rnatDstPort

In the rnat path if the sip packet has the dst port matching this port configured by the user, we will do SIP processing on it like creating persistence sessions and appending the rport.

retryDur

When the 503 message is generated we will inform the client to retry after X seconds which is specified by retryDur. Default value: 120 Minimum value: 1

addRportVip

Add rport to SIP requests coming on VIP Possible values: ENABLED, DISABLED Default value: ENABLED

sip503RateThreshold

If the sip vserver is down we will send the send a 503 message indicating that the service is unavailable. The variable will govern the number of messages we will generate per 10ms Default value: 100

Example

set sip parameter

Top

unset lb sipParameters

Synopsis

unset lb sipParameters [-rnatSrcPort] [-rnatDstPort] [-retryDur] [-addRportVip] [-sip503RateThreshold]

Description

Use this command to remove lb sipParameters settings.Refer to the set lb sipParameters command for meanings of the arguments.

Top

show lb sipParameters

Synopsis

show lb sipParameters

Description

Display the SIP parameters

Example

show sip parameter

Top

lb parameter

[set | unset | show]

set lb parameter

Synopsis

set lb parameter [-httpOnlyCookieFlag (ENABLED | DISABLED)] [-consolidatedLConn (YES | NO)] [-usePortForHashLb (YES | NO)] [-preferDirectRoute (YES | NO)] [-startupRRFactor <positive_integer>] [-monitorSkipMaxClient (ENABLED | DISABLED)] [-monitorConnectionClose (RESET | FIN)] [-vServerSpecificMac (ENABLED | DISABLED)]

Description

Set a common LB parameter

Parameters

httpOnlyCookieFlag

enable/disable httponly flag for persistence cookie Possible values: ENABLED, DISABLED Default value: ENABLED

consolidatedLConn

Indicates whether use consolidate stats to find the least connection service. Possible values: YES, NO Default value: YES

usePortForHashLb

Indicates whether to consider port of the service for hash based lb methods. Possible values: YES, NO Default value: YES

preferDirectRoute

If enabled, will do route lookup incase of wildcard server Possible values: YES, NO Default value: YES

startupRRFactor

Factor used to decide the number of requests the vserver will be serving in Round Robin mode, before switching to configured LB method

monitorSkipMaxClient

Enabling this option will skip maxClients limit check for monitoring connections Possible values: ENABLED, DISABLED Default value: DISABLED

monitorConnectionClose

This option is used to control the way the monitoring connections will be closed, either by FIN or RST . Default is FIN Possible values: RESET, FIN Default value: FIN

vServerSpecificMac

Incase of FW LB deployments, we might want that the return traffic from firewall should be send to another FW. NS defualt behavior is that we never reload balance the trafic returned from the services. However turning this knob ON, it willl make sure that NS lets other mac mode LB vserver to pick up this return traffic. The loop however is avoided as we dont pick the same vserver again Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set lb parameter -httponly (ENABLED|DISABLED)

Top

unset lb parameter

Synopsis

unset lb parameter [-httpOnlyCookieFlag] [-consolidatedLConn] [-usePortForHashLb] [-preferDirectRoute] [-startupRRFactor] [-monitorSkipMaxClient] [-monitorConnectionClose] [-vServerSpecificMac]

Description

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

Top

show lb parameter

Synopsis

show lb parameter

Description

Show LB parameters

Example

show lb parameter

Top

Networking Commands

This group of commands can be used to perform operations on the following entities:

- arp
- channel
- fis
- route
- vlan
- vrID
- vrID6
- route6
- nd6
- inat
- bridgegroup
- ipTunnel
- ip6Tunnel
- netbridge
- ipset
- linkset
- netProfile
- arpparam
- ci
- interface
- rnat
- bridgetable
- bridge
- lacp

- rnatparam
- rnatip
- vrIDParam
- ipv6
- ipTunnelParam
- ip6TunnelParam
- L2Param
- L3Param
- forwardingSession
- ptp
- rnat6

arp

[add | rm | send | show]

add arp

Synopsis

add arp -IPAddress <ip_addr> -mac <mac_addr> -ifnum <interface_name> [-ownerNode <positive_integer>]

Description

Add a static entry to the appliance's ARP table. This ARP entry never times out.

Parameters

IPAddress

IP address of the network device that you want to add to the ARP table.

mac

MAC address of a network device for the ARP entry.

ifnum

The Interface through which the network device is accessible. The format for specifying the interface is in slot/port notation (for example, 1/3).

ownerNode

The owner node for the Arp entry. Default value: VAL_NOT_SET Maximum value: 31

Example

add arp -ip 10.100.0.48 -mac 00:a0:cc:5f:76:3a -ifnum 1/1

Top

rm arp

Synopsis

rm arp (<IPAddress> | -all) [-ownerNode <positive_integer>]

Description

Remove an entry from the appliance's ARP table.

Parameters

IPAddress

IP address of the network device specified in the ARP entry that you want to remove from the ARP table.

all

Remove all ARP entries from the ARP table of the NetScaler appliance.

ownerNode

The owner node for the Arp entry. Default value: VAL_NOT_SET Maximum value: 31

Top

send arp

Synopsis

send arp (<IPAddress> | -all)

Description

Send Gratuitous Address Resolution Protocol (GARP) messages for the specified NetScaler owned IP addresses.

Parameters

IPAddress

A NetScaler owned IP address for which the NetScaler appliance sends Gratuitous Address Resolution Protocol (GARP) messages.

all

Send Gratuitous Address Resolution Protocol (GARP) messages for all NetScaler owned IP addresses on which the ARP option is enabled. If you set this option in a high availability configuration, the node sends GARP messages for only the NSIP address.

Example

send arp 10.10.10.10

Top

show arp

Synopsis

show arp [<IPAddress> [-ownerNode <positive_integer>]]

Description

Display all the entries in the system's ARP table.

Parameters

IPAddress

The IP address corresponding to an ARP entry.

ownerNode

The cluster node which owns the ARP entry. Default value: VAL_NOT_SET Maximum value: 31

Example

The output of the sh arp command is as follows:

```
   5 configured arps:
   IP              MAC             Inface      VLAN     Origin  TTL
   -------         -------         -------     ------   ------- --------
1) 10.250.11.1      00:04:76:dc:f1:b9   1/2        2       dynamic   700
2) 10.11.0.254      00:30:19:c1:7e:f4   1/1        1       dynamic   500
3) 10.11.0.41       00:d0:a8:00:7c:e4   0/1        1       dynamic   500
4) 10.11.222.2      00:ee:ff:22:00:01   0/1        1       dynamic   500
5) 10.11.201.12     00:30:48:31:23:49   0/1        1       dynamic   500
```

Top

channel

[add | rm | set | unset | bind | unbind | show]

add channel

Synopsis

add channel <id> [-ifnum <interface_name> ...] [-state (ENABLED | DISABLED)] [-speed <speed>] [-flowControl <flowControl>] [-haMonitor (ON | OFF)] [-tagall (ON | OFF)] [-ifAlias <string>] [-throughput <positive_integer>] [-bandwidthHigh <positive_integer> [-bandwidthNormal <positive_integer>]]

Description

Add a link aggregate channel.

Parameters

id

LA channel name (in form LA/* or CLA/* for Cluster LA)

ifnum

The interfaces to be bound to Link Aggregate channel.

state

The initial state for the LA channel. Possible values: ENABLED, DISABLED Default value: NSA_DVC_ENABLE

Mode

The initital mode for the LA channel. Possible values: MANUAL, AUTO

connDistr

The 'connection' distribution mode for the LA channel. Possible values: DISABLED, ENABLED

macdistr

The 'MAC' distribution mode for the LA channel. Possible values: SOURCE, DESTINATION, BOTH

speed

The speed for the LA channel. Possible values: AUTO, 10, 100, 1000, 10000 Default value: NSA_DVC_SPEED_AUTO

flowControl

Flow control for the LA channel. Possible values: OFF, RX, TX, RXTX Default value: NSA_DVC_FC_OFF

haMonitor

HA monitoring for the LA channel. Possible values: ON, OFF Default value: NSA_DVC_MONITOR_ON

tagall

The appliance adds a four-byte 802.1q tag to every packet sent on this channel. ON applies tags for all the VLANs that are bound to this channel. OFF, applies the tag for all VLANs other than the native VLAN. Possible values: ON, OFF Default value: NSA_DVC_VTRUNK_OFF

trunk

This is deprecated by tagall Possible values: ON, OFF Default value: OFF

ifAlias

The alias name for the channel. Default value: " "

throughput

Minimum required throughput for the interface. Maximum value: 80000

bandwidthHigh

High threshold, in Mbps, for bandwidth usage by the interface. A trap is sent if bandwidth usage by the interface crosses this limit. Maximum value: 80000

Top

rm channel

Synopsis

rm channel <id>

Description

Remove the specified link aggregate channel from the appliance.

Parameters

id

LA channel name (in form LA/* or CLA/* for Cluster LA)

Top

set channel

Synopsis

set channel <id> [-state (ENABLED | DISABLED)] [-speed <speed>] [-flowControl <flowControl>] [-haMonitor (ON | OFF)] [-tagall (ON | OFF)] [-ifAlias <string>] [-throughput <positive_integer>] [-bandwidthHigh <positive_integer> [-bandwidthNormal <positive_integer>]]

Description

Modify the settings of an existing channel

Parameters

id

LA channel name (in form LA/* or CLA/* for Cluster LA)

state

The packet processing state for the LA channel. Possible values: ENABLED, DISABLED Default value: NSA_DVC_ENABLE

Mode

The mode for the LA channel. Possible values: MANUAL, AUTO

connDistr

The 'connection' distribution mode for the LA channel. Possible values: DISABLED, ENABLED

macdistr

The 'MAC' distribution mode for the LA channel. Possible values: SOURCE, DESTINATION, BOTH

speed

The speed for the LA channel. Possible values: AUTO, 10, 100, 1000, 10000 Default value: NSA_DVC_SPEED_AUTO

flowControl

Required flow control for the LA channel. Possible values: OFF, RX, TX, RXTX Default value: NSA_DVC_FC_OFF

haMonitor

The state of HA monitoring for the LA channel. Possible values: ON, OFF Default value: NSA_DVC_MONITOR_ON

tagall

The appliance adds a four-byte 802.1q tag to every packet sent on this channel. ON applies tags for all the VLANs that are bound to this channel. OFF, applies the tag for all VLANs other than the native VLAN. Possible values: ON, OFF Default value: NSA_DVC_VTRUNK_OFF

trunk

This is deprecated by tagall. Possible values: ON, OFF Default value: OFF

ifAlias

The alias name for the interface. Default value: " "

throughput

Minimum required throughput for the interface. Maximum value: 80000

bandwidthHigh

High threshold, in Mbps, for bandwidth usage by the interface. A trap is sent if bandwidth usage by the interface crosses this limit. Maximum value: 80000

Top

unset channel

Synopsis

unset channel <id> [-state] [-speed] [-flowControl] [-haMonitor] [-tagall] [-ifAlias] [-throughput] [-bandwidthHigh] [-bandwidthNormal]

Description

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

Top

bind channel

Synopsis

bind channel <id> <ifnum> ...

Description

Bind the specified physical interface to the link aggregate channel.

Parameters

id

LA channel name (in form LA/* or CLA/* for Cluster LA)

ifnum

Interfaces to be bound to the LA channel.

Top

unbind channel

Synopsis

unbind channel <id> <ifnum> ...

Description

Unbind the specified interfaces from the link aggregate channel.

Parameters

id

LA channel name (in form LA/* or CLA/* for Cluster LA)

ifnum

Interfaces to be unbound from the LA channel.

Top

show channel

Synopsis

show channel [<id>]

Description

Display all the settings for a link aggregate channel (for example, slave interfaces and VLAN settings). If no channel ID is specified, a subset of the settings, pertaining to all the channels, is displayed.

Parameters

id

LA channel name in form LA/x, where x is the channel ID, which ranges from 1 to 4.
Minimum value: 1

Top

fis

[add | rm | bind | unbind | show]

add fis

Synopsis

add fis <name>

Description

Add an FIS. Each FIS is identified by a name (string max 31 letters). The FIS created is empty (without members).

Parameters

name

A name for the FIS to be created. Must begin with a letter, a number, or the underscore symbol, and can consist of from 1 to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the FIS.

Top

rm fis

Synopsis

rm fis <name>

Description

Remove the FIS created by the add fis command. Once the FIS is removed, its interfaces become CIs.

Parameters

name

The name of the FIS that you want to remove from the NetScaler appliance.

Top

bind fis

Synopsis

bind fis <name> <ifnum> ...

Description

Bind interfaces to an FIS. Adding an interface to an FIS deletes it from CIs and adds it to the new FIS.

Parameters

name

The name of the FIS to which you want to bind interfaces.

ifnum

The interface to be bound to the FIS, specified in the slot/port notation (for example, 1/3).

Top

unbind fis

Synopsis

unbind fis <name> <ifnum> ...

Description

Unbind the specified interface from the FIS. The interface unbound becomes a CI.

Parameters

name

The name of the FIS from which you want to unbind the interfaces.

ifnum

Interfaces that you want to unbind from the FIS. The format for specifying an interface is slot/port notation (for example, 1/3).

Top

show fis

Synopsis

show fis [<name>]

Description

Displays the configured FISs.

Parameters

name

The name of the FIS configured on the appliance.

Example

```
>show fis
1)      FIS: fis1
        Member Interfaces : 1/1
Done
```

Top

route

[add | clear | rm | set | unset | show]

add route

Synopsis

add route <network> <netmask> <gateway> [-distance <positive_integer>] [-cost <positive_integer>] [-weight <positive_integer>] [-advertise (DISABLED | ENABLED)] [-protocol <protocol> ...] [-msr (ENABLED | DISABLED) [-monitor <string>]]

Description

Add a static route to the routing table.

Parameters

network

An IPv4 network address for which you want to add a route entry in the routing table of the NetScaler appliance.

netmask

The subnet mask associated with the network address.

gateway

The IP address of the gateway for this route. Can be null to specify a null-interface route.

cost

The cost of a route is used to compare routes of the same type. The route having the lowest cost is the most preferred route. Possible values: 0 through 65535. Default: 0. Maximum value: 65535

distance

Administrative distance of this route from the appliance. Default value: STATIC_ROUTE_DEFAULT_DISTANCE Maximum value: 255

weight

Value to facilitate balancing the load on ECMP routes. This value is compared with the hashed value of the packet, and a route is then chosen. Specific to ECMP routes. Default

value: ROUTE_DEFAULT_WEIGHT Minimum value: 1 Maximum value: 65535

advertise

State of advertisement of this route by dynamic routing protocols. Possible values: DISABLED, ENABLED

protocol

Routing protocols used for advertising routes if route advertisement is enabled. Note: For this setting to work, you must configure the dynamic routing protocol from the VTYSH command line. For more information about configuring dynamic routing protocols on the NetScaler appliance, see the "Dynamic Routing" chapter of the Citrix NetScaler Networking Guide.

msr

Monitor this route to verify its reachability through the gateway. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add route 10.10.10.0 255.255.255.0 10.10.10.1

Top

clear route

Synopsis

clear route <routeType>

Description

Remove routes of a particular type from the routing table of the NetScaler appliance.

Parameters

routeType

The type of the route.

Top

rm route

Synopsis

rm route <network> <netmask> <gateway>

Description

Remove a configured static route from the system. You cannot remove direct routes by using this command. Use the rm ip command to remove the direct routes.

Parameters

network

The network address specified in the route entry that you want to remove from the routing table of the NetScaler appliance.

netmask

The subnet mask associated with the network address.

gateway

IP address of the gateway for the route that you want to remove.

Top

set route

Synopsis

set route <network> <netmask> <gateway> [-distance <positive_integer>] [-cost <positive_integer>] [-weight <positive_integer>] [-advertise (DISABLED | ENABLED)] [-protocol <protocol> ...] [-msr (ENABLED | DISABLED) [-monitor <string>]]

Description

Set the attributes of a route that was added by the add route command.

Parameters

network

The network address specified in the route entry that you want to modify.

netmask

The subnet mask associated with the network address.

gateway

The gateway for the destination network of the route.

distance

Administrative distance of this route from the appliance. Default value: STATIC_ROUTE_DEFAULT_DISTANCE Maximum value: 255

cost

The cost of a route is used to compare routes of the same type. The route having the lowest cost is the most preferred route. Possible values: 0 through 65535. Default: 0. Maximum value: 65535

weight

Value to facilitate balancing the load on ECMP routes. This value is compared with the hashed value of the packet, and a route is then chosen. Specific to ECMP routes. Default value: ROUTE_DEFAULT_WEIGHT Minimum value: 1 Maximum value: 65535

advertise

State of advertisement of this route by dynamic routing protocols. Possible values: DISABLED, ENABLED

protocol

Routing protocols used for advertising routes if route advertisement is enabled. Note: For this setting to work, you must configure the dynamic routing protocol from the VTYSH command line. For more information about configuring dynamic routing protocols on the NetScaler appliance, see the "Dynamic Routing" chapter of the Citrix NetScaler Networking Guide.

msr

Monitor this route to verify its reachability through the gateway. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set route 10.10.10.0 255.255.255.0 10.10.10.1 -advertise enable

Top

unset route

Synopsis

unset route <network> <netmask> <gateway> [-advertise] [-protocol <protocol> ...] [-distance] [-cost] [-weight] [-msr] [-monitor]

Description

Unset the attributes of a route that were added by the add/set route command..Refer to the set route command for meanings of the arguments.

Example

unset route 10.10.10.0 255.255.255.0 10.10.10.1 -advertise enable

Top

show route

Synopsis

show route [<network> <netmask> [<gateway>]] [<routeType>] [-detail]

Description

Display the configured routing information.

Parameters

network

The destination network or host.

routeType

The type of routes to be shown.

detail

Display a detailed view.

Example

An example of the output of the show route command is as follows:

3 configured routes:

```
   Network        Netmask        Gateway/OwnedIP     Type
   -------        -------        ---------------     ----
1) 0.0.0.0        0.0.0.0        10.11.0.254         STATIC
2) 127.0.0.0      255.0.0.0      127.0.0.1           PERMANENT
3) 10.251.0.0     255.255.0.0    10.251.0.254        NAT
```

Top

vlan

[add | rm | set | unset | bind | unbind | show | stat]

add vlan

Synopsis

add vlan <id> [-aliasName <string>] [-ipv6DynamicRouting (ENABLED | DISABLED)]

Description

Create a VLAN. Each VLAN is identified by a VID (integer from 1 through 4094). The VLAN created is empty (without members) and is not active until interfaces are bound to it. Initially, all interfaces are bound to VLAN 1, which is created automatically and cannot be deleted.

Parameters

id

An integer that uniquely identifies the VLAN that you want to remove from the NetScaler appliance. Once the VLAN is removed, its interfaces become members of VLAN 1. Minimum value: 1 Maximum value: 4094

aliasName

A name for the VLAN. Must begin with a letter, a number, or the underscore symbol, and can consist of from 1 to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the VLAN. However, you cannot perform any VLAN operation by specifying this name instead of the VLAN ID.

ipv6DynamicRouting

Enable all IPv6 dynamic routing protocols on this VLAN. Possible values: ENABLED, DISABLED Default: DISABLED. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line. For more information about configuring IPv6 dynamic routing protocols on the NetScaler appliance, see the "Dynamic Routing" chapter of the Citrix NetScaler Networking Guide. Possible values: ENABLED, DISABLED Default value: DISABLED

Top

rm vlan

Synopsis

rm vlan <id>

Description

Remove the VLAN created by the add vlan command. Once the VLAN is removed, its interfaces become members of VLAN 1.

Parameters

id

The VLAN Id. Minimum value: 2 Maximum value: 4094

Top

set vlan

Synopsis

set vlan <id> [-aliasName <string>] [-ipv6DynamicRouting (ENABLED | DISABLED)]

Description

Set VLAN parameters.

Parameters

id

An integer that uniquely identifies the VLAN that you want to remove from the NetScaler appliance. Once the VLAN is removed, its interfaces become members of VLAN 1. Minimum value: 1 Maximum value: 4094

aliasName

A name for the VLAN. Must begin with a letter, a number, or the underscore symbol, and can consist of from 1 to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the VLAN. However, you cannot perform any VLAN operation by specifying this name instead of the VLAN ID.

ipv6DynamicRouting

Enable all IPv6 dynamic routing protocols on this VLAN. Possible values: ENABLED, DISABLED Default: DISABLED. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line. For more information about configuring IPv6 dynamic routing protocols on the NetScaler appliance, see the "Dynamic Routing" chapter of the Citrix NetScaler Networking Guide. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set vlan 2 -dynamicRouting ENABLED

Top

unset vlan

Synopsis

unset vlan <id> [-aliasName] [-ipv6DynamicRouting]

Description

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

Top

bind vlan

Synopsis

bind vlan <id> [-ifnum <interface_name> ... [-tagged]] [-IPAddress <ip_addr|ipv6_addr|*> [<netmask>]]

Description

Bind an interface or an IP address to a VLAN. An interface can be bound to a VLAN as a tagged or an untagged interface. Adding an interface as an untagged member (the default) deletes it from its current native VLAN and adds it to the new VLAN. If an interface is added as a tagged member to a VLAN, it still remains a member of its native VLAN.

Parameters

id

Specifies the virtual LAN ID. Minimum value: 1 Maximum value: 4094

ifnum

The interface to be bound to the VLAN, specified in slot/port notation (for example, 1/3). Minimum value: 1

IPAddress

The network address to be associated with the VLAN. This address should exist on the appliance before you associate it with the VLAN.

Top

unbind vlan

Synopsis

unbind vlan <id> [-ifnum <interface_name> ... [-tagged]] [-IPAddress <ip_addr|ipv6_addr|*> [<netmask>]]

Description

Unbind the specified interface from the VLAN. If the interface was an untagged member of this VLAN, it is added to the default VLAN (VLAN 1).

Parameters

id

The virtual LAN (VLAN) id. Minimum value: 1 Maximum value: 4094

ifnum

The interface that you want to unbind from the VLAN, specified in slot/port notation (for example, 1/3). Minimum value: 1

IPAddress

The IP Address associated with the VLAN configuration.

Top

show vlan

Synopsis

show vlan [<id>] show vlan stats - alias for 'stat vlan'

Description

Display the configured VLANs. If an ID is specified, only that particular VLAN information is displayed. Otherwise, all configured VLANs are displayed.

Parameters

id

An integer that uniquely identifies the VLAN for which the details are to be displayed. Minimum value: 1 Maximum value: 4094

Example

An example of the output of the show vlan command is as follows:

```
1)     VLAN ID: 5      VLAN Alias Name:
       Interfaces : 1/7
       IPs :
       10.102.169.36       Mask: 255.255.255.0

2)     VLAN ID: 3      VLAN Alias Name:
       Interfaces : 1/5(T)
       Channels : LA/2
 Done

*(T) - Tagged
```

Top

stat vlan

Synopsis

stat vlan [<id>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics for VLAN(s).

Parameters

id

An integer specifying the VLAN identification number (VID). Possible values: 1 through 4094. Minimum value: 1 Maximum value: 4094

Example

stat vlan 1

Top

vrID

[add | rm | set | unset | bind | unbind | show]

add vrID

Synopsis

add vrID <id> [-priority <positive_integer>] [-preemption (ENABLED | DISABLED)] [-sharing (ENABLED | DISABLED)] [-tracking <tracking>]

Description

This command creates a virtual MAC address (VMAC). Each VMAC is identified by a VRID (integer from 1 through 255). The VMAC created is empty (without members) and is inactive until interfaces are bound to it.

Parameters

id

An integer value that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value: 1. Maximum value: 255. Minimum value: 1 Maximum value: 255

priority

Base priority (BP) that determines the master VIP address. Set this parameter only if you are configuring the appliance in the active-active mode. Default value: 255 Minimum value: 1 Maximum value: 255

preemption

Make a backup VIP address the master if its priority becomes higher than that of a master VIP address bound to this VMAC address. Set this parameter only if you are configuring the appliance in the active-active mode. Possible values: ENABLED, DISABLED Default value: ENABLED

sharing

Enable the backup VIP address to process any traffic, instead of dropping the traffic. Set this parameter only if you are configuring the appliance in the active-active mode. Possible values: ENABLED, DISABLED Default value: DISABLED

tracking

The effective priority (EP) value, relative to the base priority (BP) value. Set this parameter only if you are configuring the appliance in the active-active mode. When EP is set to a value other than None, it is EP, not BP, which determines the master VIP address. For example, if a VIP address on NetScaler appliance NS1 has a priority of 101, and the same VIP address on NS2 has a priority of 99, the VIP address on NS1 is active. However, if two virtual servers are using the VIP address on NS1, and one of them is DOWN, health tracking can reduce the EP of VIP on NS1. VRRP then makes the VIP address on NS2 the active VIP address. Possible values for EP are: NONE. No tracking. EP=BP. (This is the default.) ALL. If the status of all virtual servers is UP, EP=BP. Otherwise, EP=0. ONE. If the status of at least one virtual server is UP, EP=BP. Otherwise, EP=0. PROGRESSIVE. If the status of all virtual servers is UP, EP=BP. If the status of all virtual servers is DOWN, EP=0. Otherwise EP=BP (1 - K/N), where N is the total number of virtual servers associated with the VIP address and K is the number of virtual servers whose status is DOWN. Possible values: NONE, ONE, ALL, PROGRESSIVE Default value: TRACK_NONE

Example

add vrID 1

Top

rm vrID

Synopsis

rm vrID (<id> | -all)

Description

Remove the VRID created by the add command.

Parameters

id

An integer value that uniquely identifies the VMAC address that you want to remove. Minimum value: 1 Maximum value: 255

all

Remove all the configured VMAC addresses from the NetScaler appliance.

Top

set vrID

Synopsis

set vrID <id> [-priority <positive_integer>] [-preemption (ENABLED | DISABLED)] [-sharing (ENABLED | DISABLED)] [-tracking <tracking>]

Description

Set the attributes of a VRID that was added by the add vrID command.

Parameters

id

An integer value that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value: 1. Maximum value: 255. Minimum value: 1 Maximum value: 255

priority

Base priority (BP) that determines the master VIP address. Set this parameter only if you are configuring the appliance in the active-active mode. Default value: 255 Minimum value: 1 Maximum value: 255

preemption

Make a backup VIP address the master if its priority becomes higher than that of a master VIP address bound to this VMAC address. Set this parameter only if you are configuring the appliance in the active-active mode. Possible values: ENABLED, DISABLED Default value: ENABLED

sharing

Enable the backup VIP address to process any traffic, instead of dropping the traffic. Set this parameter only if you are configuring the appliance in the active-active mode. Possible values: ENABLED, DISABLED Default value: DISABLED

tracking

The effective priority (EP) value, relative to the base priority (BP) value. Set this parameter only if you are configuring the appliance in the active-active mode. When EP is set to a value other than None, it is EP, not BP, which determines the master VIP address. For example, if a VIP address on NetScaler appliance NS1 has a priority of 101, and the same VIP address on NS2 has a priority of 99, the VIP address on NS1 is active. However, if two virtual servers are using the VIP address on NS1, and one of them is DOWN, health tracking can reduce the EP of VIP on NS1. VRRP then makes the VIP address on NS2 the active VIP address. Possible values for EP are: NONE. No tracking. EP=BP. (This is the default.) ALL. If the status of all virtual servers is UP, EP=BP. Otherwise, EP=0. ONE. If the status of at least one virtual server is UP, EP=BP.

Otherwise, EP=0. PROGRESSIVE. If the status of all virtual servers is UP, EP=BP. If the status of all virtual servers is DOWN, EP=0. Otherwise EP=BP (1 - K/N), where N is the total number of virtual servers associated with the VIP address and K is the number of virtual servers whose status is DOWN. Possible values: NONE, ONE, ALL, PROGRESSIVE Default value: TRACK_NONE

Example

set vrID 1 -priority 100

Top

unset vrID

Synopsis

unset vrID <id> [-priority] [-preemption] [-sharing] [-tracking]

Description

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

Top

bind vrID

Synopsis

bind vrID <id> -ifnum <interface_name> ...

Description

Bind an interface to a vrID.

Parameters

id

An integer value that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value: 1. Maximum value: 255. Minimum value: 1 Maximum value: 255

ifnum

Interfaces that you want to bind to the VMAC. The format for specifying an interface is slot/port notation (for example, 1/2).

Example

add vrID 1

Top

unbind vrID

Synopsis

unbind vrID <id> -ifnum <interface_name> ...

Description

Unbind specified interfaces from the VRID.

Parameters

id

An integer value that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value: 1. Maximum value: 255. Minimum value: 1 Maximum value: 255

ifnum

Interfaces that you want to unbind from the VMAC. The format for specifying an interface is slot/port notation (for example, 1/2).

Top

show vrID

Synopsis

show vrID [<id>]

Description

Display VRID table.

Parameters

id

An integer value that uniquely identifies the VMAC address. Minimum value: 1 Maximum value: 255

Example

show vrid

Top

vrID6

[add | rm | bind | unbind | show]

add vrID6

Synopsis

add vrID6 <id>

Description

This command creates a virtual MAC address. Each VMAC is identified by a VRID (integer from 1 through 255).The VMAC created is empty (without members) and is inactive until interfaces are bound to it.

Parameters

id

An integer value that uniquely identifies a VMAC6 address. Minimum value: 1 Maximum value: 255

Example

add vrID6 1

Top

rm vrID6

Synopsis

rm vrID6 (<id> | -all)

Description

Remove the VRID created by the add command.

Parameters

id

An integer value that uniquely identifies a VMAC6 address that you want to remove. Minimum value: 1 Maximum value: 255

all

Remove all configured VMAC6 addresses from the NetScaler appliance.

Top

bind vrID6

Synopsis

bind vrID6 <id> -ifnum <interface_name> ...

Description

Bind an interface to a VRID.

Parameters

id

An integer value that uniquely identifies a VMAC6 address. Minimum value: 1 Maximum value: 255

ifnum

Interfaces that you want to bind to the VMAC6. The format for specifying an interface is in slot/port notation, (for example, 1/2).

Example

add vrID6 1

Top

unbind vrID6

Synopsis

unbind vrID6 <id> -ifnum <interface_name> ...

Description

Unbind specified interfaces from the VRID.

Parameters

id

An integer value that uniquely identifies a VMAC6 address. Minimum value: 1 Maximum value: 255

ifnum

Interfaces that you want to unbind from the VMAC6. The format for specifying an interface is slot/port notation (for example, 1/2).

Top

show vrID6

Synopsis

show vrID6 [<id>]

Description

Display VRID6 table.

Parameters

id

An integer value that uniquely identifies a VMAC6 address. Minimum value: 1 Maximum value: 255

Example

show vrid6

Top

route6

[add | clear | rm | set | unset | show]

add route6

Synopsis

add route6 <network> [<gateway>] [-vlan <positive_integer>] [-weight <positive_integer>] [-distance <positive_integer>] [-cost <positive_integer>] [-advertise (DISABLED | ENABLED)] [-msr (ENABLED | DISABLED) [-monitor <string>]]

Description

Add an IPv6 static route to the forwarding table. VLAN number is needed only for link local addresses

Parameters

network

An IPv6 network address for which you want to add a route entry in the routing table of the NetScaler appliance.

gateway

The gateway for this route. The value for this parameter is either an IPv6 address or null.

vlan

An integer that uniquely identifies the VLAN defined for this route. Maximum value: 4094

weight

Value for balancing the load on ECMP routes. This value is compared with the hashed value of the packet, and then a route is chosen. Specific to ECMP routes. Default value: 1 Minimum value: 1 Maximum value: 65535

distance

Administrative distance of this route from the appliance. Default value: 1 Minimum value: 1 Maximum value: 254

cost

The cost of a route is used to compare routes of the same type. The route having the lowest cost is the most preferred route. Default value: 1 Maximum value: 65535

advertise

The state of advertisement of this route. Possible values: DISABLED, ENABLED

msr

Enable MSR on this route. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add route6 ::/0 2004::1 add route6 ::/0 FE80::67 -vlan 5

Top

clear route6

Synopsis

clear route6 <routeType>

Description

Clear the IPv6 routes.

Parameters

routeType

The type of the ipv6 route.

Top

rm route6

Synopsis

rm route6 <network> [<gateway>] [-vlan <positive_integer>]

Description

Remove a configured static route from the appliance.

Parameters

network

The network of the route to be removed.

gateway

The gateway address of the route to be removed.

vlan

An integer that uniquely identifies the VLAN defined for this route. Maximum value: 4094

Example

```
rm route6 ::/0 2004::1
rm route6 ::/0 FE80::67 -vlan 5
```

Top

set route6

Synopsis

set route6 <network> [<gateway>] [-vlan <positive_integer>] [-weight <positive_integer>] [-distance <positive_integer>] [-cost <positive_integer>] [-advertise (DISABLED | ENABLED)] [-msr (ENABLED | DISABLED) [-monitor <string>]]

Description

Set the attributes of a route that was added by the add route command.

Parameters

network

The IPv6 network address of the route entry that you want to modify.

gateway

The gateway for the route's destination network.

vlan

An integer that uniquely identifies the VLAN defined for this route. Maximum value: 4094

weight

Value for balancing the load on ECMP routes. This value is compared with the hashed value of the packet, and then a route is chosen. Specific to ECMP routes. Default value: 1 Minimum value: 1 Maximum value: 65535

distance

Administrative distance of this route from the appliance. Default value: 1 Minimum value: 1 Maximum value: 254

cost

The cost of a route is used to compare routes of the same type. The route having the lowest cost is the most preferred route. Default value: 1 Maximum value: 65535

advertise

The state of advertisement of this route. Possible values: DISABLED, ENABLED

msr

Enable MSR on this route. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set route6 1::1/100 2000::1 -advertise enable

Top

unset route6

Synopsis

unset route6 <network> [<gateway>] [-vlan <positive_integer>] [-weight] [-distance] [-cost] [-advertise] [-msr] [-monitor]

Description

Unset the attributes of a route that were added by the add/set route command..Refer to the set route6 command for meanings of the arguments.

Example

unset route6 2000::1/100 3000::1 -advertise enable

Top

show route6

Synopsis

show route6 [<network> [<gateway>] [-vlan <positive_integer>]] [<routeType>] [-detail]

Description

Display the configured routing information.

Parameters

network

The IPv6 network address of the route entry for which the details are to be displayed.

routeType

The type of IPv6 routes to be to be displayed.

detail

To get a detailed view.

Example

Following is an example of the output of the show route6 command:

```
Flags: Static(S), Dynamic(D), Active(A)
---------------------------------------

Network      Gateway(vlan)   Flags
-------      -----------     -----
0::0/0       2001::1           S(A)
0::0/0       FE80::90(4)       D(A)
```

Top

nd6

[add | clear | rm | show]

add nd6

Synopsis

add nd6 <neighbor> <mac> <ifnum> [-vlan <integer>]

Description

Create a static entry for the ND6 table.

Parameters

neighbor

IPv6 address of the adjacent network device that you want to add to the ND6 table.

mac

MAC address of the adjacent network device.

ifnum

The interface through which the adjacent network device is available, specified in slot/port notation, (for example, 1/3).

vlan

An integer value that uniquely identifies the VLAN on which the adjacent network device exists. Minimum value: 1 Maximum value: 4094

Example

add nd6 2001::1 00:04:23:be:3c:06 5 1/1

Top

clear nd6

Synopsis

clear nd6

Description

Remove all neighbor discovery entries from the NetScaler appliance.

Top

rm nd6

Synopsis

rm nd6 <neighbor> [-vlan <integer>]

Description

Remove a static entry from the NetScaler nd6 table

Parameters

neighbor

Link-local IPv6 address of the adjacent network device that you want to remove from the ND6 table.

vlan

An integer value that uniquely identifies the VLAN for the ND6 entry you want to remove. Minimum value: 1 Maximum value: 4094

Example

rm nd6 2001::1 5 1/1

Top

show nd6

Synopsis

show nd6 [<neighbor>]

Description

Display the neighbor discovery information.

Parameters

neighbor

IPv6 address of the adjacent network device that you want to add to the ND6 table.

Example

Following is an example of the output for the show nd6 command:

```
 Neighbor          MAC-Address(Vlan, Interface)     State      TIME(hh:mm:ss)
 --------          ----------------------------      -----     --------------
 2001::1           00:04:23:be:3c:06(5, 1/1)        REACHABLE  00:00:24
 FE80::123:1       00:04:23:be:3c:07(4, 1/2)         STALE     00:03:34
```

Top

inat

[add | rm | set | unset | show]

add inat

Synopsis

add inat <name>@ <publicIP>@ <privateIP>@ [-tcpproxy (ENABLED | DISABLED)] [-ftp (ENABLED | DISABLED)] [-usip (ON | OFF)] [-usnip (ON | OFF)] [-proxyIP <ip_addr|ipv6_addr>]

Description

Create an inbound NAT with given public and private IP addresses.

Parameters

name

A Name for the Inbound NAT (INAT) entry. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

publicIP

Public IP address of packets received on the NetScaler appliance. Can be either an IPv4 or an IPv6 address. Possible values: NetScaler-owned VIPs.

privateIP

IP address of the server to which the packet is sent by the NetScaler. Can be either an IPv4 or an IPv6 address.

tcpproxy

Enable TCP proxying, which enables the NetScaler appliance to optimize the TCP traffic by using Layer 4 features. Possible values: ENABLED, DISABLED Default value: DISABLED

ftp

Enable the FTP protocol on the server for transferring files between the client and the server. Possible values: ENABLED, DISABLED Default value: DISABLED

usip

Enable the NetScaler appliance to retain the source IP address of the packets before sending the packets to the server. Possible values: ON, OFF Default value: ON

usnip

Enable the NetScaler appliance to use an SNIP address as the source IP address of the packets before sending the packets to the server. Possible values: ON, OFF Default value: ON

proxyIP

proxyIP A unique IP address used as the source IP address in packets sent to the server. Must be a MIP or SNIP address.

Example

add nat mynat 1.2.3.4 192.168.1.100

Top

rm inat

Synopsis

rm inat <name>@

Description

Remove the specified Inbound NAT configuration.

Parameters

name

Name of the Inbound NAT entry to be removed from the NetScaler appliance.

Example

rm nat mynat.

Top

set inat

Synopsis

set inat <name>@ [-privateIP <ip_addr|ipv6_addr>@] [-tcpproxy (ENABLED | DISABLED)] [-ftp (ENABLED | DISABLED)] [-usip (ON | OFF)] [-usnip (ON | OFF)] [-proxyIP <ip_addr|ipv6_addr>]

Description

Modify some of the inbound NAT attributes.

Parameters

name

The name of the Inbound NAT (INAT) entry that you want to modify.

privateIP

IP address of the server to which the packet is sent by the NetScaler. Can be either an IPv4 or an IPv6 address.

tcpproxy

Enable TCP proxying, which enables the NetScaler appliance to optimize the TCP traffic by using Layer 4 features. Possible values: ENABLED, DISABLED Default value: DISABLED

ftp

Enable the FTP protocol on the server for transferring files between the client and the server. Possible values: ENABLED, DISABLED Default value: DISABLED

usip

Enable the NetScaler appliance to retain the source IP address of the packets before sending the packets to the server. Possible values: ON, OFF Default value: ON

usnip

Enable the NetScaler appliance to use an SNIP address as the source IP address of the packets before sending the packets to the server. Possible values: ON, OFF Default value: ON

proxyIP

A unique IP address used as the source IP address in packets sent to the server. Must be a MIP or SNIP address.

Example

set nat mynat -tcpproxy ENABLED

Top

unset inat

Synopsis

unset inat <name>@ [-tcpproxy] [-ftp] [-usip] [-usnip] [-proxyIP]

Description

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

Top

show inat

Synopsis

show inat [<name>]

Description

show all configured inbound NAT.

Parameters

name

A Name for the Inbound NAT (INAT) entry. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

Example

show nat

Top

bridgegroup

[add | rm | set | unset | bind | unbind | show]

add bridgegroup

Synopsis

add bridgegroup <id> [-ipv6DynamicRouting (ENABLED | DISABLED)]

Description

Create a Bridge group.

Parameters

id

An integer that uniquely identifies the bridge group. Minimum value: 1. Maximum value: 1000. Minimum value: 1 Maximum value: 1000

ipv6DynamicRouting

Enable all IPv6 dynamic routing protocols on this VLAN. Possible values: ENABLED, DISABLED Default: DISABLED. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line. For more information about configuring IPv6 dynamic routing protocols on the NetScaler appliance, see the "Dynamic Routing" chapter of the Citrix NetScaler Networking Guide. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add bridgegroup bg1

Top

rm bridgegroup

Synopsis

rm bridgegroup <id>

Description

Remove the bridge group created by the add bridge group command.

Parameters

id

An integer that uniquely identifies the bridge group that you want to remove from the NetScaler appliance. Minimum value: 1 Maximum value: 1000

Top

set bridgegroup

Synopsis

set bridgegroup <id> -ipv6DynamicRouting (ENABLED | DISABLED)

Description

Set Bridge group parameters.

Parameters

id

An integer value that uniquely identifies the bridge group. Minimum value: 1. Maximum value: 1000. Minimum value: 1 Maximum value: 1000

ipv6DynamicRouting

Enable all IPv6 dynamic routing protocols on this bridge group. For this setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line. For more information about configuring IPv6 dynamic routing protocols on the NetScaler appliance, see the Dynamic Routing chapter of the Citrix NetScaler Networking Guide. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set bridgegroup bg1 -dynamicRouting ENABLED

Top

unset bridgegroup

Synopsis

unset bridgegroup <id> -ipv6DynamicRouting

Description

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

Top

bind bridgegroup

Synopsis

bind bridgegroup <id> [-vlan <positive_integer>] [-IPAddress <ip_addr|ipv6_addr|*> [<netmask>]]

Description

Bind a vlan or an ip address to a bridgegroup.

Parameters

id

The integer that uniquely identifies the bridge group. Minimum value: 1 Maximum value: 1000

vlan

An integer that uniquely identifies the VLAN that you want to bind to this bridge group. Minimum value: 2 Maximum value: 4094

IPAddress

A network address or addresses to be associated with the bridge group. You must add entries for these network addresses in the routing table before running this command.

Example

bind bridgegroup bg1 -vlan 2

Top

unbind bridgegroup

Synopsis

unbind bridgegroup <id> [-vlan <positive_integer>] [-IPAddress <ip_addr|ipv6_addr|*> [<netmask>]]

Description

Unbind the specified VLAN or IP address from bridge group.

Parameters

id

The integer that uniquely identifies the bridge group. Minimum value: 1 Maximum value: 1000

vlan

The ID of the VLAN that you want to unbind from this bridge group. Minimum value: 2. Maximum value: 4094. Minimum value: 2 Maximum value: 4094

IPAddress

The network address associated with the bridge group.

Top

show bridgegroup

Synopsis

show bridgegroup [<id>]

Description

Display the configured bridge group. If a name is specified, only that particular bridge group information is displayed. Otherwise, all configured bridge groups are displayed.

Parameters

id

The name of the bridge group. Minimum value: 1 Maximum value: 1000

Example

An example of the output of the show bridge group command is as follows:
2 configured Bridge Group:
1) Bridge Group: 1
Member vlans : 2 3 4
IP: 10.102.33.27 MASK: 255.255.255.0
2) Bridge Group: 2
Member vlans : 5 6

Top

ipTunnel

[add | rm | show]

add ipTunnel

Synopsis

add ipTunnel <name> <remote> <remoteSubnetMask> <local> [-protocol (IPIP | GRE) [-ipsecProfileName <string>]]

Description

Add an ip tunnel.

Parameters

name

Name of the IP Tunnel. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

remote

The remote IP address or subnet of the tunnel.

remoteSubnetMask

Subnet mask of the remote IP address of the tunnel. A public IPv4 address of the remote device used to set up the tunnel. For this parameter, you can also specify a network address if you specify IPIP (IP over IP) for the Protocol parameter.

local

A NetScaler owned public IPv4 address, configured on the local NetScaler appliance and used to set up the tunnel. Possible values: Auto, MIP, SNIP, VIP. Default: Auto.

protocol

The IP tunneling protocol. Possible values: IPIP, GRE Default value: TNL_IPIP

ipsecProfileName

Name of IPSec profile to be associated. Default value: "ns_ipsec_default_profile"

Example

add iptunnel tunnel1 10.100.20.0 255.255.255.0 *

Top

rm ipTunnel

Synopsis

rm ipTunnel <name>

Description

Remove a configured IP tunnel from the system.

Parameters

name

The name of the IP Tunnel that you want to remove from the NetScaler appliance.

Example

rm iptunnel tunnel1

Top

show ipTunnel

Synopsis

show ipTunnel [(<remote> <remoteSubnetMask>) | <name>]

Description

Display the configured IP tunnels.

Parameters

remote

The remote IP address or subnet of the tunnel.

name

Name of the IP Tunnel. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

Example

```
1)  Name.........:  t1
    Remote.......:    10.102.33.0   Mask......:   255.255.255.0
    Local........:              *   Encap.....:       0.0.0.0
    Protocol.....:           IPIP   Type......:             C

2)  Name.........:  tunnel1
    Remote.......:    10.100.20.0   Mask......:   255.255.255.0
    Local........:              *   Encap.....:       0.0.0.0
    Protocol.....:           IPIP   Type......:             C

3)  Name.........:
    Remote.......:   10.102.33.190   Mask......: 255.255.255.255
    Local........:              *   Encap.....:    10.102.33.85
    Protocol.....:           IPIP   Type......:             I
```

Top

ip6Tunnel

[add | rm | show]

add ip6Tunnel

Synopsis

add ip6Tunnel <name> <remote> <local>

Description

Add an ip tunnel.

Parameters

name

The name of the IPv6 tunnel.

remote

The remote IP address or subnet of the tunnel.

local

The local IP address of the tunnel.

Example

add ip6tunnel tun6 9901::200/64 *

Top

rm ip6Tunnel

Synopsis

rm ip6Tunnel <name>

Description

Remove a configured IPv6 tunnel from the system.

Parameters

name

The name of the IPv6 tunnel.

Example

rm ip6tunnel tun6

Top

show ip6Tunnel

Synopsis

show ip6Tunnel [<name> | <remote>]

Description

Display the configured IPv6 tunnels.

Parameters

name

The name of the IPv6 tunnel.

remote

The remote IP address or subnet of the tunnel.

Example

```
1)  Name.........:  tun61
    Remote.......:    9901::200/64  Local........:         *
    Encap.....:       ::0/128       Type......:           C

2)  Name.........:  tun62
    Remote.......:    9903::400/84  Local........:   9903::100
    Encap.....:       ::0/128       Type......:           C

3)  Name.........:
    Remote.......:   9902::300/90    Local........:         *
    Encap.....:     9902::100       Type......:           I
```

Top

netbridge

[add | rm | show | bind | unbind]

add netbridge

Synopsis

add netbridge <name>

Description

Add a network bridge.

Parameters

name

The name of the network bridge.

Example

add netbridge bridge1

Top

rm netbridge

Synopsis

rm netbridge <name>

Description

Remove a network bridge.

Parameters

name

The name of the network bridge.

Example

remove netbridge bridge1

Top

show netbridge

Synopsis

show netbridge [<name>]

Description

Show configured network bridges.

Parameters

name

The name of the network bridge.

Top

bind netbridge

Synopsis

bind netbridge <name> [-tunnel <string> ...] [-vlan <positive_integer> ...] [-IPAddress <ip_addr|ipv6_addr|*> [<netmask>]]

Description

Bind a network bridge to its attributes.

Parameters

name

The name of the network bridge.

tunnel

The name of the tunnel that needs to be a part of this network bridge.

vlan

The VLAN that needs to be extended. Minimum value: 1 Maximum value: 4094

IPAddress

The subnet that needs to be extended.

Example

bind netbridge bridge1 -tunnel tun0

Top

unbind netbridge

Synopsis

unbind netbridge <name> [-tunnel <string> ...] [-vlan <positive_integer> ...] [-IPAddress <ip_addr|ipv6_addr|*> [<netmask>]]

Description

Unbind a network bridge from its attributes.

Parameters

name

The name of the network bridge.

tunnel

The name of the tunnel that is part of this network bridge.

vlan

The vlan that is part of this network bridge. Minimum value: 1 Maximum value: 4094

IPAddress

The subnet that is part of this network bridge.

Example

unbind netbridge bridge1 -tunnel tun0

Top

ipset

[add | rm | bind | unbind | show]

add ipset

Synopsis

add ipset <name>

Description

Add an ipset.

Parameters

name

The name of the IP set.

Example

add ipset pool1

Top

rm ipset

Synopsis

rm ipset <name> ...

Description

Remove an IP set.

Parameters

name

The name of the IP set.

Example

rm ipset pool1

Top

bind ipset

Synopsis

bind ipset <name> <IPAddress>@ ...

Description

Bind an IP address to an IP set.

Parameters

name

The name of the IP set.

IPAddress

One or more IP addresses to be bound to the IP set.

Example

bind ipset ipset_1 10.102.1.10

Top

unbind ipset

Synopsis

unbind ipset <name> <IPAddress>@ ...

Description

Unbind an IP address to an IP set.

Parameters

name

The name of the IP set.

IPAddress

One or more IP addresses to be unbound from the IP set.

Example

unbind ipset ipset_1 10.102.1.10

Top

show ipset

Synopsis

show ipset [<name>]

Description

Show all IP sets, or the set of IP addresses bound to one IP set.

Parameters

name

The name of the IP set.

Example

show network ipset

Top

linkset

[add | rm | bind | unbind | show]

add linkset

Synopsis

add linkset <id>

Description

Adds a linkset to the NetScaler cluster.

Parameters

id

A unique identifier of the linkset. It must be of the form LS/x, where x can be an integer from 1 to 32.

Example

add linkset LS/1

Top

rm linkset

Synopsis

rm linkset <id>

Description

Removes the linkset from the cluster.

Parameters

id

The ID of the linkset that you want to remove.

Example

rm linkset LS/1

Top

bind linkset

Synopsis

bind linkset <id> -ifnum <interface_name> ...

Description

Binds interfaces to the linkset.

Parameters

id

The ID of the linkset to which you want to bind the interfaces.

ifnum

The interfaces to be bound to the linkset.

Example

bind linkset LS/1 -ifnum 1/1/1

Top

unbind linkset

Synopsis

unbind linkset <id> -ifnum <interface_name> ...

Description

Unbinds interfaces from the linkset.

Parameters

id

The ID of the linkset from which you want to unbind the interfaces.

ifnum

The interfaces to be unbound from the linkset.

Example

unbind linkset LS/1 -ifnum 1/1/1

Top

show linkset

Synopsis

show linkset [<id>]

Description

Display details of the linkset.

Parameters

id

The ID of the linkset whose details must be displayed. If an ID is not provided, details of all linksets available in the cluster are displayed.

Example

show linkset

Top

netProfile

[add | rm | set | unset | show]

add netProfile

Synopsis

add netProfile <name> [-srcIP <string>]

Description

Add a network profile.

Parameters

name

The name of the network profile.

srcIP

Source IP address or name of the IP set.

Example

add netProfile prof1 -srcip 10.102.1.10

Top

rm netProfile

Synopsis

rm netProfile <name> ...

Description

Remove a network profile.

Parameters

name

The name of the network profile.

Example

rm netProfile prof1

Top

set netProfile

Synopsis

set netProfile <name> [-srcIP <string>]

Description

Set the IP address or IP set for a network profile.

Parameters

name

The name of the network profile.

srcIP

Source IP address or name of the IP set.

Example

set netProfile prof_1 -srcIP 10.102.1.10

Top

unset netProfile

Synopsis

unset netProfile <name> [-srcIP]

Description

Unset the IP address or IP set for a network profile..Refer to the set netProfile command for meanings of the arguments.

Example

unset netProfile prof1 -srcIP

Top

show netProfile

Synopsis

show netProfile [<name>]

Description

Show all network profiles and the IP addresses or IP sets bound to each profile.

Parameters

name

The name of the network profile.

Example

show netProfile

Top

arpparam

[set | unset | show]

set arpparam

Synopsis

set arpparam [-timeout <positive_integer>] [-spoofValidation (ENABLED | DISABLED)]

Description

Set arp global settings

Parameters

timeout

The ARP table entry aging time, in seconds. Dynamic ARP entries are automatically removed after the specified amount of time Default value: 1200 Minimum value: 5 Maximum value: 1200

spoofValidation

enable/disable arp spoofing validation Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set arpparam -timeout 200 -spoofvalidate ENABLE

Top

unset arpparam

Synopsis

unset arpparam [-timeout] [-spoofValidation]

Description

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

Top

show arpparam

Synopsis

show arpparam

Description

Display ARP global settings.

Example

show arpparam

Top

ci

show ci

Synopsis

show ci

Description

Display all the critical interfaces of the NetScaler appliance. This command is useful in a high availability configuration.

Example

```
>show ci
Critical Interfaces: LO/1 1/2
```

interface

[clear | set | unset | enable | disable | reset | show | stat]

clear interface

Synopsis

clear interface <id>@

Description

Clear the statistics of the specified interface. The interface is not reset. Note: Resetting the interface does not clear the statistics.

Parameters

id

The interface number, in the a/b format, of the interface that needs to be cleared. 'a' can take one of the following values: 1. '0': Indicates a management interface. 2. '1': Indicates a 10/100/1000 Mbps ports and 10G ports of NetScaler 12000-10G and NetScaler MPX 15000 and 17000 platforms. 3. '10': Indicates a 10 Gbps port. 4. 'LA': Indicates a link aggregation port. 5. 'LO': Indicates a loop back port. 'b' is an integer that is used to provide a unique label for the interfaces in the groups defined by 'a'.

Top

set interface

Synopsis

set interface <id>@ [-speed <speed>] [-duplex <duplex>] [-flowControl <flowControl>] [-autoneg (DISABLED | ENABLED)] [-haMonitor (ON | OFF)] [-tagall (ON | OFF)] [-lacpMode <lacpMode>] [-lacpKey <positive_integer>] [-lagtype (NODE | CLUSTER)] [-lacpPriority <positive_integer>] [-lacpTimeout (LONG | SHORT)] [-ifAlias <string>] [-throughput <positive_integer>] [-bandwidthHigh <positive_integer> [-bandwidthNormal <positive_integer>]]

Description

Sets interface attributes such as media parameters (speed, duplex, and so on.), LACP, HA, and VLAN tags.

Parameters

id

The interface number, in a/b format, where 'a' can take one of the following values: 1. '0': Indicates a management interface. 2. '1': Indicates a 10/100/1000 Mbps port, or a 10G port on a NetScaler 12000-10G, NetScaler MPX 15000, or NetScaler 17000 platform. 3. '10': Indicates a 10 Gbps port. 4. 'LA': Indicates a link aggregation port. 5. 'LO': Indicates a loop back port. 'b' is an integer that is used to provide a unique label for the interfaces in the group defined by 'a'.

speed

The requested Ethernet speed of the interface. Possible values are: 1. AUTO: The default value. Specifies that the NetScaler appliance attempts to auto-negotiate or auto-sense the line speed of the interface when it is brought up. 2. 10, 100, 1000, and 10000: 10 Mbps, 100 Mbps, 1 Gbps, and 10 Gbps respectively. Setting a speed other than AUTO requires the device at the other end of the link to be configured identically. Mismatched speed and duplex settings lead to link errors, packet loss, and other errors. Some interfaces do not support certain speeds. If you specify an unsupported speed, an error message appears. Possible values: AUTO, 10, 100, 1000, 10000 Default value: NSA_DVC_SPEED_AUTO

duplex

The requested duplex mode for the interface. Possible values are: 1. AUTO: The default setting. Specifies that the NetScaler appliance attempts to auto-negotiate the duplex mode of the interface when it is brought up. 2. HALF 3. FULL For settings other than AUTO, duplex and speed settings should be identical at both ends of the link. Possible values: AUTO, HALF, FULL Default value: NSA_DVC_DUPLEX_AUTO

flowControl

The requested 802.3x flow control setting for the interface. Possible values are OFF (the default), RX, TX, RXTX, and ON ("forced RXTX"). The 802.3x specification does not define flow control for 10 Mbps and 100 Mbps speeds, but if a Gigabit Ethernet interface operates at those speeds, the flow control settings can be applied. The flow control setting that is finally applied to an interface depends on auto-negotiation. With the ON option, auto-negotiation gives the peer the opportunity to negotiate the flow control, but the appliance then forces two-way flow control for the interface. Any other link-parameter mismatches can sometimes cause problems and should be avoided by thoroughly checking the settings. Possible values: OFF, RX, TX, RXTX Default value: NSA_DVC_FC_OFF

autoneg

The state of auto-negotiation for the specified interface. Possible values are Enabled or Disabled. If auto-negotiation is enabled on an interface, that interface tries to auto-negotiate the speed and duplex settings with the link partner. If the user specifies a speed or duplex setting other then AUTO, auto-negotiation of that parameter does not occur. Possible values: DISABLED, ENABLED Default value: NSA_DVC_AUTONEG_ON

haMonitor

Trigger a failover when the interface on which this option is enabled goes down. By default, this option is enabled on all interfaces. Citrix recommends that this option be

disabled on all unused or noncritical interfaces. Possible values: ON, OFF Default value: NSA_DVC_MONITOR_ON

tagall

The appliance adds a four-byte 802.1q tag to every packet sent on this interface. ON applies tags for all the VLANs that are bound to this interface. OFF, applies the tag for all VLANs other than the native VLAN. Possible values: ON, OFF Default value: NSA_DVC_VTRUNK_OFF

trunk

This argument is deprecated by tagall. Possible values: ON, OFF Default value: NSA_DVC_VTRUNK_OFF

lacpMode

The LACP mode of the specified interface. The possible values are: 1. Active: A port in active mode generates LACP protocol messages on a regular basis, regardless of any need expressed by its partner to receive them. 2. Passive: A port in passive mode generally does not transmit LACP messages unless its partner is in the active mode; that is, it does not speak unless spoken to. 3. Disabled: Removes the interface from the LA channel. If this is only interface in the LA channel, the LA channel is also deleted. Possible values: DISABLED, ACTIVE, PASSIVE Default value: NSA_LACP_DISABLE

lacpKey

A digit that dentifies the LA channel to which the interface is bound. Possible values: 1, 2, 3, 4. Minimum value: 1 Maximum value: 8

lagtype

LAG Type (Node/Cluster) Possible values: NODE, CLUSTER Default value: NSA_LAG_NODE

lacpPriority

LACP port priority, expressed as an integer ranging from 1 to 65535. The highest priority is 1. The NetScaler limits the number of interfaces in an LA channel to 8. If LACP is enabled on more than 8 interfaces, the NetScaler selects 8 interfaces, in decending order of port priority, to form an channel. Default value: 32768 Minimum value: 1 Maximum value: 65535

lacpTimeout

Time to wait for the LACPDU. If a LACPDU is not received within this interval, the NetScaler markes the link partner port as DOWN. Possible values: Long and Short. Long lacptimeout is 90 sec and Short LACP timeout is 3 sec. Possible values: LONG, SHORT Default value: NSA_LACP_TIMEOUT_LONG

ifAlias

The alias name for the interface. Default value: " "

throughput

Minimum required throughput for an interface. Failover is triggered if the operating throughput of a Link Aggregation (LA) channel for which HAMON is ON falls below this value. Maximum value: 80000

bandwidthHigh

Configured high threshold of the interface bandwidth usage in Mbits/s. Trap will be sent if bandwidth usage of the interface goes above this limit. The possible values are: 1. 1000Mbps for 1G interfaces. 2. 10000Mbps for 10G interfaces. 3. 80000Mbps for Link Aggregation channels. Maximum value: 80000

Top

unset interface

Synopsis

unset interface <id>@ [-speed] [-duplex] [-flowControl] [-autoneg] [-haMonitor] [-tagall] [-lacpMode] [-lacpKey] [-lacpPriority] [-lacpTimeout] [-ifAlias] [-throughput] [-bandwidthHigh] [-bandwidthNormal]

Description

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

Top

enable interface

Synopsis

enable interface <id>@

Description

Enable the interface. If the interface is physically UP, it can transmit and receive packets. By default, all interfaces are enabled. Note: To view the status of an interface, use the show interface command.

Parameters

id

The interface number, in a/b format, where 'a' can take one of the following values: 1. '0': Indicates a management interface. 2. '1': Indicates a 10/100/1000 Mbps port, or a 10G port on a NetScaler 12000-10G, NetScaler MPX 15000, or NetScaler 17000 platform. 3. '10': Indicates a 10 Gbps port. 4. 'LA': Indicates a link aggregation port. 5. 'LO': Indicates a

loop back port. 'b' is an integer that is used to provide a unique label for the interfaces in the group defined by 'a'.

Top

disable interface

Synopsis

disable interface <id>@

Description

Disables the interface from transmitting and receiving packets. However, the link remains active and partner devices remain unaware that the interface has been disabled. Interfaces marked for HA monitoring can be disabled, but doing so causes HA failover to occur. Note: To view the status of an interface, use the show interface command.

Parameters

id

The interface number, in a/b format, where 'a' can take one of the following values: 1. '0': Indicates a management interface. 2. '1': Indicates a 10/100/1000 Mbps port, or a 10G port on a NetScaler 12000-10G, NetScaler MPX 15000, or NetScaler 17000 platform. 3. '10': Indicates a 10 Gbps port. 4. 'LA': Indicates a link aggregation port. 5. 'LO': Indicates a loop back port. 'b' is an integer that is used to provide a unique label for the interfaces in the group defined by 'a'.

Top

reset interface

Synopsis

reset interface <id>@

Description

Restart the interface but leaves the administrative state (ENABLED or DISABLED) and configuration unchanged. The link pertaining to the interface is reestablished with the existing settings.

Parameters

id

The interface number, in a/b format, where 'a' can take one of the following values: 1. '0': Indicates a management interface. 2. '1': Indicates a 10/100/1000 Mbps port, or a 10G port on a NetScaler 12000-10G, NetScaler MPX 15000, or NetScaler 17000 platform. 3. '10': Indicates a 10 Gbps port. 4. 'LA': Indicates a link aggregation port. 5. 'LO': Indicates a loop back port. 'b' is an integer that is used to provide a unique label for the interfaces in the group defined by 'a'.

Top

show interface

Synopsis

show interface [<id>@] show interface stats - alias for 'stat interface'

Description

Show the interface settings configured on the appliance for the specified interface number. If id is not specified, the settings are shown for all interfaces (in a brief format).

Parameters

id

The interface number in a/b format, where 'a' can take one of the following values: 1. '0': Indicates a management interface. 2. '1': Indicates a 10/100/1000 Mbps port, or a 10G port on a NetScaler 12000-10G, NetScaler MPX 15000, or NetScaler 17000 platform. 3. '10': Indicates a 10 Gbps port. 4. 'LA': Indicates a link aggregation port. 5. 'LO': Indicates a loop back port. 'b' is an integer that is used to provide a unique label for the interfaces in the group defined by 'a'.

Example

The output for the show interface command is as follows:

1) Interface 0/1 (Gig Ethernet 10/100/1000 MBits) #4
flags=0x4021 <ENABLED, UP, UP, autoneg, HAMON, 802.1q>
MTU=1514, native vlan=1, MAC=00:30:48:67:9a:9a, uptime 1039h54m28s
Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
throughput 0

2) Interface 1/1 (Gig Ethernet, copper SFP) #3
flags=0x4021 <ENABLED, UP, UP, autoneg, HAMON, BACKPLANE, 802.1q>
MTU=1514, native vlan=1, MAC=00:e0:ed:12:e8:b7, uptime 1039h54m28s
Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
throughput 0

3) Interface 1/2 (Gig Ethernet, copper SFP) #2
flags=0x4001 <ENABLED, DOWN, down, autoneg, HAMON, 802.1q>
MTU=1514, native vlan=1, MAC=00:e0:ed:12:e8:b6, downtime 1039h54m28s
Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,

```
        throughput 0

4)   Interface 1/3 (Gig Ethernet, copper SFP) #1
     flags=0x4001 <disabled, DOWN, down, autoneg, HAMON, 802.1q>
     MTU=1514, native vlan=1, MAC=00:e0:ed:12:e8:b5, downtime 1039h54m33s
     Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
        throughput 0

5)   Interface 1/4 (Gig Ethernet, copper SFP) #0
     flags=0x4001 <disabled, UP, down, autoneg, HAMON, 802.1q>
     MTU=1514, native vlan=1, MAC=00:e0:ed:12:e8:b4, downtime 1039h54m28s
     Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
        throughput 0

 Done
>
```

The output for the show interface 0/1 command is as follows:

```
     Interface 0/1 (Gig Ethernet 10/100/1000 MBits) #4
     flags=0xc020 <ENABLED, UP, UP, autoneg, HAMON, 802.1q>
     MTU=1514, native vlan=1, MAC=00:30:48:67:9a:9a, uptime 0h00m40s
     Requested: media AUTO, speed AUTO, duplex AUTO, fctl RXTX,
        throughput 0
     Actual: media UTP, speed 1000, duplex FULL, fctl RXTX, throughput 1000

     RX: Pkts(27) Bytes(2034) Errs(0) Drops(27) Stalls(0)
     TX: Pkts(3) Bytes(170) Errs(0) Drops(22) Stalls(0)
     NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
     Bandwidth thresholds are not set.

 Done
>
```

Top

stat interface

Synopsis

stat interface [<id>@] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of interface(s).

Parameters

id

The interface number, in a/b format, where 'a' can take one of the following values: 1. '0': Indicates a management interface. 2. '1': Indicates a 10/100/1000 Mbps port, or a 10G port on a NetScaler 12000-10G, NetScaler MPX 15000, or NetScaler 17000 platform. 3. '10': Indicates a 10 Gbps port. 4. 'LA': Indicates a link aggregation port. 5. 'LO': Indicates a loop back port. 'b' is an integer that is used to provide a unique label for the interfaces in the group defined by 'a'.

Top

rnat

[clear | set | unset | stat | show]

clear rnat

Synopsis

clear rnat ((<network> [<netmask>]) | (<aclname> [-redirectPort])) [-natIP <ip_addr|*>@ ...]

Description

Clear the Reverse NAT configuration.

Parameters

network

The network address defined for the RNAT entry.

netmask

The subnet mask for the network address.

aclname

An extended ACL defined for the RNAT entry.

redirectPort

Port number to which the packets are redirected. Applicable to TCP and UDP protocols

natIP

The NAT IP address defined for the RNAT entry.

Top

set rnat

Synopsis

set rnat ((<network> [<netmask>] [-natIP <ip_addr|*>@ ...]) | (<aclname> [-redirectPort <port>] [-natIP <ip_addr|*>@ ...]))

Description

Configure Reverse NAT on the system.

Parameters

network

The network address defined for the RNAT entry.

aclname

An extended ACL defined for the RNAT entry.

Top

unset rnat

Synopsis

unset rnat ((<network> [<netmask>]) | (<aclname> [-redirectPort])) [-natIP <ip_addr|*>@ ...]

Description

Use this command to modify the parameters of configured Reverse NAT on the system..Refer to the set rnat command for meanings of the arguments.

Top

stat rnat

Synopsis

stat rnat [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics for rnat sessions.

Example

stat rnat

Top

show rnat

Synopsis

show rnat

Description

Display the Reverse NAT configuration.

Top

bridgetable

[set | unset | show | clear]

set bridgetable

Synopsis

set bridgetable -bridgeAge <positive_integer>

Description

Set the aging time for bridge table entries. Dynamic bridge entries are automatically removed after a specified period time (the "aging time") since the entry was created or last updated has elapsed.

Parameters

bridgeAge

The time-out value for the bridge table entries, in seconds. The new value applies only to the entries that are dynamically learned after the new value is set. Previously existing bridge table entries expire after the previously configured time-out value. Minimum value: 60. Maximum value: 300. Default: 300. Default value: 300 Minimum value: 60 Maximum value: 300

Example

set bridgetable -bridgeAge 200

Top

unset bridgetable

Synopsis

unset bridgetable -bridgeAge

Description

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

Top

show bridgetable

Synopsis

show bridgetable

Description

Display the bridge aging time and bridging table.

Example

show bridgetable

Top

clear bridgetable

Synopsis

clear bridgetable [-vlan <positive_integer>] [-ifnum <interface_name>]

Description

Remove entries from bridge table

Parameters

vlan

VLAN whose entries are to be removed.

ifnum

INTERFACE whose entries are to be removed.

Top

bridge

stat bridge

Synopsis

stat bridge [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display bridging statistics.

lacp

[set | show]

set lacp

Synopsis

set lacp -sysPriority <positive_integer>

Description

Set the LACP system priority.

Parameters

sysPriority

LACP system priority Default value: 32768 Minimum value: 1 Maximum value: 65535

Top

show lacp

Synopsis

show lacp

Description

Display the LACP configuration.

Top

rnatparam

[set | unset | show]

set rnatparam

Synopsis

set rnatparam -tcpproxy (ENABLED | DISABLED)

Description

Set the rnat parameter

Parameters

tcpproxy

The state of tcpproxy. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set rnat parameter -tcpproxy ENABLED

Top

unset rnatparam

Synopsis

unset rnatparam -tcpproxy

Description

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

Top

show rnatparam

Synopsis

show rnatparam

Description

Show the rnat parameter.

Example

show rnat parameter

Top

rnatip

stat rnatip

Synopsis

stat rnatip [<rnatip>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics for RNAT sessions.

Parameters

rnatip

Specifies the NAT IP address of the configured RNAT entry for which you want to see the statistics. If you do not specify an IP address, this displays the statistics for all the configured RNAT entries.

Example

stat rnatip 1.1.1.1

vrIDParam

[set | unset | show]

set vrIDParam

Synopsis

set vrIDParam -sendToMaster (ENABLED | DISABLED)

Description

Set the VRID global settings on the NetScaler

Parameters

sendToMaster

Forward packets to the master node, in an active-active mode configuration, if the virtual server is in the backup state and sharing is disabled. Possible values: ENABLED, DISABLED. Default: DISABLED. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set vrIDParam -sendToMaster ENABLED

Top

unset vrIDParam

Synopsis

unset vrIDParam -sendToMaster

Description

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

Top

show vrIDParam

Synopsis

show vrIDParam

Description

Display the VRID global settings on the NetScaler appliance.

Top

ipv6

[set | unset | show]

set ipv6

Synopsis

set ipv6 [-ralearning (ENABLED | DISABLED)] [-natprefix <ipv6_addr|*>]

Description

Set IPv6 specific parameters RA Learning and IPv6 NAT Prefix.

Parameters

ralearning

Enable the NetScaler appliance to learn about various routes from RA and RS messages sent by the routers. Possible values: ENABLED, DISABLED Default value: DISABLED

natprefix

The prefix used for translating packets received from private IPv6 servers into IPv4 packets. This prefix has a length of 96 bits (128-32 = 96). The IPv6 servers embed the destination IP address of the IPv4 servers or hosts in the last 32 bits of the destination IP address field of the IPv6 packets. The first 96 bits of the destination IP address field are set as the IPv6 NAT prefix. IPv6 packets addressed to this prefix have to be routed to the NetScaler appliance to ensure that the IPv6-IPv4 translation is done by the appliance.

Example

set ipv6 -natprefix 2000::/96

Top

unset ipv6

Synopsis

unset ipv6 [-ralearning] [-natprefix]

Description

Use this command to remove ipv6 settings.Refer to the set ipv6 command for meanings of the arguments.

Top

show ipv6

Synopsis

show ipv6

Description

Display IPv6 settings

Example

show ipv6

Top

ipTunnelParam

[set | unset | show]

set ipTunnelParam

Synopsis

set ipTunnelParam [-srcIP <ip_addr>] [-dropFrag (YES | NO)] [-dropFragCpuThreshold <positive_integer>] [-srcIPRoundRobin (YES | NO)]

Description

Set the IP Tunnel global settings on the NetScaler

Parameters

srcIP

The common source IP address for all tunnels. For a specific tunnel, this global setting is overridden if you have specified another source IP address. Must be a MIP or SNIP address.

dropFrag

Drop any IP packet that requires fragmentation before it is sent through the tunnel. Possible values: YES, NO Default value: NO

dropFragCpuThreshold

Threshold value, as a percentage of CPU usage, at which to drop packets that require fragmentation to use the IP tunnel. Applies only if dropFrag paramenter is set to NO. Minimum value: 1. Maximum value: 100. Default: 0 (not set). Minimum value: 1 Maximum value: 100

srcIPRoundRobin

If the source IP is not configured, apply round-robin selection from the configured SNIPs. Possible values: YES, NO Default value: NO

Example

set ipTunnelParam -srcIP 10.100.20.48 -dropFrag YES -dropFragCpuThreshold 95

Top

unset ipTunnelParam

Synopsis

unset ipTunnelParam [-srcIP] [-dropFrag] [-dropFragCpuThreshold] [-srcIPRoundRobin]

Description

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

Top

show ipTunnelParam

Synopsis

show ipTunnelParam

Description

Display the IP Tunnel global settings on the NetScaler

Example

Tunnel Source IP: 10.100.20.48
Drop if Fragmentation Needed: YES
CPU usage threshold to avoid fragmentation: 95

Top

ip6TunnelParam

[set | unset | show]

set ip6TunnelParam

Synopsis

set ip6TunnelParam [-srcIP <ipv6_addr|null>] [-dropFrag (YES | NO)]
[-dropFragCpuThreshold <positive_integer>] [-srcIPRoundRobin (YES | NO)]

Description

Set the IPv6 tunnel global settings on the NetScaler

Parameters

srcIP

The source IP address used for all IPv6 tunnels, except those configured by using the add iptunnel command.

dropFrag

Drop an IPv6 packet if fragmentation is required to tunnel it. Possible values: YES, NO Default value: NO

dropFragCpuThreshold

Drop an IP6 packet if fragmentation is required to tunnel it and CPU usage is above this threshold. Minimum value: 1 Maximum value: 100

srcIPRoundRobin

If the source IP address is not configured, apply round-robin selection from the configured SNIPs. Possible values: YES, NO Default value: NO

Example

set ip6TunnelParam -srcIP 9901::100 -dropFrag YES -dropFragCpuThreshold 95

Top

unset ip6TunnelParam

Synopsis

unset ip6TunnelParam [-srcIP] [-dropFrag] [-dropFragCpuThreshold] [-srcIPRoundRobin]

Description

Unset the IPv6 tunnel global settings on the NetScaler.Refer to the set ip6TunnelParam command for meanings of the arguments.

Example

unset ip6TunnelParam -srcIP -dropFrag -dropFragCpuThreshold

Top

show ip6TunnelParam

Synopsis

show ip6TunnelParam

Description

Display the IPv6 Tunnel global settings on the NetScaler

Example

Tunnel Source IP: 9901::100
Drop if Fragmentation Needed: YES
CPU usage threshold to avoid fragmentation: 95

Top

L2Param

[set | unset | show]

set L2Param

Synopsis

set L2Param [-mbfPeermacUpdate <positive_integer>] [-maxBridgeCollision <positive_integer>] [-bdggrpProxyArp (ENABLED | DISABLED)] [-bdgSetting (ENABLED | DISABLED)] [-garpOnVridIntf (ENABLED | DISABLED)] [-macModeFwdMyPkt (ENABLED | DISABLED)] [-useMyMAC (ENABLED | DISABLED)] [-proxyArp (ENABLED | DISABLED)] [-garpReply (ENABLED | DISABLED)] [-mbfInstLearning (ENABLED | DISABLED)] [-rstIntfOnHaFo (ENABLED | DISABLED)] [-skipProxyingBsdTraffic (ENABLED | DISABLED)]

Description

Set Layer 2 related global settings on the NetScaler

Parameters

mbfPeermacUpdate

When mbf_instant_learning is enabled, learn any changes in peer's MAC after this time interval, which is in 10ms ticks. Default value: 10

maxBridgeCollision

Maximum bridge collision for loop detection Default value: 20

bdggrpProxyArp

Set/reset proxy ARP in bridge group deployment Possible values: ENABLED, DISABLED Default value: ENABLED

bdgSetting

Bridging settings for C2C behavior Possible values: ENABLED, DISABLED Default value: DISABLED

garpOnVridIntf

Send GARP messagess on VRID-configured interfaces upon failover Possible values: ENABLED, DISABLED Default value: ENABLED

macModeFwdMyPkt

MAC mode vserver forward packets destined to VIPs. Possible values: ENABLED, DISABLED Default value: DISABLED

useMyMAC

Set/reset cfg_use_my_mac Possible values: ENABLED, DISABLED Default value: DISABLED

proxyArp

Set/reset cfg_proxy_arp_dr Possible values: ENABLED, DISABLED Default value: ENABLED

garpReply

Set/reset REPLY form of GARP Possible values: ENABLED, DISABLED Default value: DISABLED

mbfInstLearning

Enable instant learning of MAC changes in MBF mode. Possible values: ENABLED, DISABLED Default value: DISABLED

rstIntfOnHaFo

Enable the reset interface upon HA failover. Possible values: ENABLED, DISABLED Default value: DISABLED

skipProxyingBsdTraffic

Enable the proxying of FreeBSD traffic. Possible values: ENABLED, DISABLED Default value: DISABLED

Top

unset L2Param

Synopsis

unset L2Param [-mbfPeermacUpdate] [-maxBridgeCollision] [-bdggrpProxyArp] [-bdgSetting] [-garpOnVridIntf] [-macModeFwdMyPkt] [-useMyMAC] [-proxyArp] [-garpReply] [-mbfInstLearning] [-rstIntfOnHaFo] [-skipProxyingBsdTraffic]

Description

Use this command to remove L2Param settings.Refer to the set L2Param command for meanings of the arguments.

Top

show L2Param

Synopsis

show L2Param

Description

Set Layer 2 related global settings on the NetScaler

Top

L3Param

[set | unset | show]

set L3Param

Synopsis

set L3Param [-srcnat (ENABLED | DISABLED)] [-icmpGenRateThreshold <positive_integer>] [-overrideRnat (ENABLED | DISABLED)] [-dropDFFlag (ENABLED | DISABLED)] [-mipRoundRobin (ENABLED | DISABLED)] [-externalLoopBack (ENABLED | DISABLED)] [-tnlPmtuWoConn (ENABLED | DISABLED)] [-usipServerStrayPkt (ENABLED | DISABLED)] [-forwardICMPFragments (ENABLED | DISABLED)]

Description

Set Layer 3 related global settings on the NetScaler

Parameters

srcnat

Perform NAT if only the source is in the private network Possible values: ENABLED, DISABLED Default value: ENABLED

icmpGenRateThreshold

NS generated ICMP pkts per 10ms rate threshold Default value: 100

overrideRnat

USNIP/USIP settings override RNAT settings for configured service/virtual server traffic.. Possible values: ENABLED, DISABLED Default value: DISABLED

dropDFFlag

Enable dropping the IP DF flag. Possible values: ENABLED, DISABLED Default value: DISABLED

mipRoundRobin

Enable round robin usage of mapped IPs. Possible values: ENABLED, DISABLED Default value: ENABLED

externalLoopBack

Enable external loopback. Possible values: ENABLED, DISABLED Default value: DISABLED

tnlPmtuWoConn

Enable external loopback. Possible values: ENABLED, DISABLED Default value: ENABLED

usipServerStrayPkt

Enable detection of stray server side pkts in USIP mode. Possible values: ENABLED, DISABLED Default value: DISABLED

forwardICMPFragments

Enable forwarding of ICMP fragments. Possible values: ENABLED, DISABLED Default value: DISABLED

Top

unset L3Param

Synopsis

unset L3Param [-srcnat] [-icmpGenRateThreshold] [-overrideRnat] [-dropDFFlag] [-mipRoundRobin] [-externalLoopBack] [-tnlPmtuWoConn] [-usipServerStrayPkt] [-forwardICMPFragments]

Description

Use this command to remove L3Param settings.Refer to the set L3Param command for meanings of the arguments.

Top

show L3Param

Synopsis

show L3Param

Description

Get Layer 3 related global settings on the NetScaler

Top

forwardingSession

[add | set | rm | show]

add forwardingSession

Synopsis

add forwardingSession <name> ((<network> <netmask>) | -aclname <string>) [-connfailover (ENABLED | DISABLED)]

Description

Configure a forwarding session on the appliance.

Parameters

name

Name of forwarding session.

network

The network or subnet from/to which the traffic is flowing.

aclname

The ACL name.

connfailover

Specifies the connection failover mode of the forwarding session. Possible values: ENABLED, DISABLED Default value: DISABLED

Top

set forwardingSession

Synopsis

set forwardingSession <name> [-connfailover (ENABLED | DISABLED)]

Description

Set the configured forwarding session.

Parameters

name

Name of forwarding session.

connfailover

Specifies the connection failover mode of the forwarding session. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set forwardsession fw1 -connfailover enabled.

Top

rm forwardingSession

Synopsis

rm forwardingSession <name>

Description

Remove the configured forwarding session.

Parameters

name

Name of forwarding session.

Example

rm forwardsession name.

Top

show forwardingSession

Synopsis

show forwardingSession [<name>]

Description

Display the forwarding-session configuration.

Parameters

name

Name of forwarding session.

Top

ptp

[set | show]

set ptp

Synopsis

set ptp -state (DISABLE | ENABLE)

Description

Sets the state of Precision Time Protocol (PTP) on the cluster. PTP is used to synchronize the time across the cluster nodes.

Parameters

state

Running State of Precision Time Protocol (PTP) on the cluster. When enabled, PTP synchronizes the time on the cluster nodes. Otherwise, you can configure NTP (on the cluster IP address) to synchronize the time on the cluster nodes. Possible values: DISABLE, ENABLE Default value: NSA_PTP_ENABLE

Top

show ptp

Synopsis

show ptp

Description

Get PTP State

Top

rnat6

[add | bind | unbind | set | unset | clear | show]

add rnat6

Synopsis

add rnat6 <name> (<network> | (<acl6name> [-redirectPort <port>]))

Description

Add a rnat6 entry

Parameters

name

Name of the RNAT6.

network

ipv6 network address for rnat with prefix len CIDR notations (<ipv6 address>/<prefix len>)

acl6name

The acl6 name.

Example

add rnat6 rnat6_name 2002::/64

Top

bind rnat6

Synopsis

bind rnat6 <name> <natIP6>@ ...

Description

Bind RNAT IP6 address to RNAT^ entry

Parameters

name

Name of the RNAT6.

natIP6

One or more IP addresses to be bound to the IP set.

Example

bind rnat6 <rnat6_name> <natIP6>@ ...

Top

unbind rnat6

Synopsis

unbind rnat6 <name> <natIP6>@ ...

Description

Unbind an IP address to an IP set.

Parameters

name

Name of the RNAT6.

natIP6

One or more IP addresses to be unbound from the rnat6 entry.

Example

unbind rnat6 <rnat6_name> <natIP6>@ ...

Top

set rnat6

Synopsis

set rnat6 <name> [-redirectPort <port>]

Description

Set the rnat6 parameters for a rnat6 config

Parameters

name

Name of the RNAT6.

redirectPort

The redirect port. Minimum value: 1 Maximum value: 65535

Top

unset rnat6

Synopsis

unset rnat6 <name> [-redirectPort]

Description

Configure Reverse ipv6 NAT on the system..Refer to the set rnat6 command for meanings of the arguments.

Top

clear rnat6

Synopsis

clear rnat6 <name>

Description

Configure Reverse ipv6 NAT on the system.

Parameters

name

Name of the RNAT6.

Top

show rnat6

Synopsis

show rnat6 [<name>]

Description

Display the Reverse NAT configuration.

Parameters

name

Name of the RNAT6.

Top

NS Commands

This group of commands can be used to perform operations on the following entities:

- shutdown
- reboot
- ns
- ns limitIdentifier
- ns acl
- ns acl6
- ns ip6
- ns ip
- ns simpleacl
- ns simpleacl6
- ns pbr
- ns xmlnamespace
- ns tcpProfile
- ns httpProfile
- ns stats
- ns ns.conf
- ns savedConfig
- ns runningConfig
- ns acls
- ns info
- ns license
- ns version
- ns config
- ns param

- ns acls6
- ns pbrs
- ns connectiontable
- ns limitSessions
- ns hostName
- ns surgeQ
- ns feature
- ns mode
- ns dhcpParams
- ns dhcpIp
- ns spParams
- ns tcpbufParam
- ns tcpParam
- ns httpParam
- ns weblogparam
- ns diameter
- ns rateControl
- ns rpcNode
- ns timeout
- ns hardware
- ns events
- ns encryptionParams
- ns rollbackcmd
- ns memory
- ns pbr6

shutdown

shutdown

Synopsis

shutdown

Description

Use this command to stop the operations of the system on which you are issuing this command. After you enter this command, you can turn off power to the system. Notes 1. When a standalone system is rebooted, all configuration changes made since the last save ns config command was issued are lost. 2. In High Availability mode, on running this command on the primary system, the secondary system takes over and will have the configuration changes made since the last time that the save ns config command was issued on the primary system. In this case, log on to the new primary system, then issue the save ns config CLI command to save these changes.

reboot

reboot

Synopsis

reboot [-warm]

Description

Use this command to restart a system. Notes: 1. When a standalone system is rebooted, all configuration changes made since the last save ns config command was issued are lost. 2. In High Availability mode, on running this command on the primary system, the secondary system takes over and will have the configuration changes made since the last time that the save ns config command was issued on the primary system. In this case, log on to the new primary system, then issue the save ns config CLI command to save these changes. 3. On nCore systems, NetScaler will restart without rebooting the system if the 'warm' option is specified. The CLI session will terminate and the user will not be able to log back into the system until the restart has completed.

Parameters

warm

When specified on nCore systems, the command restarts the NetScaler without requiring a system reboot. On Classic systems, this flag is ignored.

ns

[config | stat]

config ns

Synopsis

config ns

Description

Use this command to display the system's configuration menu. By choosing items from the menu and following the instructions on the screen, each of the configuration parameters can be modified. On entering the config CLI command, the following menu is displayed: Note: The values inside the square brackets indicate the current value of the parameters. > config ns NSCONFIG NS6.1. Reading the system configuration from the file /etc/ns.conf REVIEW CONFIGURATION PARAMETERS MENU ---------- This menu allows you to view and/or modify the system's configuration. Each configuration parameter displays its current value within brackets if it has been set. To change a value, enter the number that is displayed next to it. ---------- 1. System's IP address: [10.102.7.101] 2. Netmask: [255.255.255.0] 3. Advanced Network Configuration. 4. Time zone. 5. Cancel all the changes and exit. 6. Apply changes and exit. Select a menu item from 1 to 6 [6]: System is running. Writing the System configuration into the file /etc/ns.conf System must be rebooted to apply configuration changes. Do you want to reboot System now? [NO]: Done Notes: 1. The system needs to be rebooted every time an item on this menu is changed and the changes saved. 2. This command only modifies and saves the basic configuration set in the ns.conf file (using the set ns config command). It does not save the running configuration changes applied after the last invocation of the save ns config command. If you have applied changes to your running configuration, then you should save them with save ns config command before using the config ns command. See the note on the reboot ns command.

Top

stat ns

Synopsis

stat ns [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display general system statistics.

Top

ns limitIdentifier

[add | rm | set | unset | show]

add ns limitIdentifier

Synopsis

add ns limitIdentifier <limitIdentifier> [-threshold <positive_integer>] [-timeSlice <positive_integer>] [-mode <mode> [-limitType (BURSTY | SMOOTH)]] [-selectorName <string>] [-maxBandwidth <positive_integer>] [-trapsInTimeSlice <positive_integer>]

Description

Create a limit identifier.

Parameters

limitIdentifier

The name of rate limit identifier.

threshold

The maximum number of requests that are allowed in the given timeslice when requests are tracked per timeslice. When connections (-mode CONNECTION)are tracked its the total number of connections that would be let through Default value: 1 Minimum value: 1

timeSlice

Defines the time interval in msecs specified in multiples of 10 msec during which the requests are tracked to see if they cross the threshold. It is used only when the mode is REQUEST_RATE while tracking request rate and for defining the trap timeslice Default value: 1000 Minimum value: 10

mode

Defines what is tracked - request rate, connections or none. Request rate is used to track requests/timeslice, connections will track active transactions. For DNS please use the mode as either NONE or REQUEST_RATE as CONNECTION is not supported. Eg: 1) add limitidentifier limit_req -mode request_rate -limitType smooth -timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200 will permit 20 requests in 10 ms and 2 Traps in 10 ms 2) set limitidentifier limit_req -timeslice 1000 -Threshold 5000 -limitType smooTH will permit 50 Requests in 10 ms 3) set limitidentifier limit_req -mode smooth -timeslice 2000 -Threshold 50 will permit 1 request in 40 ms 4) set limitidentifier limit_req -timeslice 1000 -Threshold 5 -limitType smooth -trapsInTimeSlice 8 will permit 1 request in 200 ms and 1 Trap in 130 ms 5) set limitidentifier limit_req -timeslice 1000 -Threshold

5000 -limitType BURSTY will permit 5000 Requests in 1000 ms and 200 Traps in 1000 ms As you see in the above examples smooth mode is used when one wants the permitted number of requests in a given interval of time to be spread evenly across the timeslice while bursty is used when one is ok to let the permitted number of requests to exhaust the quota anytime within the timeslice. Possible values: CONNECTION, REQUEST_RATE, NONE Default value: PEMGMT_RLT_MODE_REQ_RATE

limitType

Specifies if it is a smooth or bursty request type. If the smooth mode of operation is chosen requests are tracked at the rate of 10 ms. To be specified with -mode REQUEST_RATE . Possible values: BURSTY, SMOOTH Default value: PEMGMT_RLT_REQ_RATE_TYPE_BURSTY

selectorName

The name of rate limit selector.

maxBandwidth

The maximum bandwidth permitted in kbps Maximum value: 4294967287

trapsInTimeSlice

Number of traps that would be sent in the timeslice configured. A value of zero means that the traps are disabled. Maximum value: 65535

Example

add ns limitIdentifier limit_id -threshold 2 -timeSlice 5000 -mode CONNECTION -selectorName sel_1 -maxBa

Top

rm ns limitIdentifier

Synopsis

rm ns limitIdentifier <limitIdentifier>

Description

The command deletes the rate limit identifier.

Parameters

limitIdentifier

The name of rate limit identifier.

Example

rm ns limitIdentifier limit_id

Top

set ns limitIdentifier

Synopsis

set ns limitIdentifier <limitIdentifier> [-threshold <positive_integer>] [-timeSlice <positive_integer>] [-mode <mode> [-limitType (BURSTY | SMOOTH)]] [-selectorName <string>] [-maxBandwidth <positive_integer>] [-trapsInTimeSlice <positive_integer>]

Description

set limit identifier params.

Parameters

limitIdentifier

The name of rate limit identifier.

threshold

The maximum number of requests that are allowed in the given timeslice when requests are tracked per timeslice. When connections (-mode CONNECTION)are tracked its the total number of connections that would be let through Default value: 1 Minimum value: 1

timeSlice

Defines the time interval in msecs specified in multiples of 10 msec during which the requests are tracked to see if they cross the threshold. It is used only when the mode is REQUEST_RATE while tracking request rate and for defining the trap timeslice Default value: 1000 Minimum value: 10

mode

Defines what is tracked - request rate, connections or none. Request rate is used to track requests/timeslice, connections will track active transactions. For DNS please use the mode as either NONE or REQUEST_RATE as CONNECTION is not supported. Eg: 1) add limitidentifier limit_req -mode request_rate -limitType smooth -timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200 will permit 20 requests in 10 ms and 2 Traps in 10 ms 2) set limitidentifier limit_req -timeslice 1000 -Threshold 5000 -limitType smooTH will permit 50 Requests in 10 ms 3) set limitidentifier limit_req -mode smooth -timeslice 2000 -Threshold 50 will permit 1 request in 40 ms 4) set limitidentifier limit_req -timeslice 1000 -Threshold 5 -limitType smooth -trapsInTimeSlice 8 will permit 1 request in 200 ms and 1 Trap in 130 ms 5) set limitidentifier limit_req -timeslice 1000 -Threshold 5000 -limitType BURSTY will permit 5000 Requests in 1000 ms and 200 Traps in 1000 ms As you see in the above examples smooth mode is used when one wants the permitted number of requests in a given interval of time to be spread evenly across the timeslice while bursty is used when one is ok to let the permitted number of requests to exhaust

the quota anytime within the timeslice. Possible values: CONNECTION, REQUEST_RATE, NONE Default value: PEMGMT_RLT_MODE_REQ_RATE

selectorName

The name of rate limit selector.

maxBandwidth

The maximum bandwidth permitted in kbps Maximum value: 4294967287

trapsInTimeSlice

Number of traps that would be sent in the timeslice configured. A value of zero means that the traps are disabled. Maximum value: 65535

Example

set ns limitIdentifier limit_id -threshold 2 -timeSlice 5000 -mode CONNECTION -selectorName sel_1 -maxBar

Top

unset ns limitIdentifier

Synopsis

unset ns limitIdentifier <limitIdentifier> [-selectorName] [-threshold] [-timeSlice] [-mode] [-limitType] [-maxBandwidth] [-trapsInTimeSlice]

Description

Use this command to remove ns limitIdentifier settings.Refer to the set ns limitIdentifier command for meanings of the arguments.

Top

show ns limitIdentifier

Synopsis

show ns limitIdentifier [<limitIdentifier>]

Description

Display rate limit identifiers.

Parameters

limitIdentifier

The name of the rate limit identifier.

Example

show ns limitIdentifier limit_id

Top

ns acl

[add | rm | set | unset | enable | disable | stat | rename | show]

add ns acl

Synopsis

add ns acl <aclname> <aclaction> [-srcIP [<operator>] <srcIPVal>] [-srcPort [<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-destPort [<operator>] <destPortVal>] [-TTL <positive_integer>] [-srcMac <mac_addr>] [(-protocol <protocol> [-established]) | -protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-icmpType <positive_integer> [-icmpCode <positive_integer>]] [-priority <positive_integer>] [-state <state>] [-logstate (ENABLED | DISABLED) [-ratelimit <positive_integer>]]

Description

Add an ACL to the System configuration. Each inbound packet is matched against configured ACLs and the specified action is applied to the packet. This command adds the acl to the configuration space. To commit this ACL, one should apply the ACL.

Parameters

aclname

The alphanumeric name of the ACL.

aclaction

The action associated with the ACL. Possible values: BRIDGE, DENY, ALLOW

srcIP

The source IP address (range).

srcPort

The source Port (range).

destIP

The destination IP address (range).

destPort

The destination Port (range).

TTL

The time to expire this ACL(in seconds). Minimum value: 1 Maximum value: 2147483647

srcMac

The source MAC address.

protocol

The IP protocol name. Possible values: ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS

protocolNumber

The IP protocol number (decimal). Minimum value: 1 Maximum value: 255

vlan

The VLAN number. Minimum value: 1 Maximum value: 4094

interface

The physical interface.

established

This argument indicates that the ACL should be used for TCP response traffic only.

icmpType

The ICMP message type, valid values are 0-255 Maximum value: 65536

icmpCode

The ICMP message code, valid values are 0-255 Maximum value: 65536

priority

The priority of the ACL. Minimum value: 1 Maximum value: 100000

state

The state of the ACL. Possible values: ENABLED, DISABLED, REMOVED Default value: XACLENABLED

logstate

The logging state of the ACL. Possible values: ENABLED, DISABLED Default value: GENDISABLED

ratelimit

log message rate limit for acl rule Default value: 100 Minimum value: 1 Maximum value: 10000

Example

add ns acl restrict DENY -srcport 45-1024 -destIP 192.168.1.1 -protocol TCP

Top

rm ns acl

Synopsis

rm ns acl <aclname> ...

Description

Remove an ACL. To commit this operation, one should apply the ACL.

Parameters

aclname

The name of the ACL to be deleted.

Example

rm ns acl restrict

Top

set ns acl

Synopsis

set ns acl <aclname> [-aclaction <aclaction>] [-srcIP [<operator>] <srcIPVal>] [-srcPort [<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-destPort [<operator>] <destPortVal>] [-srcMac <mac_addr>] [-protocol <protocol> | -protocolNumber <positive_integer>] [-icmpType <positive_integer> [-icmpCode <positive_integer>]] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-logstate (ENABLED | DISABLED)] [-ratelimit <positive_integer>] [-established]

Description

Modify an ACL. To commit this modified ACL, use the 'apply acls' command.

Parameters

aclname

The alphanumeric name of the ACL.

aclaction

The action associated with the ACL. Possible values: BRIDGE, DENY, ALLOW

srcIP

The source IP address (range).

srcPort

The source Port (range).

destIP

The destination IP address (range).

destPort

The destination Port (range).

srcMac

The source MAC address.

protocol

The IP protocol name. Possible values: ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS

protocolNumber

The IP protocol number (decimal). Minimum value: 1 Maximum value: 255

icmpType

The ICMP message type, valid values are 0-255 Maximum value: 65536

vlan

The VLAN number. Minimum value: 1 Maximum value: 4094

interface

The physical interface.

priority

The priority of the ACL. Minimum value: 1 Maximum value: 100000

logstate

The logging state of the ACL. Possible values: ENABLED, DISABLED Default value: GENDISABLED

established

This argument indicates that the ACL should be used for TCP response traffic only.

Example

set ns acl restrict -srcPort 50

Top

unset ns acl

Synopsis

unset ns acl <aclname> [-srcIP] [-srcPort] [-destIP] [-destPort] [-srcMac] [-protocol] [-icmpType] [-icmpCode] [-vlan] [-interface] [-logstate] [-ratelimit] [-established]

Description

Modify an ACL. To commit this modified ACL, use the 'apply acls' command..Refer to the set ns acl command for meanings of the arguments.

Example

unset ns acl rule1 -srcPort

Top

enable ns acl

Synopsis

enable ns acl <aclname> ...

Description

Enable an ACL. To commit this operation, one should apply the ACL.

Parameters

aclname

The name of the ACL to be enabled.

Example

enable ns acl foo

Top

disable ns acl

Synopsis

disable ns acl <aclname> ...

Description

Disable an ACL. To commit this operation, one should apply the ACL.

Parameters

aclname

The name of the ACL to be disabled.

Example

disable ns acl foo

Top

stat ns acl

Synopsis

stat ns acl [<aclname>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display ACL statistics.

Parameters

aclname

The ACL.

Example

stat acl

Top

rename ns acl

Synopsis

rename ns acl <aclname> <newName>

Description

Rename an ACL rule.

Parameters

aclname

The name of the ACL rule.

newName

The new name of the ACL rule.

Example

rename acl rule rule-new

Top

show ns acl

Synopsis

show ns acl [<aclname>]

Description

Display the ACLs.If name is specified, then only that particular ACL information is displayed. If it is not specified, all configured ACLs are displayed.

Parameters

aclname

The name of the ACL.

Example

```
sh acl foo
   Name: foo                    Action: ALLOW    Hits: 0
   srcIP = 10.102.1.150
   destIP = 202.54.12.47
   srcMac:                      Protocol: TCP
   srcPort                     destPort = 110
   Vlan:                       Interface:
   Active Status: ENABLED              Applied Status: NOTAPPLIED
   Priority: 1027
```

Top

ns acl6

[add | rm | set | unset | enable | disable | stat | rename | show]

add ns acl6

Synopsis

add ns acl6 <acl6name> <acl6action> [-srcIPv6 [<operator>] <srcIPv6Val>] [-srcPort [<operator>] <srcPortVal>] [-destIPv6 [<operator>] <destIPv6Val>] [-destPort [<operator>] <destPortVal>] [-TTL <positive_integer>] [-srcMac <mac_addr>] [(-protocol <protocol> [-established]) | -protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-icmpType <positive_integer> [-icmpCode <positive_integer>]] [-priority <positive_integer>] [-state <state>]

Description

Add an IPv6 ACL to the System configuration. Each inbound packet is matched against configured ACLs and the specified action is applied to the packet. This command adds the IPv6 ACL to the configuration space. To commit this ACL, one should apply the ACL.

Parameters

acl6name

Alphanumeric name of the ACL6.

acl6action

Action associated with the ACL6. Possible values: BRIDGE, DENY, ALLOW

srcIPv6

Source IPv6 address (range).

srcPort

Source port (range).

destIPv6

Destination IPv6 address (range).

destPort

Destination port (range).

TTL

Time to expire this ACL6 (in seconds). Minimum value: 1 Maximum value: 2147483647

srcMac

Source MAC address.

protocol

IPv6 protocol name. Possible values: ICMPV6, TCP, UDP

protocolNumber

IPv6 protocol number (decimal). Minimum value: 1 Maximum value: 255

vlan

VLAN number. Minimum value: 1 Maximum value: 4094

interface

Physical interface name.

established

This argument indicates that the ACL6 should be used for TCP response traffic only.

icmpType

ICMPv6 message type Maximum value: 65536

icmpCode

ICMPv6 message code Maximum value: 65536

priority

Priority of the ACL6. (Sequence of execution) Minimum value: 1 Maximum value: 80000

state

State of the ACL6. Possible values: ENABLED, DISABLED, REMOVED Default value: XACLENABLED

Example

add ns acl6 rule1 DENY -srcport 45-1024 -destIPv6 2001::45 -protocol TCP

Top

rm ns acl6

Synopsis

rm ns acl6 <acl6name> ...

Description

Remove an ACL6. To commit this operation, one should apply the ACL6.

Parameters

acl6name

Name of the ACL6 to be deleted.

Example

rm ns acl6 rule1

Top

set ns acl6

Synopsis

set ns acl6 <acl6name> [-aclaction <aclaction>] [-srcIPv6 [<operator>] <srcIPv6Val>] [-srcPort [<operator>] <srcPortVal>] [-destIPv6 [<operator>] <destIPv6Val>] [-destPort [<operator>] <destPortVal>] [-srcMac <mac_addr>] [-protocol <protocol> | -protocolNumber <positive_integer>] [-icmpType <positive_integer> [-icmpCode <positive_integer>]] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-established]

Description

Modify an ACL6. To commit this modified ACL6, use 'apply acls6' command.

Parameters

acl6name

Alphanumeric name of the ACL6.

aclaction

Action associated with the ACL6. Possible values: BRIDGE, DENY, ALLOW

srcIPv6

Source IPv6 address (range).

srcPort

Source Port (range).

destIPv6

Destination IPv6 address (range).

destPort

Destination Port (range).

srcMac

Source MAC address.

protocol

IPv6 protocol name. Possible values: ICMPV6, TCP, UDP

protocolNumber

IPv6 protocol number (decimal). Minimum value: 1 Maximum value: 255

icmpType

ICMPv6 message type Maximum value: 65536

vlan

VLAN number. Minimum value: 1 Maximum value: 4094

interface

Physical interface name.

priority

Priority of the ACL6. (Sequence of execution) Minimum value: 1 Maximum value: 80000

established

This argument indicates that the ACL6 should be used for TCP response traffic only.

Example

set ns acl6 rule1 -srcPort 50

Top

unset ns acl6

Synopsis

unset ns acl6 <acl6name> [-srcIPv6] [-srcPort] [-destIPv6] [-destPort] [-srcMac] [-protocol] [-icmpType] [-icmpCode] [-vlan] [-interface] [-established]

Description

Modify an ACL6. To commit this modified ACL6, use 'apply acls6' command..Refer to the set ns acl6 command for meanings of the arguments.

Example

unset ns acl6 rule1 -srcPort

Top

enable ns acl6

Synopsis

enable ns acl6 <acl6name> ...

Description

Enable an ACL6. To commit this operation, one should apply the ACL6.

Parameters

acl6name

Name of the ACL6 to be enabled.

Example

enable ns acl6 rule1

Top

disable ns acl6

Synopsis

disable ns acl6 <acl6name> ...

Description

Disable an ACL6. To commit this operation, one should apply the ACL6.

Parameters

acl6name

Name of the ACL6 to be disabled.

Example

disable ns acl6 rule1

Top

stat ns acl6

Synopsis

stat ns acl6 [<acl6name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display ACL6 statistics.

Parameters

acl6name

ACL6 Name.

Example

stat acl6

Top

rename ns acl6

Synopsis

rename ns acl6 <acl6name> <newName>

Description

Rename an ACL6 rule.

Parameters

acl6name

The name of the ACL6 rule.

newName

The new name of the ACL6 rule.

Example

rename acl6 rule rule-new

Top

show ns acl6

Synopsis

show ns acl6 [<acl6name>]

Description

Display the ACL6. If name is specified, then only that particular ACL6 information is displayed. If it is not specified, all configured ACL6 are displayed.

Parameters

acl6name

Name of the ACL6.

Example

```
show ns acl6 rule1
1)     Name: r1                    Action: DENY
       srcIPv6 = 2001::1
       destIPv6
       srcMac:                    Protocol:
       Vlan:                     Interface:
       Active Status: ENABLED          Applied Status: NOTAPPLIED
       Priority: 10                Hits: 0
       TTL:
```

Top

ns ip6

[add | rm | set | unset | show]

add ns ip6

Synopsis

add ns ip6 <IPv6Address>@ [-scope (global | link-local)] [-type <type> [-hostRoute (ENABLED | DISABLED) [-ip6hostRtGw <ipv6_addr|*>] [-metric <integer>] [-vserverRHILevel <vserverRHILevel>] [-ospf6LSAType (INTRA_AREA | EXTERNAL) [-ospfArea <positive_integer>]]]] [-nd (ENABLED | DISABLED)] [-icmp (ENABLED | DISABLED)] [-vServer (ENABLED | DISABLED)] [-telnet (ENABLED | DISABLED)] [-ftp (ENABLED | DISABLED)] [-gui <gui>] [-ssh (ENABLED | DISABLED)] [-snmp (ENABLED | DISABLED)] [-mgmtAccess (ENABLED | DISABLED)] [-restrictAccess (ENABLED | DISABLED)] [-dynamicRouting (ENABLED | DISABLED)] [-state (DISABLED | ENABLED)] [-map <ip_addr>] [-ownerNode <positive_integer>]

Description

Add an IPV6 address.

Parameters

IPv6Address

The IPV6 address

scope

The scope of the IPV6 address Possible values: global, link-local Default value: NS_GLOBAL

type

The type of the IPV6 address. Possible values: NSIP, VIP, SNIP, GSLBsiteIP, ADNSsvcIP, CLIP Default value: NS_IPV6_SNIP

nd

Use this option to set (enable or disable) ND responses for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

icmp

Use this option to set (enable or disable) ICMP responses for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

vServer

Use this option to set (enable or disable) the vserver attribute for this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

telnet

Use this option to set (enable or disable) the state of telnet access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

ftp

Use this option to set (enable or disable) the state of ftp access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

gui

Use this option to set (enable|Secureonly|disable) GUI access to this IP entity. Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh

Use this option to set (enable or disable) the state of SSH access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

snmp

Use this option to set (enable or disable) the state of SNMP access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess

Use this option to set (enable or disable) the state of management access to this IP entity. Possible values: ENABLED, DISABLED Default value: DISABLED

restrictAccess

Enable or disable blocking of all ports not used for management access. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicRouting

Use this option to enable or disable dynamic routing on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute

The state of advertisement of a hostroute to this IPv6 entity. Possible values: ENABLED, DISABLED

ip6hostRtGw

The gateway for the hostroute to be advertised for this IPv6 entity.

metric

The metric value to be added or subtracted from the cost of the hostroute advertised for this IP entity. Minimum value: -16777215

vserverRHILevel

The state of per VIP RHI controls. Possible values: ONE_VSERVER, ALL_VSERVERS, NONE Default value: RHI_STATE_ONE

ospf6LSAType

The OSPF6's route advertisement type. Possible values: INTRA_AREA, EXTERNAL Default value: DISABLED

ospfArea

The area ID of the area in which OSPF intra area prefix LSAs should be advertised. Default value: -1 Maximum value: 4294967294LU

state

Use this option to enable or disable the entity. Possible values: DISABLED, ENABLED Default value: ENABLED

map

The mapped IPV4 address for IPV6.

ownerNode

The owner node in a Cluster for this IPv6 address. Default value: 255

Example

add ns ip6 2001::a/96 -scope GLOBAL

Top

rm ns ip6

Synopsis

rm ns ip6 <IPv6Address>@

Description

Remove an IPv6 entity.

Parameters

IPv6Address

The IPV6 address of the entity.

Example

rm ns ip6 2002::5

Top

set ns ip6

Synopsis

set ns ip6 <IPv6Address>@ [-nd (ENABLED | DISABLED)] [-icmp (ENABLED | DISABLED)] [-vServer (ENABLED | DISABLED)] [-telnet (ENABLED | DISABLED)] [-ftp (ENABLED | DISABLED)] [-gui <gui>] [-ssh (ENABLED | DISABLED)] [-snmp (ENABLED | DISABLED)] [-mgmtAccess (ENABLED | DISABLED)] [-restrictAccess (ENABLED | DISABLED)] [-state (DISABLED | ENABLED)] [-map <ip_addr>] [-dynamicRouting (ENABLED | DISABLED)] [-hostRoute (ENABLED | DISABLED) [-ip6hostRtGw <ipv6_addr|*>] [-metric <integer>] [-vserverRHILevel <vserverRHILevel>] [-ospf6LSAType (INTRA_AREA | EXTERNAL) [-ospfArea <positive_integer>]]]

Description

Set IP6 address options.

Parameters

IPv6Address

The IPV6 address

nd

The state of ND responses for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

icmp

The state of ICMP responses for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

vServer

The state of vserver attribute for this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

telnet

The state of telnet access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

ftp

The state of ftp access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

gui

The state of GUI access to this IP entity. Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh

The state of SSH access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

snmp

The state of SNMP access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess

The state of management access to this IP entity. Possible values: ENABLED, DISABLED Default value: DISABLED

restrictAccess

Status of ports not used for management access (blocked/open) for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

state

Use this option to enable or disable the entity. Possible values: DISABLED, ENABLED Default value: ENABLED

map

The mapped IPV4 address for IPV6.

dynamicRouting

Use this option to enable or disable dynamic routing on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute

The state of advertisement of a hostroute to this IPv6 entity. Possible values: ENABLED, DISABLED

Example

set ns ip6 2001::a -map 10.102.33.27

Top

unset ns ip6

Synopsis

unset ns ip6 <IPv6Address>@ [-nd] [-icmp] [-vServer] [-telnet] [-ftp] [-gui] [-ssh] [-snmp] [-mgmtAccess] [-restrictAccess] [-state] [-map] [-dynamicRouting] [-hostRoute] [-ip6hostRtGw] [-metric] [-vserverRHILevel] [-ospf6LSAType] [-ospfArea]

Description

Use this command to remove ns ip6 settings.Refer to the set ns ip6 command for meanings of the arguments.

Top

show ns ip6

Synopsis

show ns ip6 [<IPv6Address>]

Description

Display all IPV6 addresses

Parameters

IPv6Address

The IPV6 address

Example

show ns ip6

Top

ns ip

[add | rm | set | unset | enable | disable | show]

add ns ip

Synopsis

add ns ip <IPAddress>@ <netmask> [-type <type> [-hostRoute (ENABLED | DISABLED) [-hostRtGw <ip_addr>] [-metric <integer>] [-vserverRHILevel <vserverRHILevel>] [-ospfLSAType (TYPE1 | TYPE5) [-ospfArea <positive_integer>]]]] [-arp (ENABLED | DISABLED)] [-icmp (ENABLED | DISABLED)] [-vServer (ENABLED | DISABLED)] [-telnet (ENABLED | DISABLED)] [-ftp (ENABLED | DISABLED)] [-gui <gui>] [-ssh (ENABLED | DISABLED)] [-snmp (ENABLED | DISABLED)] [-mgmtAccess (ENABLED | DISABLED)] [-restrictAccess (ENABLED | DISABLED)] [-dynamicRouting (ENABLED | DISABLED)] [-state (ENABLED | DISABLED)] [-vrID <positive_integer>] [-icmpResponse <icmpResponse>] [-ownerNode <positive_integer>] [-arpResponse <arpResponse>]

Description

Add an IP address.

Parameters

IPAddress

The IP address of the entity.

netmask

The netmask of the IP.

type

The type of the IP address. Possible values: SNIP, VIP, MIP, NSIP, GSLBsiteIP, CLIP Default value: NSADDR_SNIP

arp

Use this option to set (enable or disable) ARP and gratuitous ARP for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

icmp

Use this option to set (enable or disable) ICMP responses for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

vServer

Use this option to set (enable or disable) the vserver attribute for this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

telnet

Use this option to set (enable or disable) the state of telnet access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

ftp

Use this option to set (enable or disable) the state of ftp access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

gui

Use this option to set (enable|Secureonly|disable) GUI access to this IP entity. Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh

Use this option to set (enable or disable) the state of SSH access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

snmp

Use this option to set (enable or disable) the state of SNMP access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess

Use this option to set (enable or disable) the state of management access to this IP entity. Possible values: ENABLED, DISABLED Default value: DISABLED

restrictAccess

Enable or disable blocking of all ports not used for management access. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicRouting

Use this option to enable or disable dynamic routing on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

ospf

Use this option to enable or disable OSPF on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

bgp

Use this option to enable or disable BGP on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

rip

Use this option to enable or disable RIP on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute

The state of advertisement of a hostroute to this IP entity. Possible values: ENABLED, DISABLED

hostRtGw

The gateway for the hostroute to be advertised for this IP entity. Default value: -1

metric

The metric value to be added or subtracted from the cost of the hostroute advertised for this IP entity. Minimum value: -16777215

vserverRHILevel

The state of per VIP RHI controls. Possible values: ONE_VSERVER, ALL_VSERVERS, NONE Default value: RHI_STATE_ONE

ospfLSAType

The OSPF's route advertisement type. Possible values: TYPE1, TYPE5 Default value: DISABLED

ospfArea

The area ID of the area in which OSPF Type1 LSAs should be advertised. Default value: -1 Maximum value: 4294967294LU

state

Use this option to enable or disable the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

vrID

Use this option to bind this IP to a VRID. Minimum value: 1 Maximum value: 255

icmpResponse

ICMp response control on down vserver Possible values: NONE, ONE_VSERVER, ALL_VSERVERS, VSVR_CNTRLD Default value: NS_IP_NONE

ownerNode

The owner node in a Cluster for this IP address. Owner node can vary from 0 to 31. If ownernode is not specified then the IP is treated as Striped IP. Default value: 255

arpResponse

Arp response control on down vserver Possible values: NONE, ONE_VSERVER, ALL_VSERVERS Default value: NS_IP_NONE

Example

add ns ip 10.102.4.123 255.255.255.0

Top

rm ns ip

Synopsis

rm ns ip <IPAddress>@

Description

Remove an IP entity.

Parameters

IPAddress

The IP address of the entity.

Example

rm ns ip 10.102.4.123

Top

set ns ip

Synopsis

set ns ip <IPAddress>@ [-netmask <netmask>] [-arp (ENABLED | DISABLED)] [-icmp (ENABLED | DISABLED)] [-vServer (ENABLED | DISABLED)] [-telnet (ENABLED | DISABLED)] [-ftp (ENABLED | DISABLED)] [-gui <gui>] [-ssh (ENABLED | DISABLED)] [-snmp (ENABLED | DISABLED)] [-mgmtAccess (ENABLED | DISABLED)] [-restrictAccess (ENABLED | DISABLED)] [-dynamicRouting (ENABLED | DISABLED)] [-hostRoute (ENABLED | DISABLED) [-hostRtGw <ip_addr>] [-metric <integer>] [-vserverRHILevel <vserverRHILevel>] [-ospfLSAType (TYPE1 | TYPE5) [-ospfArea <positive_integer>]]] [-vrID <positive_integer>] [-icmpResponse <icmpResponse>] [-arpResponse <arpResponse>]

Description

Set the attributes of an IP entity.

Parameters

IPAddress

The IP address of the entity.

netmask

The netmask of the IP.

arp

The state of ARP and gratuitous ARP for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

icmp

The state of ICMP responses for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

vServer

The state of vserver attribute for this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

telnet

The state of telnet access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

ftp

The state of ftp access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

gui

The state of GUI access to this IP entity. Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh

The state of SSH access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

snmp

The state of SNMP access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess

The state of management access to this IP entity. Possible values: ENABLED, DISABLED Default value: DISABLED

restrictAccess

Status of ports not used for management access (blocked/open) for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicRouting

Use this option to enable or disable dynamic routing on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

ospf

The state of OSPF on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

bgp

The state of BGP on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

rip

The state of RIP on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute

The state of advertisement of a hostroute to this IP entity. Possible values: ENABLED, DISABLED

vrID

Use this option to bind this IP to a VRID. Minimum value: 1 Maximum value: 255

icmpResponse

ICMp response control on down vserver Possible values: NONE, ONE_VSERVER, ALL_VSERVERS, VSVR_CNTRLD Default value: NS_IP_NONE

arpResponse

Arp response control on down vserver Possible values: NONE, ONE_VSERVER, ALL_VSERVERS Default value: NS_IP_NONE

Example

set ns ip 10.102.4.123 -arp ENABLED

Top

unset ns ip

Synopsis

unset ns ip <IPAddress>@ [-netmask] [-arp] [-icmp] [-vServer] [-telnet] [-ftp] [-gui] [-ssh] [-snmp] [-mgmtAccess] [-restrictAccess] [-dynamicRouting] [-hostRoute] [-hostRtGw] [-metric] [-vserverRHILevel] [-ospfLSAType] [-ospfArea] [-vrID] [-icmpResponse] [-arpResponse]

Description

Use this command to remove ns ip settings.Refer to the set ns ip command for meanings of the arguments.

Top

enable ns ip

Synopsis

enable ns ip <IPAddress>@

Description

Enable an IP entity.

Parameters

IPAddress

The IP address of the entity.

Example

enable ns ip 10.10.10.10

Top

disable ns ip

Synopsis

disable ns ip <IPAddress>@

Description

Disable an IP entity.

Parameters

IPAddress

The IP address of the entity.

Example

disable ns ip 10.10.10.10

Top

show ns ip

Synopsis

show ns ip [<IPAddress>] [-type <type>]

Description

Display all the IP addresses such as VIP,MIP,NSIP,SNIP and CLIP.

Parameters

IPAddress

The IP address of the entity.

type

The type of this IP. Possible values: SNIP, VIP, MIP, NSIP, GSLBsiteIP, CLIP

Example

```
show ns ip
Ipaddress      Type         Mode    Arp     Icmp    Vserver State  Owner
---------      ----         ----    ---     ----    ------- -----  -----
1)10.102.169.16 Cluster IP   Active Enabled Enabled NA      Enabled Configuration Coordinator
2)10.102.169.18 NetScaler IP Active Enabled Enabled NA      Enabled 1
3)10.102.169.19 NetScaler IP Active Enabled Enabled NA      Enabled 2
4)10.102.169.17 VIP          Active Enabled Enabled Enabled Enabled ALL
```

Top

ns simpleacl

[add | clear | rm | flush | show | stat]

add ns simpleacl

Synopsis

add ns simpleacl <aclname> <aclaction> -srcIP <ip_addr> [-destPort <port> -protocol (TCP | UDP)] [-TTL <positive_integer>]

Description

Add a SimpleACL rule to the system configuration, every inbound packet is matched against configured SimpleACL rules and specified action is applied.

Parameters

aclname

Alphanumeric name of the ACL rule.

aclaction

Action associated with the ACL rule. Possible values: DENY

srcIP

Source ip for the ACL rule.

destPort

Destination port for the ACL rule.

TTL

Time to expire this ACL rule(in seconds). Timer granularity is 4 seconds. Minimum value: 4 Maximum value: 2147483647

Example

add simpleacl rule1 DENY -srcIP 1.1.1.1 -destPort 80 -protocol TCP
add simpleacl rule2 DENY -srcIP 2.2.2.2 -TTL 600

Top

clear ns simpleacl

Synopsis

clear ns simpleacl

Description

Clear all configured SimpleACL rules.

Top

rm ns simpleacl

Synopsis

rm ns simpleacl <aclname> ...

Description

Remove a SimpleACL rule.

Parameters

aclname

Name of the ACL rule to be deleted.

Example

rm ns simpleacl rule1

Top

flush ns simpleacl

Synopsis

flush ns simpleacl -estSessions

Description

Flush all active sessions matching the simple acl rule.

Top

show ns simpleacl

Synopsis

show ns simpleacl [<aclname>]

Description

Display all the SimpleACL rules. If a rule name is specified, then only that SimpleACL rule is shown.

Parameters

aclname

Name of the ACL rule.

Example

show simpleacl rule1
Name: rule1 Action: DENY
srcIP = 10.102.1.150
Protocol = TCP DestPort = 110
Hits: 5 TTL: 200(seconds)

Top

stat ns simpleacl

Synopsis

stat ns simpleacl [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display SimpleACL statistics.

Example

stat simpleacl

Top

ns simpleacl6

[add | clear | flush | rm | show | stat]

add ns simpleacl6

Synopsis

add ns simpleacl6 <aclname> <aclaction> -srcIPv6 <ipv6_addr|null> [-destPort <port> -protocol (TCP | UDP)] [-TTL <positive_integer>]

Description

Add a SimpleACL6 rule to the system configuration, every inbound ipv6 packet is matched against configured SimpleACL rules and specified action is applied.

Parameters

aclname

Alphanumeric name of the ACL rule.

aclaction

Action associated with the ACL rule. Possible values: DENY

srcIPv6

Source ip6 address for the ACL rule.

destPort

Destination port for the ACL rule.

TTL

Time to expire this ACL rule(in seconds). Timer granularity is 4 seconds. Minimum value: 4 Maximum value: 2147483647

Example

add simpleacl6 rule1 DENY -srcIP6 fe80::2c0:95ff:fec5:d9b8 -destPort 80 -protocol TCP
add simpleacl rule2 DENY -srcIP6 3ffe:100:100::1 -TTL 600

Top

clear ns simpleacl6

Synopsis

clear ns simpleacl6

Description

Clear all configured SimpleACL6 rules.

Example

clear ns simpleacl6

Top

flush ns simpleacl6

Synopsis

flush ns simpleacl6 -estSessions

Description

Flush all active sessions matching the simple acl rule.

Top

rm ns simpleacl6

Synopsis

rm ns simpleacl6 <aclname> ...

Description

Remove a SimpleACL6 rule.

Parameters

aclname

Name of the Simple ACL6 rule to be deleted.

Example

rm ns simpleacl6 rule1

Top

show ns simpleacl6

Synopsis

show ns simpleacl6 [<aclname>]

Description

Display all the SimpleACL6 rules. If a rule name is specified, then only that SimpleACL6 rule is shown.

Parameters

aclname

Name of the Simple ACL6 rule.

Example

```
show simpleacl6 rule1
   Name: rule1
   Action: DENY                    Hits: 5
   srcIP6 = 3ffe:100:100::1
   Protocol = TCP                   DestPort = 110
   TTL: 200(seconds)
```

Top

stat ns simpleacl6

Synopsis

stat ns simpleacl6 [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display SimpleACL6 statistics.

Example

stat simpleacl6

Top

ns pbr

[add | rm | set | unset | enable | disable | stat | show]

add ns pbr

Synopsis

add ns pbr <name> <action> [-srcIP [<operator>] <srcIPVal>] [-srcPort [<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-destPort [<operator>] <destPortVal>] [-nextHop <nextHopVal>] [-srcMac <mac_addr>] [-protocol <protocol> | -protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-msr (ENABLED | DISABLED) [-monitor <string>]] [-state <state>]

Description

Add a Policy Based Routing(PBR) to the system configuration. Each inbound packet is matched against configured PBRs and routed accordingly. This command adds the PBR to the configuration space. Use the 'apply pbrs' command to commit this operation.

Parameters

name

The name of the PBR

action

The action associated with the PBR. Possible values: ALLOW, DENY

srcIP

The source IP address (range).

srcPort

The source port (range).

destIP

The destination IP address (range).

destPort

The destination port (range).

nextHop

The Next Hop IP address.

srcMac

The source MAC address.

protocol

The IP protocol name. Possible values: ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS

protocolNumber

The IP protocol number (decimal). Minimum value: 1 Maximum value: 255

vlan

The VLAN number. Minimum value: 1 Maximum value: 4094

interface

The physical interface.

priority

The priority of the PBR. Minimum value: 1 Maximum value: 81920

msr

Enable/disable Monitored Static Route(MSR) on this route. Possible values: ENABLED, DISABLED Default value: DISABLED

state

The state of the PBR. Possible values: ENABLED, DISABLED, REMOVED Default value: XACLENABLED

Example

add ns pbr a allow -srcip 10.102.37.252 -destip 10.10.10.2 -nexthop 11.11.11.2

Top

rm ns pbr

Synopsis

rm ns pbr <name> ...

Description

Remove a Policy Based Routing(PBR). Use the 'apply pbrs' command to commit this operation.

Parameters

name

The name of the PBR to be deleted.

Example

rm ns pbr a

Top

set ns pbr

Synopsis

set ns pbr <name> [-action (ALLOW | DENY)] [-srcIP [<operator>] <srcIPVal>] [-srcPort [<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-destPort [<operator>] <destPortVal>] [-nextHop <nextHopVal>] [-srcMac <mac_addr>] [-protocol <protocol> | -protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-msr (ENABLED | DISABLED) [-monitor <string>]]

Description

Modify a Policy Based Routing(PBR). Use the 'apply pbrs' command to commit this operation.

Parameters

name

The name of the PBR.

action

The action associated with the PBR. Possible values: ALLOW, DENY

srcIP

The source IP address (range).

srcPort

The source port (range).

destIP

The destination IP address (range).

destPort

The destination port (range).

nextHop

The Next Hop IP address.

srcMac

The source MAC address.

protocol

The IP protocol name. Possible values: ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS

protocolNumber

The IP protocol number (decimal). Minimum value: 1 Maximum value: 255

vlan

The VLAN number. Minimum value: 1 Maximum value: 4094

interface

The physical interface.

priority

The priority of the PBR. Minimum value: 1 Maximum value: 81920

msr

Enable/disable Monitored Static Route(MSR) on this route. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set ns pbr a -srcPort 50

Top

unset ns pbr

Synopsis

unset ns pbr <name> [-srcIP] [-srcPort] [-destIP] [-destPort] [-nextHop] [-srcMac] [-protocol] [-vlan] [-interface] [-msr] [-monitor]

Description

Modify a Policy Based Routing(PBR). Use the 'apply pbrs' command to commit this operation..Refer to the set ns pbr command for meanings of the arguments.

Example

unset ns pbr rule1 -srcPort

Top

enable ns pbr

Synopsis

enable ns pbr <name> ...

Description

Enable a Policy Based Routing(PBR). Use the 'apply pbrs' command to commit this operation.

Parameters

name

The name of the PBR to be enabled.

Example

enable ns pbr foo

Top

disable ns pbr

Synopsis

disable ns pbr <name> ...

Description

Disable a Policy Based Routing(PBR). Use the 'apply pbrs' command to commit this operation.

Parameters

name

The name of the PBR to be disabled.

Example

disable ns pbr foo

Top

stat ns pbr

Synopsis

stat ns pbr [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display Policy Based Routing(PBR) statistics.

Parameters

name

The PBR.

Example

stat pbr

Top

show ns pbr

Synopsis

show ns pbr [<name>] [-detail]

Description

Display the Policy Based Routing(PBR).If name is specified, then only that particular PBR information is displayed. If it is not specified, all configured PBRs are displayed.

Parameters

name

The name of the PBR.

detail

To get a detailed view.

Example

```
show ns pbr a
   Name: a                      Action: ALLOW    Hits: 0
     srcIP = 10.102.37.252
     destIP = 10.10.10.2
     srcMac:                     Protocol:
     Vlan:                      Interface:
     Active Status: ENABLED            Applied Status: NOTAPPLIED
     Priority: 10
     NextHop: 11.11.11.2
```

Top

ns xmlnamespace

[add | rm | set | unset | show]

add ns xmlnamespace

Synopsis

add ns xmlnamespace <prefix> <namespace>

Description

Add an XML prefix to namespace URI mapping.

Parameters

prefix

The prefix of a namespace. The name must not exceed 31 characters.

namespace

The expanded namespace.

Example

add ns xmlnamespace soap http://schemas.xmlsoap.org/soap/envelope/

Top

rm ns xmlnamespace

Synopsis

rm ns xmlnamespace <prefix>

Description

Removes the XML prefix to namespace mapping for the prefix specified

Parameters

prefix

The name of the prefix.

Example

rm ns xmlnamespace soap

Top

set ns xmlnamespace

Synopsis

set ns xmlnamespace <prefix> [<namespace>] [-description <string>]

Description

Set the namespace or description for an XML prefix to namespace mapping

Parameters

prefix

The name of the prefix.

namespace

The expanded namespace.

description

Description for the prefix.

Example

set ns xmlnamespace soap -description SOAP/1.1

Top

unset ns xmlnamespace

Synopsis

unset ns xmlnamespace <prefix> [-namespace] [-description]

Description

Use this command to remove ns xmlnamespace settings.Refer to the set ns xmlnamespace command for meanings of the arguments.

Top

show ns xmlnamespace

Synopsis

show ns xmlnamespace [<prefix>]

Description

Display the configured XML prefix to namespace URI mapping(s).

Parameters

prefix

The name of the prefix.

Example

show ns xmlnamespace soap

Top

ns tcpProfile

[add | rm | set | unset | show]

add ns tcpProfile

Synopsis

add ns tcpProfile <name> [-WS (ENABLED | DISABLED)] [-SACK (ENABLED | DISABLED)] [-WSVal <positive_integer>] [-nagle (ENABLED | DISABLED)] [-ackOnPush (ENABLED | DISABLED)] [-mss <positive_integer>] [-maxBurst <positive_integer>] [-initialCwnd <positive_integer>] [-delayedAck <positive_integer>] [-oooQSize <positive_integer>] [-maxPktPerMss <positive_integer>] [-pktPerRetx <positive_integer>] [-minRTO <positive_integer>] [-slowStartIncr <positive_integer>] [-bufferSize <positive_integer>] [-synCookie (ENABLED | DISABLED)] [-KAprobeUpdateLastactivity (ENABLED | DISABLED)] [-flavor (Default | Westwood)] [-dynamicReceiveBuffering (ENABLED | DISABLED)] [-KA (ENABLED | DISABLED)] [-KAconnIdleTime <positive_integer>] [-KAmaxProbes <positive_integer>] [-KAprobeInterval <positive_integer>]

Description

Add a new TCP profile on the Netscaler

Parameters

name

Name of the TCP profile

WS

The state of WS Possible values: ENABLED, DISABLED Default value: DISABLED

SACK

The state of SACK Possible values: ENABLED, DISABLED Default value: DISABLED

WSVal

Window Scaling Factor used Default value: 4 Maximum value: 14

nagle

Whether to enable Nagle's algorithm on connections Possible values: ENABLED, DISABLED Default value: DISABLED

ackOnPush

Send immediate positive acknowledgement (ACK) on receiving TCP packets having the PUSH flag set. Possible values: ENABLED, DISABLED Default value: ENABLED

mss

Set Maximum Segment Size(MSS) to use for TCP Connection (0 forces use of global setting). Maximum value: 1460

maxBurst

Max-Burst Factor used Default value: 6 Minimum value: 1 Maximum value: 255

initialCwnd

Intial value of TCP cwnd used Default value: 4 Minimum value: 1 Maximum value: 44

delayedAck

Delayed acknowledgement timeout (in millisec) Default value: 100 Minimum value: 10 Maximum value: 300

oooQSize

Maximum size of out-of-order packet queue (0 means infinite) Default value: 64 Maximum value: 65535

maxPktPerMss

Enable packet count based congestion control by setting to non zero value Maximum value: 512

pktPerRetx

Set value for maximum number packets per retransmission Default value: 1 Minimum value: 1 Maximum value: 512

minRTO

Set minimum limit on TCP RTO (in millisec) Default value: 1000 Minimum value: 10 Maximum value: 64000

slowStartIncr

Set TCP slowstart increment factor Default value: 2 Minimum value: 1 Maximum value: 100

bufferSize

Set TCP buffer size Default value: 8190 Minimum value: 8190 Maximum value: 4194304

synCookie

Whether to enable syncookie on connections Possible values: ENABLED, DISABLED Default value: ENABLED

KAprobeUpdateLastactivity

Update last activity for KA probes Possible values: ENABLED, DISABLED Default value: ENABLED

flavor

Set TCP algorithm Possible values: Default, Westwood Default value: NS_TCP_DEFAULT

dynamicReceiveBuffering

Enable/Disable Dynamic Receive Buffering Possible values: ENABLED, DISABLED Default value: ENABLED

KA

Send periodic TCP keep-alive probes to check if peer is still up Possible values: ENABLED, DISABLED Default value: DISABLED

KAconnIdleTime

How long the connection should be idle, in seconds, before sending a keep-alive probe Default value: NSTCP_KA_DEFAULT_CONN_IDLETIME Minimum value: 1 Maximum value: 4095

KAmaxProbes

How many keep-alive probes to send, when not acknowledged, before assuming peer to be down Default value: NSTCP_KA_DEFAULT_PROBE_COUNT Minimum value: 1 Maximum value: 255

KAprobeInterval

Time interval (seconds) before the next probe, if peer does not respond Default value: NSTCP_KA_DEFAULT_INTERVAL Minimum value: 1 Maximum value: 4095

Example

add tcpprofile <profile name> -WS ENABLED -WSVAL 4

Top

rm ns tcpProfile

Synopsis

rm ns tcpProfile <name>

Description

Remove a TCP profile on the Netscaler

Parameters

name

Name of the TCP profile

Example

rm tcpprofile <profile name>

Top

set ns tcpProfile

Synopsis

set ns tcpProfile <name> [-WS (ENABLED | DISABLED)] [-SACK (ENABLED | DISABLED)] [-WSVal <positive_integer>] [-nagle (ENABLED | DISABLED)] [-ackOnPush (ENABLED | DISABLED)] [-mss <positive_integer>] [-maxBurst <positive_integer>] [-initialCwnd <positive_integer>] [-delayedAck <positive_integer>] [-oooQSize <integer>] [-maxPktPerMss <positive_integer>] [-pktPerRetx <positive_integer>] [-minRTO <positive_integer>] [-slowStartIncr <positive_integer>] [-bufferSize <positive_integer>] [-synCookie (ENABLED | DISABLED)] [-KAprobeUpdateLastactivity (ENABLED | DISABLED)] [-flavor (Default | Westwood)] [-dynamicReceiveBuffering (ENABLED | DISABLED)] [-KA (ENABLED | DISABLED)] [-KAconnIdleTime <positive_integer>] [-KAmaxProbes <positive_integer>] [-KAprobeInterval <positive_integer>]

Description

Set/modify TCP profile values

Parameters

name

Name of the TCP profile

WS

The state of WS Possible values: ENABLED, DISABLED Default value: DISABLED

SACK

The state of SACK Possible values: ENABLED, DISABLED Default value: DISABLED

WSVal

Window Scaling Factor used Default value: 4 Maximum value: 14

nagle

Whether to enable Nagle's algorithm on connections Possible values: ENABLED, DISABLED Default value: DISABLED

ackOnPush

Send immediate positive acknowledgement (ACK) on receiving TCP packets having the PUSH flag set. Possible values: ENABLED, DISABLED Default value: ENABLED

mss

Set Maximum Segment Size(MSS) to use for TCP Connection(0 forces use of global setting) Maximum value: 1460

maxBurst

Max-Burst Factor used Default value: 6 Minimum value: 1 Maximum value: 255

initialCwnd

Intial value of TCP cwnd used Default value: 4 Minimum value: 1 Maximum value: 44

delayedAck

Delayed acknowledgement timeout (in millisec) Default value: 100 Minimum value: 10 Maximum value: 300

oooQSize

Maximum size of out-of-order packet queue (0 means infinite) Default value: 64 Maximum value: 65535

maxPktPerMss

Enable packet count based congestion control by setting to non zero value Maximum value: 512

pktPerRetx

Set value for maximum number packets per retransmission Default value: 1 Minimum value: 1 Maximum value: 512

minRTO

Set minimum limit on TCP RTO (in millisec) Default value: 1000 Minimum value: 10 Maximum value: 64000

slowStartIncr

Set TCP slowstart increment factor Default value: 2 Minimum value: 1 Maximum value: 100

bufferSize

Set TCP buffer size Default value: 8190 Minimum value: 8190 Maximum value: 4194304

synCookie

Whether to enable syncookie on connections Possible values: ENABLED, DISABLED Default value: ENABLED

KAprobeUpdateLastactivity

Update last activity for KA probes Possible values: ENABLED, DISABLED Default value: ENABLED

flavor

Set TCP algorithm Possible values: Default, Westwood Default value: NS_TCP_DEFAULT

dynamicReceiveBuffering

Enable/Disable Dynamic Receive Buffering Possible values: ENABLED, DISABLED Default value: ENABLED

KA

Send periodic TCP keep-alive probes to check if peer is still up Possible values: ENABLED, DISABLED Default value: DISABLED

KAconnIdleTime

How long the connection should be idle, in seconds, before sending a keep-alive probe Default value: NSTCP_KA_DEFAULT_CONN_IDLETIME Minimum value: 1 Maximum value: 4095

KAmaxProbes

How many keep-alive probes to send, when not acknowledged, before assuming peer to be down Default value: NSTCP_KA_DEFAULT_PROBE_COUNT Minimum value: 1 Maximum value: 255

KAprobeInterval

Time interval (seconds) before the next probe, if peer does not respond Default value: NSTCP_KA_DEFAULT_INTERVAL Minimum value: 1 Maximum value: 4095

Example

set tcpprofile <profile name> -WS ENABLED -WSVAL 4

Top

unset ns tcpProfile

Synopsis

unset ns tcpProfile <name> [-WS] [-SACK] [-WSVal] [-nagle] [-ackOnPush] [-mss] [-maxBurst] [-initialCwnd] [-delayedAck] [-oooQSize] [-maxPktPerMss] [-pktPerRetx] [-minRTO] [-slowStartIncr] [-bufferSize] [-synCookie] [-KAprobeUpdateLastactivity] [-flavor] [-dynamicReceiveBuffering] [-KA] [-KAmaxProbes] [-KAconnIdleTime] [-KAprobeInterval]

Description

Unset a TCP profile values.Refer to the set ns tcpProfile command for meanings of the arguments.

Top

show ns tcpProfile

Synopsis

show ns tcpProfile [<name>]

Description

Display all the configured TCP profiles in the system. If a name is specified, then only that profile is shown.

Parameters

name

Name of the TCP profile.

Example

show tcp profile [profile name]

Top

ns httpProfile

[add | rm | set | unset | show]

add ns httpProfile

Synopsis

add ns httpProfile <name> [-dropInvalReqs (ENABLED | DISABLED)] [-markHttp09Inval (ENABLED | DISABLED)] [-markConnReqInval (ENABLED | DISABLED)] [-cmpOnPush (ENABLED | DISABLED)] [-conMultiplex (ENABLED | DISABLED)] [-maxReusePool <positive_integer>] [-dropExtraCRLF (ENABLED | DISABLED)] [-incompHdrDelay <positive_integer>] [-webSocket (ENABLED | DISABLED)] [-reqTimeout <positive_integer>] [-adptTimeout (ENABLED | DISABLED)] [-reqTimeoutAction <string>] [-dropExtraData (ENABLED | DISABLED)] [-webLog (ENABLED | DISABLED)] [-clientIpHdrExpr <expression>] [-maxReq <positive_integer>] [-persistentETag (ENABLED | DISABLED)]

Description

Add a new HTTP profile on the Netscaler

Parameters

name

Name of the HTTP profile

dropInvalReqs

Enable/disable dropping of invalid HTTP requests/responses Possible values: ENABLED, DISABLED Default value: DISABLED

markHttp09Inval

Enable/disable invalidating HTTP 0.9 requests Possible values: ENABLED, DISABLED Default value: DISABLED

markConnReqInval

Enable/disable invalidating CONNECT HTTP requests Possible values: ENABLED, DISABLED Default value: DISABLED

cmpOnPush

Enable/disable compression on PUSH packet Possible values: ENABLED, DISABLED Default value: DISABLED

conMultiplex

Connection multiplexing Possible values: ENABLED, DISABLED Default value: ENABLED

maxReusePool

Maximum connections in reusepool. If set to zero, limit will not be applied Maximum value: 360000

dropExtraCRLF

Drop extra CRLF after header is complete Possible values: ENABLED, DISABLED Default value: ENABLED

incompHdrDelay

Maximum time to wait between incomplete header packets (ms ticks) Default value: 7000 Maximum value: 4294967294LU

webSocket

Enable or disable WebSocket connections. Possible values: ENABLED, DISABLED Default value: DISABLED

reqTimeout

The time (in seconds) within which the HTTP request must complete. Maximum value: 86400

adptTimeout

The configured request timeout changed to adapt to the flow conditions. Possible values: ENABLED, DISABLED Default value: DISABLED

reqTimeoutAction

The responder action to respond to the client when timeout occurs. It can be either of RESET|DROP|Custom Responder Action. Connection is dropped silently if no action is set. RESET: Send RST to client when timeout occurs. DROP: Drop the connection when timeout occurs. Responder Action: Name of the responder action to trigger when timeout occurs, used to send custom message.

dropExtraData

Enable or disable dropping extra data from server. Possible values: ENABLED, DISABLED Default value: DISABLED

webLog

Enable or disable weblogging Possible values: ENABLED, DISABLED Default value: ENABLED

clientIpHdrExpr

Name of the header that contains real client IP.

maxReq

Maximum requests allowed on a single connection Maximum value: 65534

persistentETag

Generate the persistent NetScaler specific ETag for the HTTP response with ETag header. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add httpprofile <profile name> -dropInvalReqs ON -markHttp09Inval ON

Top

rm ns httpProfile

Synopsis

rm ns httpProfile <name>

Description

Remove a HTTP profile on the Netscaler

Parameters

name

Name of the TCP profile

Example

rm httpprofile <profile name>

Top

set ns httpProfile

Synopsis

set ns httpProfile <name> [-dropInvalReqs (ENABLED | DISABLED)] [-markHttp09Inval (ENABLED | DISABLED)] [-markConnReqInval (ENABLED | DISABLED)] [-cmpOnPush (ENABLED | DISABLED)] [-conMultiplex (ENABLED | DISABLED)] [-maxReusePool <positive_integer>] [-dropExtraCRLF (ENABLED | DISABLED)] [-incompHdrDelay <positive_integer>] [-webSocket (ENABLED | DISABLED)] [-reqTimeout <positive_integer>] [-adptTimeout (ENABLED | DISABLED)] [-reqTimeoutAction <string>] [-dropExtraData (ENABLED | DISABLED)] [-webLog (ENABLED | DISABLED)] [-clientIpHdrExpr <expression>] [-maxReq <positive_integer>] [-persistentETag (ENABLED | DISABLED)]

Description

Set/modify HTTP profile values

Parameters

name

Name of the HTTP profile

dropInvalReqs

Enable/disable dropping of invalid HTTP requests/responses Possible values: ENABLED, DISABLED Default value: DISABLED

markHttp09Inval

Enable/disable invalidating HTTP 0.9 requests Possible values: ENABLED, DISABLED Default value: DISABLED

markConnReqInval

Enable/disable invalidating CONNECT HTTP requests Possible values: ENABLED, DISABLED Default value: DISABLED

cmpOnPush

Enable/disable compression on PUSH packet Possible values: ENABLED, DISABLED Default value: DISABLED

conMultiplex

Connection multiplexing Possible values: ENABLED, DISABLED Default value: ENABLED

maxReusePool

Maximum connections in reusepool. If set to zero, limit will not be applied. Maximum value: 360000

dropExtraCRLF

Drop extra CRLF after header is complete Possible values: ENABLED, DISABLED Default value: ENABLED

incompHdrDelay

Maximum time to wait between incomplete header packets (ms ticks) Default value: 7000 Maximum value: 4294967294LU

webSocket

Enable or disable WebSocket connections. Possible values: ENABLED, DISABLED Default value: DISABLED

reqTimeout

The time (in seconds) within which the HTTP request must complete. Maximum value: 86400

adptTimeout

The configured request timeout changed to adapt to the flow conditions. Possible values: ENABLED, DISABLED Default value: DISABLED

reqTimeoutAction

The responder action to respond to the client when timeout occurs. It can be either of RESET|DROP|Custom Responder Action. Connection is dropped silently if no action is set. RESET: Send RST to client when timeout occurs. DROP: Drop the connection when timeout occurs. Responder Action: Name of the responder action to trigger when timeout occurs, used to send custom message.

dropExtraData

Enable or disable dropping extra data from server. Possible values: ENABLED, DISABLED Default value: DISABLED

webLog

Enable or disable weblogging Possible values: ENABLED, DISABLED Default value: ENABLED

clientIpHdrExpr

Name of the header that contains real client IP.

maxReq

Maximum requests allowed on a single connection Maximum value: 65534

persistentETag

Generate the persistent NetScaler specific ETag for the HTTP response with ETag header. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set httpprofile <profile name> -dropInvalReqs ON -markHttp09Inval ON

Top

unset ns httpProfile

Synopsis

unset ns httpProfile <name> [-dropInvalReqs] [-markHttp09Inval] [-markConnReqInval] [-cmpOnPush] [-conMultiplex] [-maxReusePool] [-dropExtraCRLF] [-incompHdrDelay] [-webSocket] [-dropExtraData] [-clientIpHdrExpr] [-reqTimeout] [-adptTimeout] [-reqTimeoutAction] [-webLog] [-maxReq] [-persistentETag]

Description

Unset HTTP profile values.Refer to the set ns httpProfile command for meanings of the arguments.

Top

show ns httpProfile

Synopsis

show ns httpProfile [<name>]

Description

Display all the configured HTTP profiles in the system. If a name is specified, then only that profile is shown.

Parameters

name

Name of the HTTP profile.

Example

show http profile [profile name]

Top

ns stats

show ns stats

Synopsis

show ns stats - alias for 'stat ns'

Description

show ns stats is an alias for stat ns

ns ns.conf

show ns ns.conf

Synopsis

show ns ns.conf

Description

Display the last saved configuration.

ns savedConfig

show ns savedConfig

Synopsis

show ns savedConfig

Description

Display the last saved configuration.

ns runningConfig

show ns runningConfig

Synopsis

show ns runningConfig [-withDefaults]

Description

Display the information pertaining to all the configuration that has been applied to the system, including settings that have not yet been saved to the system's ns.conf file using the save config command.

ns acls

[renumber | clear | apply]

renumber ns acls

Synopsis

renumber ns acls

Description

Reorganize ACL priorities. This will introduce gaps between ACL priorities. This command does not affect the behaviour of ACLs.

Example

renumber acls

Top

clear ns acls

Synopsis

clear ns acls

Description

Clear all configured ACLs. This operation does not require an explicit apply.

Example

clear ns acls

Top

apply ns acls

Synopsis

apply ns acls

Description

Commit the ACL in the configuration space to the system. This is required after you add ACLs or modify the ACLs.

Example

apply ns acls

Top

ns info

show ns info

Synopsis

show ns info

Description

Display the most relevant information about a system, including: l Software version l Features that are enabled and disabled l Modes that are enabled and disabled l Whether the system is acting as a normal or master node l The system IP address and mapped IP.

Example

An example of this command's output is shown below:
System Rainier: Build 24, Date: Apr 25 2002, 21:13:25
System IP: 10.101.4.22 (mask: 255.255.0.0)
Mapped IP: 10.101.4.23
Node: Standalone
HTTP port(s): (none)
Max connections: 0
Max requests per connection: 0
Client IP insertion enabled: NO
Cookie version: 0
Feature status:
Web Logging: ON
Surge Protection: ON
Load Balancing: ON
Content Switching: ON
Cache Redirection: ON

Sure Connect: ON
Compression Control: OFF
Priority Queuing: ON
SSL Offloading: ON
Global Server Load Balancing: ON
HTTP DoS Protection: OFF
N+1: OFF
Dynamic Routing: OFF
Content Filtering: ON
Internal Caching: ON
SSL VPN: OFF
Mode status:
Fast Ramp: ON
Layer 2 mode: ON
Use Source IP: OFF

Client Keep-alive: ON
TCP Buffering: OFF
MAC-based forwarding: ON
Edge configuration: OFF
Use Subnet IP: OFF
Layer 3 mode (ip forwarding): ON

ns license

show ns license

Synopsis

show ns license

Description

Display information about the current system license.

ns version

show ns version

Synopsis

show ns version

Description

Display the version and build number of the system.

ns config

[clear | set | unset | save | show | diff]

clear ns config

Synopsis

clear ns config [-force] <level>

Description

Clear NS Config.

Parameters

force

Specifies whether the configurations must be cleared without prompting for confirmation.

level

The types of configurations to be cleared. Possible values basic: Clears all configurations except the following: NSIP, default route (gateway), MIPs, and SNIPs Network settings (DG, VLAN, RHI, NTP and DNS settings) Cluster settings HA node definitions Feature and mode settings nsroot password extended: Clears the same configurations as the .basic. option. In addition, it clears the nsroot password and feature and mode settings. full: Clears all configurations except NSIP, default route, and interface settings. Possible values: basic, extended, full

Top

set ns config

Synopsis

set ns config [-IPAddress <ip_addr> -netmask <netmask>] [-nsvlan <positive_integer> -ifnum <interface_name> ... [-tagged (YES | NO)]]

Description

Sets the NetScaler IP address and NetScaler VLAN. To set other NetScaler parameters, use the "set ns param" command. Note: To change the NSIP address or the NSVLAN of an appliance that is part of a cluster, first remove the appliance from the cluster, change the NSIP or the NSVLAN, and then add the appliance back to the cluster.

Parameters

IPAddress

The IP address of the system.

nsvlan

The VLAN (NSVLAN) for the subnet on which the IP resides. Minimum value: 2 Maximum value: 4094

httpPort

The HTTP ports on the Web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports. Minimum value: 1

maxConn

The maximum number of connections that will be made from the system to the web server(s) attached to it. The value entered here is applied globally to all attached servers. Maximum value: 4294967294

maxReq

The maximum number of requests that the system can pass on a particular connection between the system and a server attached to it. Setting this value to 0 allows an unlimited number of requests to be passed. Maximum value: 65535

cip

The option to control (enable or disable) the insertion of the actual client IP address into the HTTP header request passed from the client to one, some, or all servers attached to the system. The passed address can then be accessed through a minor modification to the server. l If cipHeader is specified, it will be used as the client IP header. l If it is not specified, then the value that has been set by the set ns param CLI command will be used as the client IP header. Possible values: ENABLED, DISABLED

cookieversion

The version of the cookie inserted by system. Possible values: 0, 1

secureCookie

enable/disable secure flag for persistence cookie Possible values: ENABLED, DISABLED Default value: ENABLED

pmtuMin

The minimum Path MTU. Default value: 576 Minimum value: 168 Maximum value: 1500

pmtuTimeout

The timeout value in minutes. Default value: 10 Minimum value: 1 Maximum value: 1440

ftpPortRange

Port range configured for FTP services. Minimum value: 1024 Maximum value: 64000

crPortRange

Port range for cache redirection services. Minimum value: 1 Maximum value: 65535

timezone

Name of the timezone Possible values: GMT+01:00-CET-Europe/Andorra,
GMT+04:00-GST-Asia/Dubai, GMT+04:30-AFT-Asia/Kabul,
GMT-04:00-AST-America/Antigua, GMT-04:00-AST-America/Anguilla,
GMT+01:00-CET-Europe/Tirane, GMT+04:00-AMT-Asia/Yerevan,
GMT+01:00-WAT-Africa/Luanda, GMT+13:00-NZDT-Antarctica/McMurdo,
GMT+13:00-NZDT-Antarctica/South_Pole, GMT-03:00-ROTT-Antarctica/Rothera,
GMT-04:00-CLT-Antarctica/Palmer, GMT+05:00-MAWT-Antarctica/Mawson,
GMT+07:00-DAVT-Antarctica/Davis, GMT+08:00-WST-Antarctica/Casey,
GMT+06:00-VOST-Antarctica/Vostok, GMT+10:00-DDUT-Antarctica/DumontDUrville,
GMT+03:00-SYOT-Antarctica/Syowa, GMT+11:00-MIST-Antarctica/Macquarie,
GMT-03:00-ART-America/Argentina/Buenos_Aires,
GMT-03:00-ART-America/Argentina/Cordoba, GMT-03:00-ART-America/Argentina/Salta,
GMT-03:00-ART-America/Argentina/Jujuy, GMT-03:00-ART-America/Argentina/Tucuman,
GMT-03:00-ART-America/Argentina/Catamarca,
GMT-03:00-ART-America/Argentina/La_Rioja,
GMT-03:00-ART-America/Argentina/San_Juan,
GMT-03:00-ART-America/Argentina/Mendoza,
GMT-03:00-WARST-America/Argentina/San_Luis,
GMT-03:00-ART-America/Argentina/Rio_Gallegos,
GMT-03:00-ART-America/Argentina/Ushuaia, GMT-11:00-SST-Pacific/Pago_Pago,
GMT+01:00-CET-Europe/Vienna, GMT+11:00-LHST-Australia/Lord_Howe,
GMT+11:00-EST-Australia/Hobart, GMT+11:00-EST-Australia/Currie,
GMT+11:00-EST-Australia/Melbourne, GMT+11:00-EST-Australia/Sydney,
GMT+10:30-CST-Australia/Broken_Hill, GMT+10:00-EST-Australia/Brisbane,
GMT+10:00-EST-Australia/Lindeman, GMT+10:30-CST-Australia/Adelaide,
GMT+09:30-CST-Australia/Darwin, GMT+08:00-WST-Australia/Perth,
GMT+08:45-CWST-Australia/Eucla, GMT-04:00-AST-America/Aruba,
GMT+02:00-EET-Europe/Mariehamn, GMT+04:00-AZT-Asia/Baku,
GMT+01:00-CET-Europe/Sarajevo, GMT-04:00-AST-America/Barbados,
GMT+06:00-BDT-Asia/Dhaka, GMT+01:00-CET-Europe/Brussels,
GMT+00:00-GMT-Africa/Ouagadougou, GMT+02:00-EET-Europe/Sofia,
GMT+03:00-AST-Asia/Bahrain, GMT+02:00-CAT-Africa/Bujumbura,
GMT+01:00-WAT-Africa/Porto-Novo, GMT-04:00-AST-America/St_Barthelemy,
GMT-03:00-ADT-Atlantic/Bermuda, GMT+08:00-BNT-Asia/Brunei,
GMT-04:00-BOT-America/La_Paz, GMT-02:00-FNT-America/Noronha,
GMT-03:00-BRT-America/Belem, GMT-03:00-BRT-America/Fortaleza,
GMT-03:00-BRT-America/Recife, GMT-03:00-BRT-America/Araguaina,
GMT-03:00-BRT-America/Maceio, GMT-03:00-BRT-America/Bahia,
GMT-03:00-BRT-America/Sao_Paulo, GMT-04:00-AMT-America/Campo_Grande,
GMT-04:00-AMT-America/Cuiaba, GMT-03:00-BRT-America/Santarem,

GMT-04:00-AMT-America/Porto_Velho, GMT-04:00-AMT-America/Boa_Vista,
GMT-04:00-AMT-America/Manaus, GMT-04:00-AMT-America/Eirunepe,
GMT-04:00-AMT-America/Rio_Branco, GMT-04:00-EDT-America/Nassau,
GMT+06:00-BTT-Asia/Thimphu, GMT+02:00-CAT-Africa/Gaborone,
GMT+03:00-FET-Europe/Minsk, GMT-06:00-CST-America/Belize,
GMT-02:30-NDT-America/St_Johns, GMT-03:00-ADT-America/Halifax,
GMT-03:00-ADT-America/Glace_Bay, GMT-03:00-ADT-America/Moncton,
GMT-03:00-ADT-America/Goose_Bay, GMT-04:00-AST-America/Blanc-Sablon,
GMT-04:00-EDT-America/Montreal, GMT-04:00-EDT-America/Toronto,
GMT-04:00-EDT-America/Nipigon, GMT-04:00-EDT-America/Thunder_Bay,
GMT-04:00-EDT-America/Iqaluit, GMT-04:00-EDT-America/Pangnirtung,
GMT-05:00-CDT-America/Resolute, GMT-05:00-EST-America/Atikokan,
GMT-05:00-CDT-America/Rankin_Inlet, GMT-05:00-CDT-America/Winnipeg,
GMT-05:00-CDT-America/Rainy_River, GMT-06:00-CST-America/Regina,
GMT-06:00-CST-America/Swift_Current, GMT-06:00-MDT-America/Edmonton,
GMT-06:00-MDT-America/Cambridge_Bay, GMT-06:00-MDT-America/Yellowknife,
GMT-06:00-MDT-America/Inuvik, GMT-07:00-MST-America/Dawson_Creek,
GMT-07:00-PDT-America/Vancouver, GMT-07:00-PDT-America/Whitehorse,
GMT-07:00-PDT-America/Dawson, GMT+06:30-CCT-Indian/Cocos,
GMT+01:00-WAT-Africa/Kinshasa, GMT+02:00-CAT-Africa/Lubumbashi,
GMT+01:00-WAT-Africa/Bangui, GMT+01:00-WAT-Africa/Brazzaville,
GMT+01:00-CET-Europe/Zurich, GMT+00:00-GMT-Africa/Abidjan,
GMT-10:00-CKT-Pacific/Rarotonga, GMT-04:00-CLT-America/Santiago,
GMT-06:00-EAST-Pacific/Easter, GMT+01:00-WAT-Africa/Douala,
GMT+08:00-CST-Asia/Shanghai, GMT+08:00-CST-Asia/Harbin,
GMT+08:00-CST-Asia/Chongqing, GMT+08:00-CST-Asia/Urumqi,
GMT+08:00-CST-Asia/Kashgar, GMT-05:00-COT-America/Bogota,
GMT-06:00-CST-America/Costa_Rica, GMT-04:00-CDT-America/Havana,
GMT-01:00-CVT-Atlantic/Cape_Verde, GMT+07:00-CXT-Indian/Christmas,
GMT+02:00-EET-Asia/Nicosia, GMT+01:00-CET-Europe/Prague,
GMT+01:00-CET-Europe/Berlin, GMT+03:00-EAT-Africa/Djibouti,
GMT+01:00-CET-Europe/Copenhagen, GMT-04:00-AST-America/Dominica,
GMT-04:00-AST-America/Santo_Domingo, GMT+01:00-CET-Africa/Algiers,
GMT-05:00-ECT-America/Guayaquil, GMT-06:00-GALT-Pacific/Galapagos,
GMT+02:00-EET-Europe/Tallinn, GMT+02:00-EET-Africa/Cairo,
GMT+00:00-WET-Africa/El_Aaiun, GMT+03:00-EAT-Africa/Asmara,
GMT+01:00-CET-Europe/Madrid, GMT+01:00-CET-Africa/Ceuta,
GMT+00:00-WET-Atlantic/Canary, GMT+03:00-EAT-Africa/Addis_Ababa,
GMT+02:00-EET-Europe/Helsinki, GMT+12:00-FJT-Pacific/Fiji,
GMT-03:00-FKST-Atlantic/Stanley, GMT+10:00-CHUT-Pacific/Chuuk,
GMT+11:00-PONT-Pacific/Pohnpei, GMT+11:00-KOST-Pacific/Kosrae,
GMT+00:00-WET-Atlantic/Faroe, GMT+01:00-CET-Europe/Paris,
GMT+01:00-WAT-Africa/Libreville, GMT+00:00-GMT-Europe/London,
GMT-04:00-AST-America/Grenada, GMT+04:00-GET-Asia/Tbilisi,
GMT-03:00-GFT-America/Cayenne, GMT+00:00-GMT-Europe/Guernsey,
GMT+00:00-GMT-Africa/Accra, GMT+01:00-CET-Europe/Gibraltar,
GMT-03:00-WGT-America/Godthab, GMT+00:00-GMT-America/Danmarkshavn,
GMT-01:00-EGT-America/Scoresbysund, GMT-03:00-ADT-America/Thule,
GMT+00:00-GMT-Africa/Banjul, GMT+00:00-GMT-Africa/Conakry,
GMT-04:00-AST-America/Guadeloupe, GMT+01:00-WAT-Africa/Malabo,
GMT+02:00-EET-Europe/Athens, GMT-02:00-GST-Atlantic/South_Georgia,
GMT-06:00-CST-America/Guatemala, GMT+10:00-ChST-Pacific/Guam,
GMT+00:00-GMT-Africa/Bissau, GMT-04:00-GYT-America/Guyana,
GMT+08:00-HKT-Asia/Hong_Kong, GMT-06:00-CST-America/Tegucigalpa,
GMT+01:00-CET-Europe/Zagreb, GMT-05:00-EST-America/Port-au-Prince,
GMT+01:00-CET-Europe/Budapest, GMT+07:00-WIT-Asia/Jakarta,

GMT+07:00-WIT-Asia/Pontianak, GMT+08:00-CIT-Asia/Makassar,
GMT+09:00-EIT-Asia/Jayapura, GMT+00:00-GMT-Europe/Dublin,
GMT+02:00-IST-Asia/Jerusalem, GMT+00:00-GMT-Europe/Isle_of_Man,
GMT+05:30-IST-Asia/Kolkata, GMT+06:00-IOT-Indian/Chagos,
GMT+03:00-AST-Asia/Baghdad, GMT+03:30-IRST-Asia/Tehran,
GMT+00:00-GMT-Atlantic/Reykjavik, GMT+01:00-CET-Europe/Rome,
GMT+00:00-GMT-Europe/Jersey, GMT-05:00-EST-America/Jamaica,
GMT+02:00-EET-Asia/Amman, GMT+09:00-JST-Asia/Tokyo,
GMT+03:00-EAT-Africa/Nairobi, GMT+06:00-KGT-Asia/Bishkek,
GMT+07:00-ICT-Asia/Phnom_Penh, GMT+12:00-GILT-Pacific/Tarawa,
GMT+13:00-PHOT-Pacific/Enderbury, GMT+14:00-LINT-Pacific/Kiritimati,
GMT+03:00-EAT-Indian/Comoro, GMT-04:00-AST-America/St_Kitts,
GMT+09:00-KST-Asia/Pyongyang, GMT+09:00-KST-Asia/Seoul,
GMT+03:00-AST-Asia/Kuwait, GMT-05:00-EST-America/Cayman,
GMT+06:00-ALMT-Asia/Almaty, GMT+06:00-QYZT-Asia/Qyzylorda,
GMT+05:00-AQTT-Asia/Aqtobe, GMT+05:00-AQTT-Asia/Aqtau,
GMT+05:00-ORAT-Asia/Oral, GMT+07:00-ICT-Asia/Vientiane, GMT+02:00-EET-Asia/Beirut,
GMT-04:00-AST-America/St_Lucia, GMT+01:00-CET-Europe/Vaduz,
GMT+05:30-IST-Asia/Colombo, GMT+00:00-GMT-Africa/Monrovia,
GMT+02:00-SAST-Africa/Maseru, GMT+02:00-EET-Europe/Vilnius,
GMT+01:00-CET-Europe/Luxembourg, GMT+02:00-EET-Europe/Riga,
GMT+02:00-EET-Africa/Tripoli, GMT+00:00-WET-Africa/Casablanca,
GMT+01:00-CET-Europe/Monaco, GMT+02:00-EET-Europe/Chisinau,
GMT+01:00-CET-Europe/Podgorica, GMT-04:00-AST-America/Marigot,
GMT+03:00-EAT-Indian/Antananarivo, GMT+12:00-MHT-Pacific/Majuro,
GMT+12:00-MHT-Pacific/Kwajalein, GMT+01:00-CET-Europe/Skopje,
GMT+00:00-GMT-Africa/Bamako, GMT+06:30-MMT-Asia/Rangoon,
GMT+08:00-ULAT-Asia/Ulaanbaatar, GMT+07:00-HOVT-Asia/Hovd,
GMT+08:00-CHOT-Asia/Choibalsan, GMT+08:00-CST-Asia/Macau,
GMT+10:00-ChST-Pacific/Saipan, GMT-04:00-AST-America/Martinique,
GMT+00:00-GMT-Africa/Nouakchott, GMT-04:00-AST-America/Montserrat,
GMT+01:00-CET-Europe/Malta, GMT+04:00-MUT-Indian/Mauritius,
GMT+05:00-MVT-Indian/Maldives, GMT+02:00-CAT-Africa/Blantyre,
GMT-06:00-CST-America/Mexico_City, GMT-06:00-CST-America/Cancun,
GMT-06:00-CST-America/Merida, GMT-06:00-CST-America/Monterrey,
GMT-05:00-CDT-America/Matamoros, GMT-07:00-MST-America/Mazatlan,
GMT-07:00-MST-America/Chihuahua, GMT-06:00-MDT-America/Ojinaga,
GMT-07:00-MST-America/Hermosillo, GMT-07:00-PDT-America/Tijuana,
GMT-08:00-PST-America/Santa_Isabel, GMT-06:00-CST-America/Bahia_Banderas,
GMT+08:00-MYT-Asia/Kuala_Lumpur, GMT+08:00-MYT-Asia/Kuching,
GMT+02:00-CAT-Africa/Maputo, GMT+02:00-WAST-Africa/Windhoek,
GMT+11:00-NCT-Pacific/Noumea, GMT+01:00-WAT-Africa/Niamey,
GMT+11:30-NFT-Pacific/Norfolk, GMT+01:00-WAT-Africa/Lagos,
GMT-06:00-CST-America/Managua, GMT+01:00-CET-Europe/Amsterdam,
GMT+01:00-CET-Europe/Oslo, GMT+05:45-NPT-Asia/Kathmandu,
GMT+12:00-NRT-Pacific/Nauru, GMT-11:00-NUT-Pacific/Niue,
GMT+13:00-NZDT-Pacific/Auckland, GMT+13:45-CHADT-Pacific/Chatham,
GMT+04:00-GST-Asia/Muscat, GMT-05:00-EST-America/Panama,
GMT-05:00-PET-America/Lima, GMT-10:00-TAHT-Pacific/Tahiti,
GMT-09:30-MART-Pacific/Marquesas, GMT-09:00-GAMT-Pacific/Gambier,
GMT+10:00-PGT-Pacific/Port_Moresby, GMT+08:00-PHT-Asia/Manila,
GMT+05:00-PKT-Asia/Karachi, GMT+01:00-CET-Europe/Warsaw,
GMT-02:00-PMDT-America/Miquelon, GMT-08:00-PST-Pacific/Pitcairn,
GMT-04:00-AST-America/Puerto_Rico, GMT+02:00-EET-Asia/Gaza,
GMT+02:00-EET-Asia/Hebron, GMT+00:00-WET-Europe/Lisbon,
GMT+00:00-WET-Atlantic/Madeira, GMT-01:00-AZOT-Atlantic/Azores,

GMT+09:00-PWT-Pacific/Palau, GMT-03:00-PYST-America/Asuncion,
GMT+03:00-AST-Asia/Qatar, GMT+04:00-RET-Indian/Reunion,
GMT+02:00-EET-Europe/Bucharest, GMT+01:00-CET-Europe/Belgrade,
GMT+03:00-FET-Europe/Kaliningrad, GMT+04:00-MSK-Europe/Moscow,
GMT+04:00-VOLT-Europe/Volgograd, GMT+04:00-SAMT-Europe/Samara,
GMT+06:00-YEKT-Asia/Yekaterinburg, GMT+07:00-OMST-Asia/Omsk,
GMT+07:00-NOVT-Asia/Novosibirsk, GMT+07:00-NOVT-Asia/Novokuznetsk,
GMT+08:00-KRAT-Asia/Krasnoyarsk, GMT+09:00-IRKT-Asia/Irkutsk,
GMT+10:00-YAKT-Asia/Yakutsk, GMT+11:00-VLAT-Asia/Vladivostok,
GMT+11:00-SAKT-Asia/Sakhalin, GMT+12:00-MAGT-Asia/Magadan,
GMT+12:00-PETT-Asia/Kamchatka, GMT+12:00-ANAT-Asia/Anadyr,
GMT+02:00-CAT-Africa/Kigali, GMT+03:00-AST-Asia/Riyadh,
GMT+11:00-SBT-Pacific/Guadalcanal, GMT+04:00-SCT-Indian/Mahe,
GMT+03:00-EAT-Africa/Khartoum, GMT+01:00-CET-Europe/Stockholm,
GMT+08:00-SGT-Asia/Singapore, GMT+00:00-GMT-Atlantic/St_Helena,
GMT+01:00-CET-Europe/Ljubljana, GMT+01:00-CET-Arctic/Longyearbyen,
GMT+01:00-CET-Europe/Bratislava, GMT+00:00-GMT-Africa/Freetown,
GMT+01:00-CET-Europe/San_Marino, GMT+00:00-GMT-Africa/Dakar,
GMT+03:00-EAT-Africa/Mogadishu, GMT-03:00-SRT-America/Paramaribo,
GMT+00:00-GMT-Africa/Sao_Tome, GMT-06:00-CST-America/El_Salvador,
GMT+02:00-EET-Asia/Damascus, GMT+02:00-SAST-Africa/Mbabane,
GMT-04:00-EDT-America/Grand_Turk, GMT+01:00-WAT-Africa/Ndjamena,
GMT+05:00-TFT-Indian/Kerguelen, GMT+00:00-GMT-Africa/Lome,
GMT+07:00-ICT-Asia/Bangkok, GMT+05:00-TJT-Asia/Dushanbe,
GMT-10:00-TKT-Pacific/Fakaofo, GMT+09:00-TLT-Asia/Dili,
GMT+05:00-TMT-Asia/Ashgabat, GMT+01:00-CET-Africa/Tunis,
GMT+13:00-TOT-Pacific/Tongatapu, GMT+02:00-EET-Europe/Istanbul,
GMT-04:00-AST-America/Port_of_Spain, GMT+12:00-TVT-Pacific/Funafuti,
GMT+08:00-CST-Asia/Taipei, GMT+03:00-EAT-Africa/Dar_es_Salaam,
GMT+02:00-EET-Europe/Kiev, GMT+02:00-EET-Europe/Uzhgorod,
GMT+02:00-EET-Europe/Zaporozhye, GMT+02:00-EET-Europe/Simferopol,
GMT+03:00-EAT-Africa/Kampala, GMT-10:00-HST-Pacific/Johnston,
GMT-11:00-SST-Pacific/Midway, GMT+12:00-WAKT-Pacific/Wake,
GMT-04:00-EDT-America/New_York, GMT-04:00-EDT-America/Detroit,
GMT-04:00-EDT-America/Kentucky/Louisville,
GMT-04:00-EDT-America/Kentucky/Monticello,
GMT-04:00-EDT-America/Indiana/Indianapolis,
GMT-04:00-EDT-America/Indiana/Vincennes, GMT-04:00-EDT-America/Indiana/Winamac,
GMT-04:00-EDT-America/Indiana/Marengo, GMT-04:00-EDT-America/Indiana/Petersburg,
GMT-04:00-EDT-America/Indiana/Vevay, GMT-05:00-CDT-America/Chicago,
GMT-05:00-CDT-America/Indiana/Tell_City, GMT-05:00-CDT-America/Indiana/Knox,
GMT-05:00-CDT-America/Menominee, GMT-05:00-CDT-America/North_Dakota/Center,
GMT-05:00-CDT-America/North_Dakota/New_Salem,
GMT-05:00-CDT-America/North_Dakota/Beulah, GMT-06:00-MDT-America/Denver,
GMT-06:00-MDT-America/Boise, GMT-06:00-MDT-America/Shiprock,
GMT-07:00-MST-America/Phoenix, GMT-07:00-PDT-America/Los_Angeles,
GMT-08:00-AKDT-America/Anchorage, GMT-08:00-AKDT-America/Juneau,
GMT-08:00-AKDT-America/Sitka, GMT-08:00-AKDT-America/Yakutat,
GMT-08:00-AKDT-America/Nome, GMT-09:00-HADT-America/Adak,
GMT-08:00-MeST-America/Metlakatla, GMT-10:00-HST-Pacific/Honolulu,
GMT-03:00-UYT-America/Montevideo, GMT+05:00-UZT-Asia/Samarkand,
GMT+05:00-UZT-Asia/Tashkent, GMT+01:00-CET-Europe/Vatican,
GMT-04:00-AST-America/St_Vincent, GMT-04:30-VET-America/Caracas,
GMT-04:00-AST-America/Tortola, GMT-04:00-AST-America/St_Thomas,
GMT+07:00-ICT-Asia/Ho_Chi_Minh, GMT+11:00-VUT-Pacific/Efate,
GMT+12:00-WFT-Pacific/Wallis, GMT+14:00-WSDT-Pacific/Apia,

GMT+03:00-AST-Asia/Aden, GMT+03:00-EAT-Indian/Mayotte, GMT+02:00-SAST-Africa/Johannesburg, GMT+02:00-CAT-Africa/Lusaka, GMT+02:00-CAT-Africa/Harare

grantQuotaMaxClient

The percentage of shared quota to be granted at a time for maxClient Default value: 10 Maximum value: 100

exclusiveQuotaMaxClient

The percentage of maxClient to be given to PEs Default value: 80 Maximum value: 100

grantQuotaSpillOver

The percentage of shared quota to be granted at a time for spillover Default value: 10 Maximum value: 100

exclusiveQuotaSpillOver

The percentage of max limit to be given to PEs Default value: 80 Maximum value: 100

Top

unset ns config

Synopsis

unset ns config [-nsvlan] [-IPAddress] [-netmask] [-ifnum] [-tagged]

Description

Unset the system parameters. Use "unset nsparam" command to unset other netscaler parameters..Refer to the set ns config command for meanings of the arguments.

Top

save ns config

Synopsis

save ns config

Description

Save the system configuration to the system's FLASH. In a high availability setup, the command is sent to the primary system. The primary system then forwards the command to the secondary system. The entire system configuration is saved to the ns.conf file located in the /nsconfig directory. Backup configuration files are named ns.conf.n. The most recent backup file has the smallest value for n.

Top

show ns config

Synopsis

show ns config

Description

Display the version, build, and feature information of the system. Note: If you want to see the complete configuration parameters that have been set for the system, use ns runningconfig.

Top

diff ns config

Synopsis

diff ns config [<config1>] [<config2>] [-outtype (cli | xml)] [-template] [-ignoreDeviceSpecific]

Description

Difference between two configuration

Parameters

config1

Config options.

config2

Config options.

outtype

The format in which result is desired. Possible values: cli, xml

template

Enable template diff.This will only compare commands given in template file.

ignoreDeviceSpecific

Suppress device specific differences

Example

diff ns config runningconfig savedConfig

Top

ns param

[set | unset | show]

set ns param

Synopsis

set ns param [-httpPort <port> ...] [-maxConn <positive_integer>] [-maxReq <positive_integer>] [-cip (ENABLED | DISABLED) <cipHeader>] [-cookieversion (0 | 1)] [-secureCookie (ENABLED | DISABLED)] [-pmtuMin <positive_integer>] [-pmtuTimeout <mins>] [-ftpPortRange <int[-int]>] [-crPortRange <int[-int]>] [-timezone <timezone>] [-grantQuotaMaxClient <positive_integer>] [-exclusiveQuotaMaxClient <positive_integer>] [-grantQuotaSpillOver <positive_integer>] [-exclusiveQuotaSpillOver <positive_integer>]

Description

Set the netscaler parameters.

Parameters

httpPort

The HTTP ports on the Web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports. Minimum value: 1

maxConn

The maximum number of connections that will be made from the system to the web server(s) attached to it. The value entered here is applied globally to all attached servers. Maximum value: 4294967294

maxReq

The maximum number of requests that the system can pass on a particular connection between the system and a server attached to it. Setting this value to 0 allows an unlimited number of requests to be passed. Maximum value: 65535

cip

The option to control (enable or disable) the insertion of the actual client IP address into the HTTP header request passed from the client to one, some, or all servers attached to the system. The passed address can then be accessed through a minor modification to the server. l If cipHeader is specified, it will be used as the client IP header. l If it is not specified, then the value that has been set by the set ns param CLI command will be used as the client IP header. Possible values: ENABLED, DISABLED

cookieversion

The version of the cookie inserted by system. Possible values: 0, 1

secureCookie

enable/disable secure flag for persistence cookie Possible values: ENABLED, DISABLED Default value: ENABLED

pmtuMin

The minimum Path MTU. Default value: 576 Minimum value: 168 Maximum value: 1500

pmtuTimeout

The timeout value in minutes. Default value: 10 Minimum value: 1 Maximum value: 1440

ftpPortRange

Port range configured for FTP services. Minimum value: 1024 Maximum value: 64000

crPortRange

Port range for cache redirection services. Minimum value: 1 Maximum value: 65535

timezone

Name of the timezone Possible values: GMT+01:00-CET-Europe/Andorra, GMT+04:00-GST-Asia/Dubai, GMT+04:30-AFT-Asia/Kabul, GMT-04:00-AST-America/Antigua, GMT-04:00-AST-America/Anguilla, GMT+01:00-CET-Europe/Tirane, GMT+04:00-AMT-Asia/Yerevan, GMT+01:00-WAT-Africa/Luanda, GMT+13:00-NZDT-Antarctica/McMurdo, GMT+13:00-NZDT-Antarctica/South_Pole, GMT-03:00-ROTT-Antarctica/Rothera, GMT-04:00-CLT-Antarctica/Palmer, GMT+05:00-MAWT-Antarctica/Mawson, GMT+07:00-DAVT-Antarctica/Davis, GMT+08:00-WST-Antarctica/Casey, GMT+06:00-VOST-Antarctica/Vostok, GMT+10:00-DDUT-Antarctica/DumontDUrville, GMT+03:00-SYOT-Antarctica/Syowa, GMT+11:00-MIST-Antarctica/Macquarie, GMT-03:00-ART-America/Argentina/Buenos_Aires, GMT-03:00-ART-America/Argentina/Cordoba, GMT-03:00-ART-America/Argentina/Salta, GMT-03:00-ART-America/Argentina/Jujuy, GMT-03:00-ART-America/Argentina/Tucuman, GMT-03:00-ART-America/Argentina/Catamarca, GMT-03:00-ART-America/Argentina/La_Rioja, GMT-03:00-ART-America/Argentina/San_Juan, GMT-03:00-ART-America/Argentina/Mendoza, GMT-03:00-WARST-America/Argentina/San_Luis, GMT-03:00-ART-America/Argentina/Rio_Gallegos, GMT-03:00-ART-America/Argentina/Ushuaia, GMT-11:00-SST-Pacific/Pago_Pago, GMT+01:00-CET-Europe/Vienna, GMT+11:00-LHST-Australia/Lord_Howe, GMT+11:00-EST-Australia/Hobart, GMT+11:00-EST-Australia/Currie, GMT+11:00-EST-Australia/Melbourne, GMT+11:00-EST-Australia/Sydney, GMT+10:30-CST-Australia/Broken_Hill, GMT+10:00-EST-Australia/Brisbane, GMT+10:00-EST-Australia/Lindeman, GMT+10:30-CST-Australia/Adelaide, GMT+09:30-CST-Australia/Darwin, GMT+08:00-WST-Australia/Perth, GMT+08:45-CWST-Australia/Eucla, GMT-04:00-AST-America/Aruba, GMT+02:00-EET-Europe/Mariehamn, GMT+04:00-AZT-Asia/Baku, GMT+01:00-CET-Europe/Sarajevo, GMT-04:00-AST-America/Barbados,

GMT+06:00-BDT-Asia/Dhaka, GMT+01:00-CET-Europe/Brussels,
GMT+00:00-GMT-Africa/Ouagadougou, GMT+02:00-EET-Europe/Sofia,
GMT+03:00-AST-Asia/Bahrain, GMT+02:00-CAT-Africa/Bujumbura,
GMT+01:00-WAT-Africa/Porto-Novo, GMT-04:00-AST-America/St_Barthelemy,
GMT-03:00-ADT-Atlantic/Bermuda, GMT+08:00-BNT-Asia/Brunei,
GMT-04:00-BOT-America/La_Paz, GMT-02:00-FNT-America/Noronha,
GMT-03:00-BRT-America/Belem, GMT-03:00-BRT-America/Fortaleza,
GMT-03:00-BRT-America/Recife, GMT-03:00-BRT-America/Araguaina,
GMT-03:00-BRT-America/Maceio, GMT-03:00-BRT-America/Bahia,
GMT-03:00-BRT-America/Sao_Paulo, GMT-04:00-AMT-America/Campo_Grande,
GMT-04:00-AMT-America/Cuiaba, GMT-03:00-BRT-America/Santarem,
GMT-04:00-AMT-America/Porto_Velho, GMT-04:00-AMT-America/Boa_Vista,
GMT-04:00-AMT-America/Manaus, GMT-04:00-AMT-America/Eirunepe,
GMT-04:00-AMT-America/Rio_Branco, GMT-04:00-EDT-America/Nassau,
GMT+06:00-BTT-Asia/Thimphu, GMT+02:00-CAT-Africa/Gaborone,
GMT+03:00-FET-Europe/Minsk, GMT-06:00-CST-America/Belize,
GMT-02:30-NDT-America/St_Johns, GMT-03:00-ADT-America/Halifax,
GMT-03:00-ADT-America/Glace_Bay, GMT-03:00-ADT-America/Moncton,
GMT-03:00-ADT-America/Goose_Bay, GMT-04:00-AST-America/Blanc-Sablon,
GMT-04:00-EDT-America/Montreal, GMT-04:00-EDT-America/Toronto,
GMT-04:00-EDT-America/Nipigon, GMT-04:00-EDT-America/Thunder_Bay,
GMT-04:00-EDT-America/Iqaluit, GMT-04:00-EDT-America/Pangnirtung,
GMT-05:00-CDT-America/Resolute, GMT-05:00-EST-America/Atikokan,
GMT-05:00-CDT-America/Rankin_Inlet, GMT-05:00-CDT-America/Winnipeg,
GMT-05:00-CDT-America/Rainy_River, GMT-06:00-CST-America/Regina,
GMT-06:00-CST-America/Swift_Current, GMT-06:00-MDT-America/Edmonton,
GMT-06:00-MDT-America/Cambridge_Bay, GMT-06:00-MDT-America/Yellowknife,
GMT-06:00-MDT-America/Inuvik, GMT-07:00-MST-America/Dawson_Creek,
GMT-07:00-PDT-America/Vancouver, GMT-07:00-PDT-America/Whitehorse,
GMT-07:00-PDT-America/Dawson, GMT+06:30-CCT-Indian/Cocos,
GMT+01:00-WAT-Africa/Kinshasa, GMT+02:00-CAT-Africa/Lubumbashi,
GMT+01:00-WAT-Africa/Bangui, GMT+01:00-WAT-Africa/Brazzaville,
GMT+01:00-CET-Europe/Zurich, GMT+00:00-GMT-Africa/Abidjan,
GMT-10:00-CKT-Pacific/Rarotonga, GMT-04:00-CLT-America/Santiago,
GMT-06:00-EAST-Pacific/Easter, GMT+01:00-WAT-Africa/Douala,
GMT+08:00-CST-Asia/Shanghai, GMT+08:00-CST-Asia/Harbin,
GMT+08:00-CST-Asia/Chongqing, GMT+08:00-CST-Asia/Urumqi,
GMT+08:00-CST-Asia/Kashgar, GMT-05:00-COT-America/Bogota,
GMT-06:00-CST-America/Costa_Rica, GMT-04:00-CDT-America/Havana,
GMT-01:00-CVT-Atlantic/Cape_Verde, GMT+07:00-CXT-Indian/Christmas,
GMT+02:00-EET-Asia/Nicosia, GMT+01:00-CET-Europe/Prague,
GMT+01:00-CET-Europe/Berlin, GMT+03:00-EAT-Africa/Djibouti,
GMT+01:00-CET-Europe/Copenhagen, GMT-04:00-AST-America/Dominica,
GMT-04:00-AST-America/Santo_Domingo, GMT+01:00-CET-Africa/Algiers,
GMT-05:00-ECT-America/Guayaquil, GMT-06:00-GALT-Pacific/Galapagos,
GMT+02:00-EET-Europe/Tallinn, GMT+02:00-EET-Africa/Cairo,
GMT+00:00-WET-Africa/El_Aaiun, GMT+03:00-EAT-Africa/Asmara,
GMT+01:00-CET-Europe/Madrid, GMT+01:00-CET-Africa/Ceuta,
GMT+00:00-WET-Atlantic/Canary, GMT+03:00-EAT-Africa/Addis_Ababa,
GMT+02:00-EET-Europe/Helsinki, GMT+12:00-FJT-Pacific/Fiji,
GMT-03:00-FKST-Atlantic/Stanley, GMT+10:00-CHUT-Pacific/Chuuk,
GMT+11:00-PONT-Pacific/Pohnpei, GMT+11:00-KOST-Pacific/Kosrae,
GMT+00:00-WET-Atlantic/Faroe, GMT+01:00-CET-Europe/Paris,
GMT+01:00-WAT-Africa/Libreville, GMT+00:00-GMT-Europe/London,
GMT-04:00-AST-America/Grenada, GMT+04:00-GET-Asia/Tbilisi,
GMT-03:00-GFT-America/Cayenne, GMT+00:00-GMT-Europe/Guernsey,

GMT+00:00-GMT-Africa/Accra, GMT+01:00-CET-Europe/Gibraltar,
GMT-03:00-WGT-America/Godthab, GMT+00:00-GMT-America/Danmarkshavn,
GMT-01:00-EGT-America/Scoresbysund, GMT-03:00-ADT-America/Thule,
GMT+00:00-GMT-Africa/Banjul, GMT+00:00-GMT-Africa/Conakry,
GMT-04:00-AST-America/Guadeloupe, GMT+01:00-WAT-Africa/Malabo,
GMT+02:00-EET-Europe/Athens, GMT-02:00-GST-Atlantic/South_Georgia,
GMT-06:00-CST-America/Guatemala, GMT+10:00-ChST-Pacific/Guam,
GMT+00:00-GMT-Africa/Bissau, GMT-04:00-GYT-America/Guyana,
GMT+08:00-HKT-Asia/Hong_Kong, GMT-06:00-CST-America/Tegucigalpa,
GMT+01:00-CET-Europe/Zagreb, GMT-05:00-EST-America/Port-au-Prince,
GMT+01:00-CET-Europe/Budapest, GMT+07:00-WIT-Asia/Jakarta,
GMT+07:00-WIT-Asia/Pontianak, GMT+08:00-CIT-Asia/Makassar,
GMT+09:00-EIT-Asia/Jayapura, GMT+00:00-GMT-Europe/Dublin,
GMT+02:00-IST-Asia/Jerusalem, GMT+00:00-GMT-Europe/Isle_of_Man,
GMT+05:30-IST-Asia/Kolkata, GMT+06:00-IOT-Indian/Chagos,
GMT+03:00-AST-Asia/Baghdad, GMT+03:30-IRST-Asia/Tehran,
GMT+00:00-GMT-Atlantic/Reykjavik, GMT+01:00-CET-Europe/Rome,
GMT+00:00-GMT-Europe/Jersey, GMT-05:00-EST-America/Jamaica,
GMT+02:00-EET-Asia/Amman, GMT+09:00-JST-Asia/Tokyo,
GMT+03:00-EAT-Africa/Nairobi, GMT+06:00-KGT-Asia/Bishkek,
GMT+07:00-ICT-Asia/Phnom_Penh, GMT+12:00-GILT-Pacific/Tarawa,
GMT+13:00-PHOT-Pacific/Enderbury, GMT+14:00-LINT-Pacific/Kiritimati,
GMT+03:00-EAT-Indian/Comoro, GMT-04:00-AST-America/St_Kitts,
GMT+09:00-KST-Asia/Pyongyang, GMT+09:00-KST-Asia/Seoul,
GMT+03:00-AST-Asia/Kuwait, GMT-05:00-EST-America/Cayman,
GMT+06:00-ALMT-Asia/Almaty, GMT+06:00-QYZT-Asia/Qyzylorda,
GMT+05:00-AQTT-Asia/Aqtobe, GMT+05:00-AQTT-Asia/Aqtau,
GMT+05:00-ORAT-Asia/Oral, GMT+07:00-ICT-Asia/Vientiane, GMT+02:00-EET-Asia/Beirut,
GMT-04:00-AST-America/St_Lucia, GMT+01:00-CET-Europe/Vaduz,
GMT+05:30-IST-Asia/Colombo, GMT+00:00-GMT-Africa/Monrovia,
GMT+02:00-SAST-Africa/Maseru, GMT+02:00-EET-Europe/Vilnius,
GMT+01:00-CET-Europe/Luxembourg, GMT+02:00-EET-Europe/Riga,
GMT+02:00-EET-Africa/Tripoli, GMT+00:00-WET-Africa/Casablanca,
GMT+01:00-CET-Europe/Monaco, GMT+02:00-EET-Europe/Chisinau,
GMT+01:00-CET-Europe/Podgorica, GMT-04:00-AST-America/Marigot,
GMT+03:00-EAT-Indian/Antananarivo, GMT+12:00-MHT-Pacific/Majuro,
GMT+12:00-MHT-Pacific/Kwajalein, GMT+01:00-CET-Europe/Skopje,
GMT+00:00-GMT-Africa/Bamako, GMT+06:30-MMT-Asia/Rangoon,
GMT+08:00-ULAT-Asia/Ulaanbaatar, GMT+07:00-HOVT-Asia/Hovd,
GMT+08:00-CHOT-Asia/Choibalsan, GMT+08:00-CST-Asia/Macau,
GMT+10:00-ChST-Pacific/Saipan, GMT-04:00-AST-America/Martinique,
GMT+00:00-GMT-Africa/Nouakchott, GMT-04:00-AST-America/Montserrat,
GMT+01:00-CET-Europe/Malta, GMT+04:00-MUT-Indian/Mauritius,
GMT+05:00-MVT-Indian/Maldives, GMT+02:00-CAT-Africa/Blantyre,
GMT-06:00-CST-America/Mexico_City, GMT-06:00-CST-America/Cancun,
GMT-06:00-CST-America/Merida, GMT-06:00-CST-America/Monterrey,
GMT-05:00-CDT-America/Matamoros, GMT-07:00-MST-America/Mazatlan,
GMT-07:00-MST-America/Chihuahua, GMT-06:00-MDT-America/Ojinaga,
GMT-07:00-MST-America/Hermosillo, GMT-07:00-PDT-America/Tijuana,
GMT-08:00-PST-America/Santa_Isabel, GMT-06:00-CST-America/Bahia_Banderas,
GMT+08:00-MYT-Asia/Kuala_Lumpur, GMT+08:00-MYT-Asia/Kuching,
GMT+02:00-CAT-Africa/Maputo, GMT+02:00-WAST-Africa/Windhoek,
GMT+11:00-NCT-Pacific/Noumea, GMT+01:00-WAT-Africa/Niamey,
GMT+11:30-NFT-Pacific/Norfolk, GMT+01:00-WAT-Africa/Lagos,
GMT-06:00-CST-America/Managua, GMT+01:00-CET-Europe/Amsterdam,
GMT+01:00-CET-Europe/Oslo, GMT+05:45-NPT-Asia/Kathmandu,

GMT+12:00-NRT-Pacific/Nauru, GMT-11:00-NUT-Pacific/Niue,
GMT+13:00-NZDT-Pacific/Auckland, GMT+13:45-CHADT-Pacific/Chatham,
GMT+04:00-GST-Asia/Muscat, GMT-05:00-EST-America/Panama,
GMT-05:00-PET-America/Lima, GMT-10:00-TAHT-Pacific/Tahiti,
GMT-09:30-MART-Pacific/Marquesas, GMT-09:00-GAMT-Pacific/Gambier,
GMT+10:00-PGT-Pacific/Port_Moresby, GMT+08:00-PHT-Asia/Manila,
GMT+05:00-PKT-Asia/Karachi, GMT+01:00-CET-Europe/Warsaw,
GMT-02:00-PMDT-America/Miquelon, GMT-08:00-PST-Pacific/Pitcairn,
GMT-04:00-AST-America/Puerto_Rico, GMT+02:00-EET-Asia/Gaza,
GMT+02:00-EET-Asia/Hebron, GMT+00:00-WET-Europe/Lisbon,
GMT+00:00-WET-Atlantic/Madeira, GMT-01:00-AZOT-Atlantic/Azores,
GMT+09:00-PWT-Pacific/Palau, GMT-03:00-PYST-America/Asuncion,
GMT+03:00-AST-Asia/Qatar, GMT+04:00-RET-Indian/Reunion,
GMT+02:00-EET-Europe/Bucharest, GMT+01:00-CET-Europe/Belgrade,
GMT+03:00-FET-Europe/Kaliningrad, GMT+04:00-MSK-Europe/Moscow,
GMT+04:00-VOLT-Europe/Volgograd, GMT+04:00-SAMT-Europe/Samara,
GMT+06:00-YEKT-Asia/Yekaterinburg, GMT+07:00-OMST-Asia/Omsk,
GMT+07:00-NOVT-Asia/Novosibirsk, GMT+07:00-NOVT-Asia/Novokuznetsk,
GMT+08:00-KRAT-Asia/Krasnoyarsk, GMT+09:00-IRKT-Asia/Irkutsk,
GMT+10:00-YAKT-Asia/Yakutsk, GMT+11:00-VLAT-Asia/Vladivostok,
GMT+11:00-SAKT-Asia/Sakhalin, GMT+12:00-MAGT-Asia/Magadan,
GMT+12:00-PETT-Asia/Kamchatka, GMT+12:00-ANAT-Asia/Anadyr,
GMT+02:00-CAT-Africa/Kigali, GMT+03:00-AST-Asia/Riyadh,
GMT+11:00-SBT-Pacific/Guadalcanal, GMT+04:00-SCT-Indian/Mahe,
GMT+03:00-EAT-Africa/Khartoum, GMT+01:00-CET-Europe/Stockholm,
GMT+08:00-SGT-Asia/Singapore, GMT+00:00-GMT-Atlantic/St_Helena,
GMT+01:00-CET-Europe/Ljubljana, GMT+01:00-CET-Arctic/Longyearbyen,
GMT+01:00-CET-Europe/Bratislava, GMT+00:00-GMT-Africa/Freetown,
GMT+01:00-CET-Europe/San_Marino, GMT+00:00-GMT-Africa/Dakar,
GMT+03:00-EAT-Africa/Mogadishu, GMT-03:00-SRT-America/Paramaribo,
GMT+00:00-GMT-Africa/Sao_Tome, GMT-06:00-CST-America/El_Salvador,
GMT+02:00-EET-Asia/Damascus, GMT+02:00-SAST-Africa/Mbabane,
GMT-04:00-EDT-America/Grand_Turk, GMT+01:00-WAT-Africa/Ndjamena,
GMT+05:00-TFT-Indian/Kerguelen, GMT+00:00-GMT-Africa/Lome,
GMT+07:00-ICT-Asia/Bangkok, GMT+05:00-TJT-Asia/Dushanbe,
GMT-10:00-TKT-Pacific/Fakaofo, GMT+09:00-TLT-Asia/Dili,
GMT+05:00-TMT-Asia/Ashgabat, GMT+01:00-CET-Africa/Tunis,
GMT+13:00-TOT-Pacific/Tongatapu, GMT+02:00-EET-Europe/Istanbul,
GMT-04:00-AST-America/Port_of_Spain, GMT+12:00-TVT-Pacific/Funafuti,
GMT+08:00-CST-Asia/Taipei, GMT+03:00-EAT-Africa/Dar_es_Salaam,
GMT+02:00-EET-Europe/Kiev, GMT+02:00-EET-Europe/Uzhgorod,
GMT+02:00-EET-Europe/Zaporozhye, GMT+02:00-EET-Europe/Simferopol,
GMT+03:00-EAT-Africa/Kampala, GMT-10:00-HST-Pacific/Johnston,
GMT-11:00-SST-Pacific/Midway, GMT+12:00-WAKT-Pacific/Wake,
GMT-04:00-EDT-America/New_York, GMT-04:00-EDT-America/Detroit,
GMT-04:00-EDT-America/Kentucky/Louisville,
GMT-04:00-EDT-America/Kentucky/Monticello,
GMT-04:00-EDT-America/Indiana/Indianapolis,
GMT-04:00-EDT-America/Indiana/Vincennes, GMT-04:00-EDT-America/Indiana/Winamac,
GMT-04:00-EDT-America/Indiana/Marengo, GMT-04:00-EDT-America/Indiana/Petersburg,
GMT-04:00-EDT-America/Indiana/Vevay, GMT-05:00-CDT-America/Chicago,
GMT-05:00-CDT-America/Indiana/Tell_City, GMT-05:00-CDT-America/Indiana/Knox,
GMT-05:00-CDT-America/Menominee, GMT-05:00-CDT-America/North_Dakota/Center,
GMT-05:00-CDT-America/North_Dakota/New_Salem,
GMT-05:00-CDT-America/North_Dakota/Beulah, GMT-06:00-MDT-America/Denver,
GMT-06:00-MDT-America/Boise, GMT-06:00-MDT-America/Shiprock,

GMT-07:00-MST-America/Phoenix, GMT-07:00-PDT-America/Los_Angeles, GMT-08:00-AKDT-America/Anchorage, GMT-08:00-AKDT-America/Juneau, GMT-08:00-AKDT-America/Sitka, GMT-08:00-AKDT-America/Yakutat, GMT-08:00-AKDT-America/Nome, GMT-09:00-HADT-America/Adak, GMT-08:00-MeST-America/Metlakatla, GMT-10:00-HST-Pacific/Honolulu, GMT-03:00-UYT-America/Montevideo, GMT+05:00-UZT-Asia/Samarkand, GMT+05:00-UZT-Asia/Tashkent, GMT+01:00-CET-Europe/Vatican, GMT-04:00-AST-America/St_Vincent, GMT-04:30-VET-America/Caracas, GMT-04:00-AST-America/Tortola, GMT-04:00-AST-America/St_Thomas, GMT+07:00-ICT-Asia/Ho_Chi_Minh, GMT+11:00-VUT-Pacific/Efate, GMT+12:00-WFT-Pacific/Wallis, GMT+14:00-WSDT-Pacific/Apia, GMT+03:00-AST-Asia/Aden, GMT+03:00-EAT-Indian/Mayotte, GMT+02:00-SAST-Africa/Johannesburg, GMT+02:00-CAT-Africa/Lusaka, GMT+02:00-CAT-Africa/Harare

grantQuotaMaxClient

The percentage of shared quota to be granted at a time for maxClient Default value: 10 Maximum value: 100

exclusiveQuotaMaxClient

The percentage of maxClient to be given to PEs Default value: 80 Maximum value: 100

grantQuotaSpillOver

The percentage of shared quota to be granted at a time for spillover Default value: 10 Maximum value: 100

exclusiveQuotaSpillOver

The percentage of max limit to be given to PEs Default value: 80 Maximum value: 100

Top

unset ns param

Synopsis

unset ns param [-ftpPortRange] [-crPortRange] [-timezone] [-httpPort] [-maxConn] [-maxReq] [-cip] [-cipHeader] [-cookieversion] [-secureCookie] [-pmtuMin] [-pmtuTimeout] [-grantQuotaMaxClient] [-exclusiveQuotaMaxClient] [-grantQuotaSpillOver] [-exclusiveQuotaSpillOver]

Description

Unset the netscaler parameters..Refer to the set ns param command for meanings of the arguments.

Top

show ns param

Synopsis

show ns param

Description

Display the version, build, and feature information of the system. Note: If you want to see the complete configuration parameters that have been set for the system, use ns runningconfig.

Top

ns acls6

[clear | apply | renumber]

clear ns acls6

Synopsis

clear ns acls6

Description

Clear all configured ACL6. This operation does not require an explicit apply.

Example

clear ns acls6

Top

apply ns acls6

Synopsis

apply ns acls6

Description

Commit the ACL6 in the configuration space to the system. This is required after an ACL6 is added or modified.

Example

apply ns acls6

Top

renumber ns acls6

Synopsis

renumber ns acls6

Description

Reorganize ACL6 priorities. This will introduce gaps between ACL6 priorities. This command does not affect the behaviour of ACLs.

Example

renumber acls6

Top

ns pbrs

[renumber | clear | apply]

renumber ns pbrs

Synopsis

renumber ns pbrs

Description

Reorganize Policy Based Routing(PBR) priorities. This will introduce gaps between PBR priorities. This command does not affect the behaviour of PBRs.

Example

renumber pbrs

Top

clear ns pbrs

Synopsis

clear ns pbrs

Description

Clear all configured Policy Based Routing(PBR). This operation does not require an explicit 'apply pbrs' commad.

Example

clear ns pbrs

Top

apply ns pbrs

Synopsis

apply ns pbrs

Description

Commit the Policy Based Routing(PBR) in the configuration space to the system. This is required after you add PBRs or modify the PBRs.

Example

apply ns pbrs

Top

ns connectiontable

show ns connectiontable

Synopsis

show ns connectiontable [<filterexpression>] [-detail <detail> ...]

Description

Display the current TCP/IP connection table

Parameters

filterexpression

The maximum length of filter expression is 255 and it can be of following format: <expression> [<relop> <expression>] <relop> = (&& | ||) connectiontable supports two types of filter expressions: Classic Expressions: <expression> = the expression string in the format: <qualifier> <operator> <qualifier-value> <qualifier> = SOURCEIP. <qualifier-value> = A valid IP address. <qualifier> = SOURCEPORT. <qualifier-value> = A valid port number. <qualifier> = DESTIP. <qualifier-value> = A valid IP address. <qualifier> = DESTPORT. <qualifier-value> = A valid port number. <qualifier> = IP. <qualifier-value> = A valid IP address. <qualifier> = PORT. <qualifier-value> = A valid port number. <qualifier> = IDLETIME. <qualifier-value> = A positive integer indicating the idle time. <qualifier> = SVCNAME. <qualifier-value> = The name of a service. <qualifier> = VSVRNAME. <qualifier-value> = The name of a vserver. <qualifier> = CONNID <qualifier-value> = A valid PCB dev number. <qualifier> = INTF <qualifier-value> = A valid interface id in the form of x/y (n/x/y in case of cluster interface). <qualifier> = VLAN <qualifier-value> = A valid VLAN ID. <qualifier> = STATE. <qualifier-value> = (CLOSE_WAIT | CLOSED | CLOSING | ESTABLISHED | FIN_WAIT_1 | FIN_WAIT_2 | LAST_ACK | LISTEN | SYN_RECEIVED | SYN_SENT | TIME_WAIT) <qualifier> = SVCTYPE. <qualifier-value> = (HTTP | FTP | TCP | UDP | SSL | SSL_BRIDGE | SSL_TCP | NNTP | RPCSVR | RPCSVRS | RPCCLNT | DNS | ADNS | SNMP | RTSP | DHCPRA | ANY | MONITOR | MONITOR_UDP | MONITOR_PING | SIP_UDP | MYSQL | MSSQL | UNKNOWN) <operator> = (== | eq | != | neq | > | gt | < | lt | >= | ge | <= | le | BETWEEN) Default Expressions: <expression> = CONNECTION.<qualifier>.<qualifier-method>.(<qualifier-value>) <qualifier> = SRCIP <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address example = CONNECTION.SRCIP.EQ(127.0.0.1) <qualifier> = DSTIP <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address. example = CONNECTION.DSTIP.EQ(127.0.0.1) <qualifier> = IP <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address. example = CONNECTION.IP.EQ(127.0.0.1) <qualifier> = SRCIPv6 <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv6 address. example = CONNECTION.SRCIPv6.EQ(2001:db8:0:0:1::1) <qualifier> = DSTIPv6 <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv6 address. example = CONNECTION.DSTIPv6.EQ(2001:db8:0:0:1::1) <qualifier> = IPv6 <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv6 address. example =

CONNECTION.IPv6.EQ(2001:db8:0:0:1::1) <qualifier> = SRCPORT <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A valid port number. example = CONNECTION.SRCPORT.EQ(80) <qualifier> = DSTPORT <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A valid port number. example = CONNECTION.DSTPORT.EQ(80) <qualifier> = PORT <qualifier-method> = [EQ | NE] <qualifier-value> = A valid port number. example = CONNECTION.PORT.EQ(80) <qualifier> = SVCNAME <qualifier-method> = [EQ | NE | CONTAINS | STARTSWITH | ENDSWITH] <qualifier-value> = service name. example = CONNECTION.SVCNAME.EQ("name") <qualifier> = LB_VSERVER.NAME <qualifier-method> = [EQ | NE | CONTAINS | STARTSWITH | ENDSWITH] <qualifier-value> = LB vserver name. example = CONNECTION.LB_VSERVER.NAME.EQ("name") <qualifier> = CS_VSERVER.NAME <qualifier-method> = [EQ | NE | CONTAINS | STARTSWITH | ENDSWITH] <qualifier-value> = CS vserver name. example = CONNECTION.CS_VSERVER.NAME.EQ("name") <qualifier> = INTF <qualifier-method> = [EQ | NE] <qualifier-value> = A valid interface id in the form of x/y (n/x/y in case of cluster interface). examle = CONNECTION.INTF.EQ("0/1/1") <qualifier> = VLANID <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A valid VLAN ID. example = CONNECTION.VLANID.EQ(0) <qualifier> = CONNID <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A valid PCB dev number. example = CONNECTION.CONNID.EQ(0) <qualifier> = IDLETIME <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A positive integer indicating the idletime. example = CONNECTION.IDLETIME.LT(100) <qualifier> = TCPSTATE <qualifier-method> = [EQ | NE] <qualifier-value> = (CLOSE_WAIT | CLOSED | CLOSING | ESTABLISHED | FIN_WAIT_1 | FIN_WAIT_2 | LAST_ACK | LISTEN | SYN_RECEIVED | SYN_SENT | TIME_WAIT | NOT_APPLICABLE) example = CONNECTION.TCPSTATE.EQ(LISTEN) <qualifier> = SERVICE_TYPE <qualifier-method> = [EQ | NE] <qualifier-value> = (SVC_HTTP | FTP | TCP | UDP | SSL | SSL_BRIDGE | SSL_TCP | NNTP | RPCSVR | RPCSVRS | RPCCLNT | SVC_DNS | ADNS | SNMP | RTSP | DHCPRA | ANY| MONITOR | MONITOR_UDP | MONITOR_PING | SIP_UDP | SVC_MYSQL | SVC_MSSQL | SERVICE_UNKNOWN) example = CONNECTION.SERVICE_TYPE.EQ(ANY) common usecases: Filtering out loopback connections and view present connections through netsclaer show connectiontable "CONNECTION.IP.NEQ(127.0.0.1) && CONNECTION.TCPSTATE.EQ(ESTABLISHED)" -detail full show connections from a particular sourceip and targeted to port 80 show connectiontable "CONNECTION.SRCIP.EQ(10.102.1.91) && CONNECTION.DSTPORT.EQ(80)" show connection particular to a service and its linked client connections show connectiontable "CONNECTION.SVCNAME.EQ("S1")" -detail link show connections for a particular servicetype(e.g.http) show connectiontable "CONNECTION.SERVICE_TYPE.EQ(TCP)" viewing connections that have been idle for a long time show connectiontable "CONNECTION.IDLETIME.GT(100)" show connections for a particular interface and vlan show connectiontable "CONNECTION.INTF.EQ("1/1") && CONNECTION.VLANID.EQ(1)"

link

Display link information if available

name

Display name instead of IP for local entities

detail

Display options for the connection table.

ns limitSessions

[show | clear]

show ns limitSessions

Synopsis

show ns limitSessions <limitIdentifier> [-detail]

Description

Display rate limit sessions.

Parameters

limitIdentifier

The name of the rate limit identifer.

detail

Displays the individual hash values

Top

clear ns limitSessions

Synopsis

clear ns limitSessions <limitIdentifier>

Parameters

limitIdentifier

The name of the rate limit identifer.

Top

ns hostName

[set | show]

set ns hostName

Synopsis

set ns hostName <hostName> [-ownerNode <positive_integer>]

Description

Sets the host name for the system.

Parameters

hostName

Desired host name.

ownerNode

The owner node in a Cluster for which we are setting the hostname. Owner node can vary from 0 to 31. Default value: 255 Maximum value: 31

Example

set ns hostname nspri

Top

show ns hostName

Synopsis

show ns hostName

Description

Display the host name of the system.

Example

show ns hostname

Top

ns surgeQ

flush ns surgeQ

Synopsis

flush ns surgeQ [-name <string> [-serverName <string> <port>]]

Description

Use this command to flush the connections that are waiting in SurgeQ.

Parameters

name

The name of the entity.Entity can be a Vserver, Service or a Servicegroup.

serverName

Name of the Server bound to the entity(Servicegroup).

Example

To flush the surgeQ system wide, use the command: flush ns SurgeQ.
To flush the surgeQ specific to a vserver/service/svcgrp use the command: flush ns SurgeQ -name <name>
To flush the surgeQ specific to a svcgrp member, use the command: flush ns surgeQ [-name <string> [-serve

ns feature

[enable | disable | show]

enable ns feature

Synopsis

enable ns feature <feature> ...

Description

Enable a specific feature.

Parameters

feature

Name of the feature(s)

Example

enable ns feature sc
This CLI command enables the SureConnect feature.

Top

disable ns feature

Synopsis

disable ns feature <feature> ...

Description

Disable a specified feature or features.

Parameters

feature

Name of the feature(s)

Top

show ns feature

Synopsis

show ns feature

Description

Display the current status of System features.

Top

ns mode

[enable | disable | show]

enable ns mode

Synopsis

enable ns mode <Mode> ...

Description

Enable a specified mode.

Parameters

Mode

The name of the mode to be enabled.

Example

This CLI command enables the system's client keep-alive feature:
enable ns mode CKA

Top

disable ns mode

Synopsis

disable ns mode <Mode> ...

Description

Disable the specified feature or features.

Parameters

Mode

The feature to be disabled.

Example

This example shows the command to disable the system's client keep-alive feature:
disable ns mode CKA

Top

show ns mode

Synopsis

show ns mode

Description

Display the state of Fast Ramp, Layer 2, USIP, client keep-alive, TCP buffering, and MAC-based forwarding features.

Top

ns dhcpParams

[set | unset | show]

set ns dhcpParams

Synopsis

set ns dhcpParams [-dhcpClient (ON | OFF)] [-saveroute (ON | OFF)]

Description

Set the dhcp-client parameters.

Parameters

dhcpClient

Setting this argument to ON makes the netscaler to enable dhcp-client for acquiring IP from the DHCP server in the next boot. Setting it to OFF disables the dhcp-client in the next boot. Possible values: ON, OFF Default value: OFF

saveroute

If this flag is set, then DHCP acquired routes are saved during saveconfig. Possible values: ON, OFF Default value: OFF

Top

unset ns dhcpParams

Synopsis

unset ns dhcpParams [-dhcpClient] [-saveroute]

Description

Use this command to remove ns dhcpParams settings.Refer to the set ns dhcpParams command for meanings of the arguments.

Top

show ns dhcpParams

Synopsis

show ns dhcpParams

Description

Show dhcp-client parameters.

Top

ns dhcpIp

release ns dhcpIp

Synopsis

release ns dhcpIp

Description

Release IP acquired by DHCP client

ns spParams

[set | unset | show]

set ns spParams

Synopsis

set ns spParams [-baseThreshold <integer>] [-throttle <throttle>]

Description

Set the base threshold and/or the throttle rate for surge protection.

Parameters

baseThreshold

The base threshold. This is the maximum number of server connections that can be opened before surge protection is activated. Default value: 200 Maximum value: 32767

throttle

The throttle rate, which is the rate at which the system opens connections to the server. The different names of throttle are the keywords: relaxed, normal, and aggressive. Possible values: Aggressive, Normal, Relaxed Default value: NORM_SP_TABLE

Example

set ns spparams -baseThreshold 1000 -throttle aggressive
set ns spparams -throttle relaxed

Top

unset ns spParams

Synopsis

unset ns spParams [-baseThreshold] [-throttle]

Description

Use this command to remove ns spParams settings.Refer to the set ns spParams command for meanings of the arguments.

Top

show ns spParams

Synopsis

show ns spParams

Description

Display the surge protection configuration on the system. This includes the base threshold value and throttle value. These values are set using the setnsparams command.

Example

```
> show ns spparams
      Surge Protection parameters:
      BaseThreshold:  200
      Throttle:  Normal
 Done
```

Top

ns tcpbufParam

[set | unset | show]

set ns tcpbufParam

Synopsis

set ns tcpbufParam [-size <KBytes>] [-memLimit <MBytes>]

Description

Display the current TCP buffer size. The command also displays the percentage of the system memory that is used for buffering.

Parameters

size

The size (in KBytes) of the TCP buffer per connection. Default value: 64 Minimum value: 4 Maximum value: 20480

memLimit

The maximum memory that can be used for buffering, in megabytes. Default value: 64

Top

unset ns tcpbufParam

Synopsis

unset ns tcpbufParam [-size] [-memLimit]

Description

Use this command to remove ns tcpbufParam settings.Refer to the set ns tcpbufParam command for meanings of the arguments.

Top

show ns tcpbufParam

Synopsis

show ns tcpbufParam

Description

Display the current TCP buffer size. The command also displays the percentage of the system memory that is used for buffering.

Example

An example of this command's output is as follows:
TCP buffer size: 64KBytes
TCP buffer percentage: 50%

Top

ns tcpParam

[set | unset | show]

set ns tcpParam

Synopsis

set ns tcpParam [-WS (ENABLED | DISABLED)] [-WSVal <positive_integer>] [-SACK (ENABLED | DISABLED)] [-learnVsvrMSS (ENABLED | DISABLED)] [-maxBurst <positive_integer>] [-initialCwnd <positive_integer>] [-delayedAck <positive_integer>] [-downStateRST (ENABLED | DISABLED)] [-nagle (ENABLED | DISABLED)] [-limitedPersist (ENABLED | DISABLED)] [-oooQSize <positive_integer>] [-ackOnPush (ENABLED | DISABLED)] [-maxPktPerMss <integer>] [-pktPerRetx <integer>] [-minRTO <integer>] [-slowStartIncr <integer>] [-maxDynServerProbes <positive_integer>] [-synHoldFastGiveup <positive_integer>] [-maxSynholdPerprobe <positive_integer>] [-maxSynhold <positive_integer>] [-mssLearnInterval <positive_integer>] [-mssLearnDelay <positive_integer>] [-maxTimeWaitConn <positive_integer>] [-maxSynAckRetx <positive_integer>] [-synAttackDetection (ENABLED | DISABLED)] [-connFlushIfNoMem <connFlushIfNoMem>] [-connFlushThres <positive_integer>]

Description

Set the TCP settings on the NetScaler

Parameters

WS

The state of WS Possible values: ENABLED, DISABLED Default value: DISABLED

WSVal

Window Scaling Factor used Default value: 4 Maximum value: 8

SACK

The state of SACK Possible values: ENABLED, DISABLED Default value: DISABLED

learnVsvrMSS

enable/disable MSS learning for vservers Possible values: ENABLED, DISABLED Default value: DISABLED

maxBurst

Max-Burst Factor used Default value: 6 Minimum value: 1 Maximum value: 255

initialCwnd

Intial value of TCP cwnd used Default value: 4 Minimum value: 1 Maximum value: 44

recvBuffSize

TCP Receive buffer size Default value: 8190 Minimum value: 8190 Maximum value: 20971520

delayedAck

Delayed acknowledgement timeout (in millisec) Default value: 100 Minimum value: 10 Maximum value: 300

downStateRST

Flag to switch on RST on down services Possible values: ENABLED, DISABLED Default value: DISABLED

nagle

Whether to enable Nagle's algorithm on connections Possible values: ENABLED, DISABLED Default value: DISABLED

limitedPersist

Whether to limit the number of persist(zero window) probes Possible values: ENABLED, DISABLED Default value: ENABLED

oooQSize

Maximum size of out-of-order packet queue (0 means infinite) Default value: 64 Maximum value: 65535

ackOnPush

Enable immediate ACK on receiving packet with PUSH flag Possible values: ENABLED, DISABLED Default value: ENABLED

maxPktPerMss

Set maximum packtes to be sent for each MSS in CWND for packet count based congestion control Maximum value: 1460

pktPerRetx

Set maximum packets should be retransmitted on partial ACK case Default value: 1 Minimum value: 1 Maximum value: 100

minRTO

Minimum TCP RTO(in millisec) Default value: 1000 Minimum value: 10 Maximum value: 64000

slowStartIncr

Set TCP slow start increment factor Default value: 2 Minimum value: 1 Maximum value: 100

maxDynServerProbes

Max server probes in 10ms Default value: 7 Minimum value: 1 Maximum value: 65535

synHoldFastGiveup

Max threshold after which NetScaler reduces the number of retries for server probes Default value: 1024 Minimum value: 256 Maximum value: 65535

maxSynholdPerprobe

Maximum number of SYN allowed to be queued per probe PCB Default value: 128 Minimum value: 1 Maximum value: 255

maxSynhold

Maximum number of SYN that NetScaler can hold while probing for backend services Default value: 16384 Minimum value: 256 Maximum value: 65535

mssLearnInterval

Time period (in seconds) for which the backend service MSS are sampled for Vserver MSS learning Default value: 180 Minimum value: 1 Maximum value: 1048576

mssLearnDelay

Vserver MSS learning delay(seconds) Default value: 3600 Minimum value: 1 Maximum value: 1048576

maxTimeWaitConn

max connection limit for FIN TIME WAIT Default value: 7000 Minimum value: 1

KAprobeUpdateLastactivity

Update last activity for KA probes Possible values: ENABLED, DISABLED Default value: ENABLED

maxSynAckRetx

Max limit for syn+ack retransmissions in a given interval Default value: 100 Minimum value: 100 Maximum value: 1048576

synAttackDetection

Enable/disable synattack detection Possible values: ENABLED, DISABLED Default value: ENABLED

connFlushIfNoMem

Flush an existing connection if no memory can be obtained for new connection. HALF_CLOSED_AND_IDLE: Flush a connection that is closed by us but not by peer, or failing that, a connection that is past configured idle time. New connection fails if no

such connection can be found. FIFO: If no half-closed or idle connection can be found, flush the oldest non-management connection, even if it is active. New connection fails if the oldest few connections are management connections. Note: If you enable this setting, you should also consider lowering the zombie timeout and half-close timeout (see NSCLI command: set ns timeout). See Also: connFlushThres argument below. Possible values: NONE, HALFCLOSED_AND_IDLE, FIFO Default value: NSA_CONNFLUSH_NONE

connFlushThres

Flush an existing connection (as configured through -connFlushIfNoMem FIFO) if the system has more than specified number of connections, and a new connection is to be established. Note: This value may be rounded down to be a whole multiple of the number of packet engines running. Minimum value: 1

Top

unset ns tcpParam

Synopsis

unset ns tcpParam [-WS] [-WSVal] [-SACK] [-learnVsvrMSS] [-maxBurst] [-initialCwnd] [-delayedAck] [-downStateRST] [-nagle] [-limitedPersist] [-oooQSize] [-ackOnPush] [-maxPktPerMss] [-pktPerRetx] [-minRTO] [-slowStartIncr] [-maxDynServerProbes] [-synHoldFastGiveup] [-maxSynholdPerprobe] [-maxSynhold] [-mssLearnInterval] [-mssLearnDelay] [-maxTimeWaitConn] [-maxSynAckRetx] [-synAttackDetection] [-connFlushIfNoMem] [-connFlushThres]

Description

Use this command to remove ns tcpParam settings.Refer to the set ns tcpParam command for meanings of the arguments.

Top

show ns tcpParam

Synopsis

show ns tcpParam

Description

Display the TCP settings on the NetScaler

Top

ns httpParam

[set | unset | show]

set ns httpParam

Synopsis

set ns httpParam [-dropInvalReqs (ON | OFF)] [-markHttp09Inval (ON | OFF)] [-markConnReqInval (ON | OFF)] [-insNsSrvrHdr (ON | OFF) [<nsSrvrHdr>]] [-logErrResp (ON | OFF)] [-conMultiplex (ENABLED | DISABLED)] [-maxReusePool <positive_integer>]

Description

Set configurable HTTP parameters on the NetScaler

Parameters

dropInvalReqs

Whether to drop invalid HTTP requests/responses Possible values: ON, OFF Default value: OFF

markHttp09Inval

Whether to mark HTTP/0.9 requests as invalid Possible values: ON, OFF Default value: OFF

markConnReqInval

Whether to mark CONNECT requests as invalid Possible values: ON, OFF Default value: OFF

insNsSrvrHdr

Enable/disable NetScaler server header insertion for NetScaler generated HTTP responses. Possible values: ON, OFF Default value: OFF

logErrResp

Whether to log HTTP error responses generated by NetScaler Possible values: ON, OFF Default value: ON

conMultiplex

Connection multiplexing Possible values: ENABLED, DISABLED Default value: ENABLED

maxReusePool

Maximum connections in reusepool

Example

set ns httpParam -dropInvalReqs ON

Top

unset ns httpParam

Synopsis

unset ns httpParam [-dropInvalReqs] [-markHttp09Inval] [-markConnReqInval] [-insNsSrvrHdr] [-nsSrvrHdr] [-logErrResp] [-conMultiplex] [-maxReusePool]

Description

Use this command to remove ns httpParam settings.Refer to the set ns httpParam command for meanings of the arguments.

Top

show ns httpParam

Synopsis

show ns httpParam

Description

Display configured HTTP parameters on the NetScaler

Top

ns weblogparam

[set | show]

set ns weblogparam

Synopsis

set ns weblogparam -bufferSizeMB <positive_integer>

Description

Set the current web log buffer size.

Parameters

bufferSizeMB

The buffer size (in MB) allocated for log transaction data on the system. Maximum value is limited by the memory available in the system. Minimum value: 1 Maximum value: 4294967294LU

Top

show ns weblogparam

Synopsis

show ns weblogparam

Description

Display the current size of the buffer, which is used to store log transactions.

Top

ns diameter

[set | unset | show]

set ns diameter

Synopsis

set ns diameter [-identity <string>] [-realm <string>] [-serverClosePropagation (YES | NO)]

Description

Set the diameter configuration on NS.

Parameters

identity

DiameterIdentity to be used by NS. DiameterIdentity is used to identify a Diameter node uniquely. Before setting up diameter configuration, Netscaler (as a Diameter node) MUST be assigned a unique DiameterIdentity. example => set ns diameter -identity netscaler.com Now whenever Netscaler system needs to use identity in diameter messages. It will use 'netscaler.com' as Origin-Host AVP as defined in RFC3588

realm

Diameter Realm to be used by NS. example => set ns diameter -realm com Now whenever Netscaler system needs to use realm in diameter messages. It will use 'com' as Origin-Realm AVP as defined in RFC3588

serverClosePropagation

when a Server connection goes down, whether to close the corresponding client connection if there were requests pending on the server. Possible values: YES, NO Default value: NO

Top

unset ns diameter

Synopsis

unset ns diameter -serverClosePropagation

Description

Use this command to remove ns diameter settings.Refer to the set ns diameter command for meanings of the arguments.

Top

show ns diameter

Synopsis

show ns diameter

Description

Display the diameter configuration on NS.

Top

ns rateControl

[set | unset | show]

set ns rateControl

Synopsis

set ns rateControl [-tcpThreshold <positive_integer>] [-udpThreshold <positive_integer>] [-icmpThreshold <positive_integer>]

Description

Configure udp/tcp/icmp packet rate controls for any application that is not configured at System(ie., direct access to the backend through System). This rate limit should be specified in the number of packets to allow per 10ms.

Parameters

tcpThreshold

The number of SYNs permitted per 10 milli second.

udpThreshold

The number of UDP packets permitted per 10 milli second.

icmpThreshold

The number of ICMP packets permitted per 10 milli second. Default value: 100

Example

The following command will set the SYN rate to 100, icmp rate to 10 and the udp rate to unlimited.

set ns ratecontrol -tcpThreshold 100 -udpThreshold 0 -icmpThreshold 10

The 'show ns rate control' command can be used to view the current settings of the rate controls.

```
> show ns ratecontrol
      UDP threshold:        0 per 10 ms
      TCP threshold:        0 per 10 ms
      ICMP threshold:       100 per 10 ms
 Done
```

Top

unset ns rateControl

Synopsis

unset ns rateControl [-tcpThreshold] [-udpThreshold] [-icmpThreshold]

Description

Use this command to remove ns rateControl settings.Refer to the set ns rateControl command for meanings of the arguments.

Top

show ns rateControl

Synopsis

show ns rateControl

Description

Check the current rate control values.

Example

By default, there is no rate control for TCP/UDP and for ICMP it will be 100. The output of the "show ns rate

```
> show ns ratecontrol
      UDP threshold:        0 per 10 ms
      TCP threshold:        0 per 10 ms
      ICMP threshold:       100 per 10 ms
 Done
```

Top

ns rpcNode

[set | unset | show]

set ns rpcNode

Synopsis

set ns rpcNode <IPAddress> {-password } [-srcIP <ip_addr|ipv6_addr|*>] [-secure (YES | NO)]

Description

Set the authentication attributes associated with peer System node. All System nodes use remote procedure calls to communicate.

Parameters

IPAddress

The IP address of the node. This has to be in same subnet as NSIP.

password

The password to be used in authentication with the peer System node.

srcIP

The src ip to be used in communiction with the peer System node.

secure

The state of the channel when talking to the node. Channel can be secure or insecure.
Possible values: YES, NO

Example

Example-1: Failover configuration
In a failover configuration define peer NS as:
add node 1 10.101.4.87
Set peer ha-unit's password as:
set ns rpcnode 10.101.4.87 -password testpass -secure yes

System will now use the configured password to authenticate with its failover unit.

Example-2: GSLB configuration

In a GSLB configuration define peer NS GSLB site as:
add gslb site us_east_coast remote 206.123.3.4
Set peer GSLB-NS's password as:
set ns rpcnode 206.123.3.4 -password testrun

System will now use the configured password to authenticate with east-coast GSLB site.

Top

unset ns rpcNode

Synopsis

unset ns rpcNode <IPAddress> [-password] [-srcIP] [-secure]

Description

Use this command to remove ns rpcNode settings.Refer to the set ns rpcNode command for meanings of the arguments.

Top

show ns rpcNode

Synopsis

show ns rpcNode [<IPAddress>]

Description

Display a list of nodes currently communicating using RPC. All nodes use remote procedure calls to communicate.

Parameters

IPAddress

The IP address of the node. This has to be in same subnet as NSIP.

Example

Following example shows list of nodes communicating using RPC:

```
> sh rpcnode
1)      IPAddress:  10.101.4.84 Password:  ..8a7b474124957776b56cf03b28 Srcip: 1.1.1.1
2)      IPAddress:  10.101.4.87 Password:  ..ca2a035465d22c            Srcip: 2.2.2.2
 Done
```

Top

ns timeout

[set | unset | show]

set ns timeout

Synopsis

set ns timeout [-zombie <positive_integer>] [-httpClient <positive_integer>] [-httpServer <positive_integer>] [-tcpClient <positive_integer>] [-tcpServer <positive_integer>] [-anyClient <positive_integer>] [-anyServer <positive_integer>] [-halfclose <positive_integer>] [-nontcpZombie <positive_integer>] [-ReducedFinTimeOut <positive_integer>] [-NewConnIdleTimeOut <positive_integer>]

Description

Set various timeout values for NetScaler device. Caution: Modifying these values may affect system performance.

Parameters

zombie

Timer interval(in seconds) for zombie process that cleanup inactive TCP connections Default value: 120 Minimum value: 1 Maximum value: 600

client

Client idle timeout (in seconds). If zero, the service-type default value is taken when service is created. Maximum value: 18000

server

Server idle timeout (in seconds). If zero, the service-type default is taken when service is created. Maximum value: 18000

httpClient

HTTP client idle timeout (in seconds) Maximum value: 18000

httpServer

HTTP server idle timeout (in seconds) Maximum value: 18000

tcpClient

TCP client idle timeout (in seconds) Maximum value: 18000

tcpServer

TCP server idle timeout (in seconds) Maximum value: 18000

anyClient

ANY client idle timeout (in seconds) Maximum value: 31536000

anyServer

ANY server idle timeout (in seconds) Maximum value: 31536000

halfclose

Half-closed connection timeout (in seconds) Default value: 10 Minimum value: 1 Maximum value: 600

nontcpZombie

Timer interval(in seconds) for zombie process that cleanup inactive IP NAT connections Default value: 60 Minimum value: 1 Maximum value: 600

ReducedFinTimeOut

Timer interval(in seconds) for NATPCB for tcp flow Default value: 30 Minimum value: 1 Maximum value: 300

NewConnIdleTimeOut

Timer interval(in seconds) for new NATPCB for tcp connections. Default value: 4 Minimum value: 1 Maximum value: 20

Example

set ns timeout -zombie 200

Top

unset ns timeout

Synopsis

unset ns timeout [-zombie] [-httpClient] [-httpServer] [-tcpClient] [-tcpServer] [-anyClient] [-anyServer] [-halfclose] [-nontcpZombie] [-ReducedFinTimeOut] [-NewConnIdleTimeOut]

Description

Use this command to remove ns timeout settings.Refer to the set ns timeout command for meanings of the arguments.

Top

show ns timeout

Synopsis

show ns timeout

Description

Display various timeout values for NetScaler device. The timeouts having default values are not displayed.

Example

show ns timeout

Top

ns hardware

show ns hardware

Synopsis

show ns hardware

Description

Displays hardware and product related information like SystemId, HostId, SerialId.

ns events

show ns events

Synopsis

show ns events [<eventNo>]

Description

display the events

Parameters

eventNo

Last retrieved event no. This command will return all events after that.

Example

show ns events

ns encryptionParams

[set | show]

set ns encryptionParams

Synopsis

set ns encryptionParams -method <method> [-keyValue]

Description

Set parameters for content encryption and decryption.

Parameters

method

The cipher method (and key length) used to encrypt and decrypt content. The default method is AES256. Possible values: NONE, RC4, DES3, AES128, AES192, AES256

keyValue

The base64-encoded key generation number, method, and key value. The parameter should be omitted when the encryption method is being changed, but can be specified with an empty string argument ("") for the generation of a new key value for the current encryption method. The parameter is passed implicitly, with its automatically generated value, to the NetScaler Packet Engines even when it is not specified in the command. This enables the appliance to save the key value to the configuration file and to enable propagation of the key value to the secondary appliance in an HA pair.

Example

set ns encryptionParams -method aes128

Top

show ns encryptionParams

Synopsis

show ns encryptionParams

Description

Display the parameters in effect for content encryption.

Top

ns rollbackcmd

show ns rollbackcmd

Synopsis

show ns rollbackcmd [-fileName <input_filename>] [-outtype (cli | xml)]

Description

Rollback commands for the ones specified in input file

Parameters

fileName

Input file for generating rollback commands

outtype

The format in which result is desired. Possible values: cli, xml

Example

show ns rollbackcmd -file <file_name>

ns memory

stat ns memory

Synopsis

stat ns memory [<pool>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display NetScaler feature memory statistics

Parameters

pool

Feature name

ns pbr6

[add | renumber | rm | set | unset | enable | disable | stat | show | clear | apply]

add ns pbr6

Synopsis

add ns pbr6 <name> <action> [-srcIPv6 [<operator>] <srcIPv6Val>] [-srcPort [<operator>] <srcPortVal>] [-destIPv6 [<operator>] <destIPv6Val>] [-destPort [<operator>] <destPortVal>] [-srcMac <mac_addr>] [-protocol <protocol> | -protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-state <state>] [-msr (ENABLED | DISABLED) [-monitor <string>]] [-nextHop <nextHopVal>] [-nextHopVlan <positive_integer>]

Description

Add an IPv6 PBR to the System configuration. Each inbound IPv6 packet is matched against configured PBRs and routed accordingly. This command adds the IPv6 PBR to the configuration space. To commit this PBR, one should apply the PBR6.

Parameters

name

Alphanumeric name of the PBR6.

action

Action associated with the PBR6. Possible values: ALLOW, DENY

srcIPv6

Source IPv6 address (range).

srcPort

Source port (range).

destIPv6

Destination IPv6 address (range).

destPort

Destination port (range).

srcMac

Source MAC address.

protocol

IPv6 protocol name. Possible values: ICMPV6, TCP, UDP

protocolNumber

IPv6 protocol number (decimal). Minimum value: 1 Maximum value: 255

vlan

VLAN number. Minimum value: 1 Maximum value: 4094

interface

Physical interface name.

priority

Priority of the PBR6. (Sequence of execution) Minimum value: 1 Maximum value: 80000

state

State of the PBR6. Possible values: ENABLED, DISABLED, REMOVED Default value: XACLENABLED

msr

Enable/disable Monitored Static Route(MSR) on this route. Possible values: ENABLED, DISABLED Default value: DISABLED

nextHop

The Next Hop IPv6 address.

nextHopVlan

VLAN number to be used for link local nexthop . Minimum value: 1 Maximum value: 4094

Example

add ns pbr6 rule1 ALLOW -srcport 45-1024 -destIPv6 2001::45 -nexthop 2001::49

Top

renumber ns pbr6

Synopsis

renumber ns pbr6

Description

Reorganize PBR6 priorities. This will introduce gaps between PBR6 priorities. This command does not affect the behaviour of PBRs.

Example

renumber pbr6

Top

rm ns pbr6

Synopsis

rm ns pbr6 <name> ...

Description

Remove a PBR6 configuration. To commit this operation, one should apply the PBR6.

Parameters

name

Name of the PBR6 to be deleted.

Example

rm ns pbr6 rule1

Top

set ns pbr6

Synopsis

set ns pbr6 <name> [-action (ALLOW | DENY)] [-srcIPv6 [<operator>] <srcIPv6Val>] [-srcPort [<operator>] <srcPortVal>] [-destIPv6 [<operator>] <destIPv6Val>] [-destPort [<operator>] <destPortVal>] [-srcMac <mac_addr>] [-protocol <protocol> | -protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-msr (ENABLED | DISABLED) [-monitor <string>]] [-nextHop <nextHopVal>] [-nextHopVlan <positive_integer>]

Description

Modify a PBR6. To commit this modified PBR6, use 'apply pbr6' command.

Parameters

name

Alphanumeric name of the PBR6.

action

Action associated with the PBR6. Possible values: ALLOW, DENY

srcIPv6

Source IPv6 address (range).

srcPort

Source Port (range).

destIPv6

Destination IPv6 address (range).

destPort

Destination Port (range).

srcMac

Source MAC address.

protocol

IPv6 protocol name. Possible values: ICMPV6, TCP, UDP

protocolNumber

IPv6 protocol number (decimal). Minimum value: 1 Maximum value: 255

vlan

VLAN number. Minimum value: 1 Maximum value: 4094

interface

Physical interface name.

priority

Priority of the PBR6. (Sequence of execution) Minimum value: 1 Maximum value: 80000

msr

Enable/disable Monitored Static Route(MSR) on this route. Possible values: ENABLED, DISABLED Default value: DISABLED

nextHop

The Next Hop IPv6 address.

nextHopVlan

VLAN number to be used for link local nexthop . Minimum value: 1 Maximum value: 4094

Example

set ns pbr6 rule1 -srcPort 50

Top

unset ns pbr6

Synopsis

unset ns pbr6 <name> [-srcIPv6] [-srcPort] [-destIPv6] [-destPort] [-srcMac] [-protocol] [-interface] [-vlan] [-msr] [-monitor] [-nextHop] [-nextHopVlan]

Description

Modify PBR6 configuration. To commit this modified PBR6, use 'apply pbr6' command..Refer to the set ns pbr6 command for meanings of the arguments.

Example

unset ns pbr6 rule1 -srcPort

Top

enable ns pbr6

Synopsis

enable ns pbr6 <name> ...

Description

Enable an PBR6. To commit this operation, one should apply the PBR6.

Parameters

name

Name of the PBR6 to be enabled.

Example

enable ns pbr6 rule1

Top

disable ns pbr6

Synopsis

disable ns pbr6 <name> ...

Description

Disable an PBR6. To commit this operation, one should apply the PBR6.

Parameters

name

Name of the PBR6 to be disabled.

Example

disable ns pbr6 rule1

Top

stat ns pbr6

Synopsis

stat ns pbr6 [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display PBR6 statistics.

Parameters

name

PBR6 Name.

Example

stat pbr6

Top

show ns pbr6

Synopsis

show ns pbr6 [<name>] [-detail]

Description

Display the PBR6. If name is specified, then only that particular PBR6 information is displayed. If it is not specified, all configured PBR6 are displayed.

Parameters

name

Name of the PBR6.

detail

To get a detailed view.

Example

```
show ns pbr6 rule1
1)     Name: r1                    Action: DENY
       srcIPv6 = 2001::1
       destIPv6
       srcMac:                    Protocol:
       Vlan:                     Interface:
       Active Status: ENABLED          Applied Status: NOTAPPLIED
       Priority: 10               Hits: 0
       Nexthop:
```

Top

clear ns pbr6

Synopsis

clear ns pbr6

Description

Clear all configured PBR6 rules. This operation does not require an explicit apply.

Example

```
clear ns pbr6
```

Top

apply ns pbr6

Synopsis

apply ns pbr6

Description

Commit the PBR6 in the configuration space to the system. This is required after an PBR6 is added or modified.

Example

```
apply ns pbr6
```

Top

NTP Commands

This group of commands can be used to perform operations on the following entities:

- ntp server
- ntp sync
- ntp status
- ntp param

ntp server

[add | rm | set | unset | show]

add ntp server

Synopsis

add ntp server (<serverIP> | <serverName>) [-minpoll <positive_integer>] [-maxpoll <positive_integer>] [-autokey | -key <positive_integer>]

Description

Add NTP server

Parameters

serverIP

IP address of the NTP server.

serverName

Fully qualified domain name of the NTP server.

minpoll

Specifies the minimum poll intervals for NTP messages, in seconds to the power of two. Value defaults to 6 (64 s), but can be decreased to a lower limit of 4 (16 s). Default value: NS_NTP_MINPOLL_DEFAULT_VALUE Minimum value: 4 Maximum value: 17

maxpoll

Specifies the maximum poll intervals for NTP messages, in seconds to the power of two. Value defaults to 10 (1,024 s), but can be increased to an upper limit of 17 (36.4 h). Default value: NS_NTP_MAXPOLL_DEFAULT_VALUE Minimum value: 4 Maximum value: 17

autokey

Specifies if autokey is to be used for the specified server

key

Specifies the key to be used for the specified server Minimum value: 1 Maximum value: 65534

Top

rm ntp server

Synopsis

rm ntp server (<serverIP> | <serverName>)

Description

Remove NTP server entry

Parameters

serverIP

IP address of the NTP server.

serverName

Fully qualified domain name of the NTP server.

Top

set ntp server

Synopsis

set ntp server (<serverIP> | <serverName>) [-minpoll <positive_integer>] [-maxpoll <positive_integer>] [-preferredNtpServer (YES | NO)] [-autokey | -key <positive_integer>]

Description

Modify the NTP server entries.

Parameters

serverIP

IP address of the NTP server.

serverName

Fully qualified domain name of the NTP server.

minpoll

Specifies the minimum poll intervals for NTP messages, in seconds to the power of two. Value defaults to 6 (64 s), but can be decreased to a lower limit of 4 (16 s) Default value: NS_NTP_MINPOLL_DEFAULT_VALUE Minimum value: 4 Maximum value: 17

maxpoll

Specifies the maximum poll intervals for NTP messages, in seconds to the power of two. Value defaults to 10 (1,024 s), but can be increased to an upper limit of 17 (36.4 h). Default value: NS_NTP_MAXPOLL_DEFAULT_VALUE Minimum value: 4 Maximum value: 17

preferredNtpServer

Specifies if the server is preferred one Possible values: YES, NO Default value: NO

autokey

Specifies if autokey is to be used for the specified server

key

Specifies the key to be used for the specified server Minimum value: 1 Maximum value: 65534

Top

unset ntp server

Synopsis

unset ntp server [<serverIP>] [<serverName>] [-minpoll] [-maxpoll] [-preferredNtpServer] [-autokey] [-key]

Description

Use this command to remove ntp server settings.Refer to the set ntp server command for meanings of the arguments.

Top

show ntp server

Synopsis

show ntp server [<serverIP> | <serverName>]

Description

Show NTP server information.

Parameters

serverIP

IP address of the NTP server.

serverName

Fully qualified domain name of the NTP server.

Top

ntp sync

[enable | disable | show]

enable ntp sync

Synopsis

enable ntp sync

Description

Enable NTP synchronization

Top

disable ntp sync

Synopsis

disable ntp sync

Description

Disable NTP synchronization

Top

show ntp sync

Synopsis

show ntp sync

Description

Show NTP sync info

Top

ntp status

show ntp status

Synopsis

show ntp status

Description

Show NTP Status

ntp param

[set | unset | show]

set ntp param

Synopsis

set ntp param [-authentication (YES | NO)] [-trustedkey <positive_integer> ...] [-autokeyLogsec <positive_integer>] [-revokeLogsec <positive_integer>]

Description

Set values for NTP parameters

Parameters

authentication

Specifies if NTP AUTH is enabled or not. Default is YES. Possible values: YES, NO Default value: YES

trustedkey

Specifies the trusted keys entered. Minimum value: 1 Maximum value: 65534

autokeyLogsec

Specifies the interval between regenerations of the session key list used with the Autokey protocol, as a power of 2 in seconds. Default value: 12 Maximum value: 32

revokeLogsec

Specifies the interval between re-randomization of certain cryptographic values used by the Autokey scheme, as a power of 2 in seconds. Default value: 16 Maximum value: 32

Top

unset ntp param

Synopsis

unset ntp param [-authentication] [-trustedkey] [-autokeyLogsec] [-revokeLogsec]

Description

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

Top

show ntp param

Synopsis

show ntp param

Description

Get values for NTP parameters

Top

Policy Commands

This group of commands can be used to perform operations on the following entities:

- policy expression
- policy map
- policy patset
- policy dataset
- policy httpCallout
- policy stringmap

policy expression

[add | rm | set | unset | show]

add policy expression

Synopsis

add policy expression <name> <value> [-comment <string>] [-clientSecurityMessage <string>]

Description

Create an expression.

Parameters

name

The name of the expression that will be created.

value

The expression string.

description

Description for the expression.

comment

Comments associated with this expression.

clientSecurityMessage

The client security message that will be displayed on failure of this expression.Only relevant for end point check expressions.

Top

rm policy expression

Synopsis

rm policy expression <name> ...

Description

Remove a previously defined expression. If the expression is part of a policy or filter, you must remove the policy or filter before removing the expression.

Parameters

name

The name of the expression.

Top

set policy expression

Synopsis

set policy expression <name> [<value>] [-comment <string>] [-clientSecurityMessage <string>]

Description

This command modifies an existing expression.

Parameters

name

The name of the expression.

value

The expression string.

description

Description for the expression.

comment

Comments associated with this expression.

clientSecurityMessage

The client security message that will be displayed on failure of this expression. Only relevant for end point check expressions.

Top

unset policy expression

Synopsis

unset policy expression <name> [-comment] [-clientSecurityMessage]

Description

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

Top

show policy expression

Synopsis

show policy expression [<name> | -type (CLASSIC | ADVANCED)]

Description

Display the expressions defined in the system.

Parameters

name

The name of the expression. if no name is given then all expressions will be displayed.

type

The type of expression. This is for input only. Possible values: CLASSIC, ADVANCED

Top

policy map

[add | rm | show]

add policy map

Synopsis

add policy map <mapPolicyName> -sd <string> [-su <string>] [-td <string>] [-tu <string>]

Description

Create a policy to map publicly-known domain name to a target domain name for a reverse proxy virtual server used in the cache redirection feature. Optionally, a source and target URL can also be specified. The map policy created can be associated with a reverse proxy cache redirection virtual server using the ###bind cr vserver### command. There can be only one default map policy for a domain.

Parameters

mapPolicyName

The name of the map policy to be created.

sd

The source domain name which is publicly known. This is the domain name with which a client request arrives to a reverse proxy virtual server for cache redirection on the system.

su

The source URL. The format to specify the argument is: / [[prefix] [*]] [.suffix]

td

The domain name sent to the server. It replaces the source domain name.

tu

The target URL.The format to specify the argument is: / [[prefix] [*]] [.suffix]

Example

Example 1
The following example creates a default map policy (map1) for the source domain www.a.com. Any client re

add policy map map2 -sd www.a.com -td www.real.a.com
Example 2
This example shows how to create a URL map policy (map2) if you want to translate /sports.html in the inco
add policy map map2 -sd www.a.com
-td www.real_a.com -su /sports.html
-tu /news.html
These type of map policies, called "URL map policies," have the following restrictions:
- URL map policies belonging to www.a.com cannot be added without first adding a default map policy as d
- If a source suffix has been specified for URL map policy, a destination suffix must also be specified.
- If an exact URL has been specified as the source, then the target URL should also be exact URL.
- If there is a source prefix in the URL, there must be also a destination prefix in the URL.

Top

rm policy map

Synopsis

rm policy map <mapPolicyName>

Description

Remove the map policies. Note: Before removing the map policy, you must first unbind the map policy from the reverse proxy virtual server.

Parameters

mapPolicyName

The name of the map policy.

Top

show policy map

Synopsis

show policy map [<mapPolicyName>]

Description

Display the map policies that have been configured and the related map policy information.

Parameters

mapPolicyName

The name of the map policy to be displayed.

Top

policy patset

[add | rm | bind | unbind | show]

add policy patset

Synopsis

add policy patset <name>

Description

Add a patset. Each patset is identified by a name.

Parameters

name

The name of the patset. The name must not exceed 127 characters.

Example

add policy patset pat1

Top

rm policy patset

Synopsis

rm policy patset <name>

Description

Remove the patset created by the add patset command.

Parameters

name

The name of the patset.

Example

rm policy patset pat1

Top

bind policy patset

Synopsis

bind policy patset <name> <string> [-index <positive_integer>] [-charset (ASCII | UTF_8)]

Description

Bind string to a patset. If first patern(string) is bound using index label then next bind statements to that patset should provide index, and vice versa

Parameters

name

The name of the patset.

string

The string associated with the patset.

Example

bind policy patset pat1 bar -index 2

Top

unbind policy patset

Synopsis

unbind policy patset <name> <string> ...

Description

Unbind string(s) from a patset.

Parameters

name

The name of the patset.

string

The string associated with the patset.

Example

unbind policy patset pat1 bar xyz

Top

show policy patset

Synopsis

show policy patset [<name>]

Description

Display the configured patset(s).

Parameters

name

The name of the patset.

Example

show policy patset pat1

Top

policy dataset

[add | rm | bind | unbind | show]

add policy dataset

Synopsis

add policy dataset <name> <type>

Description

Add a dataset. Each dataset is identified by a name.

Parameters

name

The name of the set. The name must not exceed 127 characters.

type

The type of set: ipv4, ipv6, number Possible values: ipv4, number, ipv6

Example

add policy dataset ts1 -type IPV4

Top

rm policy dataset

Synopsis

rm policy dataset <name>

Description

Remove the set created by the add set command.

Parameters

name

The name of the set. The name must not exceed 127 characters.

Example

rm policy dataset pat1

Top

bind policy dataset

Synopsis

bind policy dataset <name> <value> [-index <positive_integer>]

Description

Bind a value (ipv4, ipv6, number) to a dataset. If first value is bound using index label then next bind statements to that set should provide index, and vice versa

Parameters

name

The name of the set. The name must not exceed 127 characters.

value

The value (ipv4, ipv6, number) associated with the set.

Example

bind policy dataset ts1 192.168.20.1 -index 2

Top

unbind policy dataset

Synopsis

unbind policy dataset <name> <value>

Description

Unbind string(s) from a set.

Parameters

name

The name of the set. The name must not exceed 127 characters.

value

The value (ipv4, ipv6, number) associated with the set.

Example

unbind policy dataset pat1 bar xyz

Top

show policy dataset

Synopsis

show policy dataset [<name>]

Description

Display the configured dataset(s).

Parameters

name

The name of the set. The name must not exceed 127 characters.

Example

show policy dataset set1

Top

policy httpCallout

[add | rm | set | unset | show]

add policy httpCallout

Synopsis

add policy httpCallout <name>

Description

Add a httpcallout. Each httpcallout is identified by a name.

Parameters

name

The name of the httpcallout. The name must not exceed 31 characters.

Example

add policy httpcallout h1

Top

rm policy httpCallout

Synopsis

rm policy httpCallout <name>

Description

Removes the httpcallout entity

Parameters

name

The name of the httpcallout.

Example

rm policy httpcallout h1

Top

set policy httpCallout

Synopsis

set policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-port <port|*>] [-vServer <string>] [-returnType <returnType>] [-httpMethod (GET | POST)] [-hostExpr <string>] [-urlStemExpr <string>] [-headers <name(value)> ...] [-parameters <name(value)> ...] [-fullReqExpr <string>] [-resultExpr <string>]

Description

Sets attributes for an httpcallout policy. You invoke this policy by specifying the SYS.HTTP_CALLOUT expression prefix in an advanced expression.

Parameters

name

The name of the httpcallout.

IPAddress

IPv4 or IPv6 address of the server to which the callout is sent, or a wildcard. Mutually exclusive with the -vserver argument.

port

If you specify an IP address, this is the port on the server to which the callout is sent, or a wildcard.

vServer

The name of a load balancing, content switching, or cache redirection virtual server with a service type of HTTP. This is where the callout is sent. This option is mutually exclusive with IP address and port.

returnType

Type of data that the target application returns in the response to the callout. Possible values: BOOL, NUM, TEXT

httpMethod

Method used in the HTTP request that this callout sends. Mutually exclusive with -fullReqExpr. Possible values: GET, POST

hostExpr

Advanced text expression to configure the Host header. The expression can contain a literal value (10.101.10.11) or a derived value (for example, http.req.header. . .). Mutually exclusive with -fullReqExpr.

urlStemExpr

An advanced string expression for generating the URL stem. The expression can contain a literal string (for example, /mysite/index.html) or an expression that derives the value (for example, http.req.url). Mutually exclusive with -fullReqExpr.

headers

Advanced text expression to insert HTTP headers and their values in the HTTP callout request. You must specify a value for every header. You specify the header name as a string and the header value as an advanced expression. Mutually exclusive with -fullReqExpr.

parameters

Advanced expression to insert query parameters in the HTTP request that the callout sends. You must specify a value for every parameter that you configure. If the callout request uses the GET method, these parameters are inserted in the URL. If the callout request uses the POST method, these parameters are inserted in the POST body. You configure the query parameter name as a string, and the value as an advanced expression. The parameter values are URL encoded. Mutually exclusive with -fullReqExpr.

fullReqExpr

Exact HTTP request that the NetScaler is to send, as an advanced expression of up to 8191 characters. If you specify this parameter, you must omit the httpMethod, hostExpr, urlStemExpr, headers, and parameters arguments. The request expression is constrained by the feature where the callout is used. For example, an HTTP.RES expression cannot be used in a request-time policy bank or in a TCP content switching policy bank. The NetScaler does not check the validity of this request. You must manually validate the request.

resultExpr

Advanced expression that extracts HTTP.RES objects from the response to the HTTP callout. The maximum length is 8191. The operations in this expression must match the return type. For example, if you configure a return type of TEXT, the result expression must be a text-based expression. If the return type is NUM, the result expression (resultExpr) must return a numeric value, as in the following: http.res.body(10000).length.

Example

set policy httpcallout h1 -vServer v1

Top

unset policy httpCallout

Synopsis

unset policy httpCallout <name> [-IPAddress] [-port] [-vServer] [-httpMethod] [-hostExpr] [-urlStemExpr] [-headers] [-parameters] [-fullReqExpr] [-resultExpr]

Description

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

Top

show policy httpCallout

Synopsis

show policy httpCallout [<name>]

Description

Display the configured httpcallout(s).

Parameters

name

The name of the httpcallout.

Example

show policy httpcallout h1

Top

policy stringmap

[add | rm | set | unset | bind | unbind | show]

add policy stringmap

Synopsis

add policy stringmap <name> [-comment <string>]

Description

Create a string map. String map consists of key-value pairs. It must contain unique keys.

Parameters

name

The name of the string map that will be created.

comment

Comments associated with this string map.

Example

i) add stringmap custom_stringmap
. This creates a new string map with name custom_stringmap.

Top

rm policy stringmap

Synopsis

rm policy stringmap <name>

Description

Remove a previously defined string map. String map can only be removed if it is not used in any part of policy, action or expression.

Parameters

name

The name of the string map that will be removed.

Example

i) rm stringmap custom_stringmap
. This removes a string map whose name is custom_stringmap

Top

set policy stringmap

Synopsis

set policy stringmap <name> -comment <string>

Description

This command modifies a existing string map.

Parameters

name

The name of the string map.

comment

Comments associated with this string map.

Example

i) set stringmap custom_stringmap -comment "custom string map is for URLs."
. This updates the comment associated with the string map whose name is custom_stringmap

Top

unset policy stringmap

Synopsis

unset policy stringmap <name> -comment

Description

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

Top

bind policy stringmap

Synopsis

bind policy stringmap <name> <key> <value>

Description

Bind key-value to a string map. This adds the key and its associated value in the string map. If the key already exist, and has a different value, old value is over-written with new value.

Parameters

name

The name of the string map.

key

The key in the string map.

Example

bind stringmap custom_stringmap "key-string" "value-string"
. This adds the key "key-string" and its associated value "value-string" to the string map whose name is cust

Top

unbind policy stringmap

Synopsis

unbind policy stringmap <name> <key>

Description

Unbind key from a string map. Removes key from the string map

Parameters

name

The name of the string map.

key

The key to be removed from the string map.

Example

unbind stringmap custom_stringmap key1
. This removes the key "key1" and its associated value from the string map whose name is custom_stringma

Top

show policy stringmap

Synopsis

show policy stringmap [<name>]

Description

Display the configured string map. It displays all the keys and their corresponding values in the string map.

Parameters

name

The name of the string map, if no name is given then names of all string maps will be displayed.

Example

show stringmap custom_stringmap
. Displays all the key-value pairs of a string map whose name is custom-stringmap

Top

PQ Commands

This group of commands can be used to perform operations on the following entities:

- pq
- pq policy
- pq stats

pq

stat pq

Synopsis

stat pq [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Displays statistics of priority queuing.

pq policy

[add | rm | set | unset | show | stat]

add pq policy

Synopsis

add pq policy <policyName> -rule <expression> -priority <positive_integer> [-weight <positive_integer>] [-qDepth <positive_integer> | -polqDepth <positive_integer>]

Description

Adds a priority queuing policy to the appliance. Note: To use the priority queuing policy on a virtual server, the virtual server must have priority queuing enabled by using the 'set lb vserver' command and the priority queuing policy must be bound to the load balancing virtual server by using the 'bind lb vserver' command.

Parameters

policyName

The name for the priority queuing policy. The name can include a maximum of 31 characters that include letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. The name can begin with a letter, number, or the underscore (_) symbol.

rule

The condition for applying the policy. When requests are received by a system, they are classified into different priority levels based on the expression logic that they match. Expression logic is expression names, separated by the logical operators || and &&, and possibly grouped using parenthesis. If the expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes. The following are valid expression logic: - ns_ext_cgi||ns_ext_asp - ns_non_get && (ns_header_cookie||ns_header_pragma) When a request comes to the system, it is prioritized based on the expression list that is matched.

priority

The priority of queuing the request. When a request matches the configured rule, and if server resources are not available, this option specifies a priority for queuing the request until server resources are available. Enter the value as a positive integer 1, 2 or 3. The highest priority is 1 and the lowest priority is 3. Minimum value: 1 Maximum value: 3

weight

The weight for the priorty level. Each priority level is assigned a weight according to which it is served when server resources are available. The weight for a higher priority request must be set higher than that of a lower priority request. The default weights for the priority queues 1, 2, and 3 are 3, 2, and 1 respectively. Specify the weights as 0 through 101. A weight of 0 indicates that the particular priority level must be served only when there are no requests in any of the priority queues. A weight of 101 specifies a weight of infinity. This means that this priority level is served irrespective of the number of clients waiting in other priority queues. Maximum value: 101

qDepth

The queue depth threshold value. When the number of waiting requests in the queue (or queue size) on the virtual server to which this policy is bound, increases to the specified qdepth value, any subsequent requests are dropped to the lowest priority level. Maximum value: 4294967294

polqDepth

The policy queue depth threshold value. When the number of waiting requests in all the queue belonging to this policy (or the policy queue size) increases to the specified polqdepth value, all subsequent requests are dropped to the lowest priority level. Maximum value: 4294967294

Top

rm pq policy

Synopsis

rm pq policy <policyName> ...

Description

Removes a priority queuing policy from the appliance.

Parameters

policyName

The name of the priority queuing policy to be removed.

Top

set pq policy

Synopsis

set pq policy <policyName> [-weight <positive_integer>] [-qDepth <positive_integer> | -polqDepth <positive_integer>]

Description

Modifies the attributes of a priority queuing policy.

Parameters

policyName

The name of the priority queuing policy to be modified.

weight

The weight for the priorty level. Each priority level is assigned a weight according to which it is served when server resources are available. The weight for a higher priority request must be set higher than that of a lower priority request. The default weights for the priority queues 1, 2, and 3 are 3, 2, and 1 respectively. Specify the weights as 0 through 101. A weight of 0 indicates that the particular priority level must be served only when there are no requests in any of the priority queues. A weight of 101 specifies a weight of infinity. This means that this priority level is served irrespective of the number of clients waiting in other priority queues. Maximum value: 101

qDepth

The queue depth threshold value. When the number of waiting requests in the queue (or queue size) on the virtual server to which this policy is bound, increases to the specified qdepth value, any subsequent requests are dropped to the lowest priority level. Maximum value: 4294967294

polqDepth

The policy queue depth threshold value. When the number of waiting requests in all the queue belonging to this policy (or the policy queue size) increases to the specified polqdepth value, all subsequent requests are dropped to the lowest priority level. Maximum value: 4294967294

Top

unset pq policy

Synopsis

unset pq policy <policyName> [-weight] [-qDepth] [-polqDepth]

Description

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

Top

show pq policy

Synopsis

show pq policy [<policyName>]

Description

Displays details of the priority queuing policy.

Parameters

policyName

The name of the priority queuing policy whose details must be displayed. If a name is not provided, details of all priority queuing policies available on the appliance are displayed.

Top

stat pq policy

Synopsis

stat pq policy [<policyName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display priority queuing policy statistics.

Parameters

policyName

The name of the priority queuing policy whose statistics must be displayed. If a name is not provided, details of all priority queuing policies available on the appliance are displayed.

Top

pq stats

show pq stats

Synopsis

show pq stats - alias for 'stat pq'

Description

show pq stats is an alias for stat pq

Protocol Commands

This group of commands can be used to perform operations on the following entities:

- protocol tcp
- protocol http
- protocol icmp
- protocol ipv6
- protocol icmpv6
- protocol ip
- protocol udp
- protocol httpBand

protocol tcp

stat protocol tcp

Synopsis

stat protocol tcp [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display TCP protocol statistics

protocol http

stat protocol http

Synopsis

stat protocol http [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display HTTP protocol statistics

protocol icmp

stat protocol icmp

Synopsis

stat protocol icmp [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display ICMP protocol statistics

protocol ipv6

stat protocol ipv6

Synopsis

stat protocol ipv6 [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display ipv6 protocol statistics

protocol icmpv6

stat protocol icmpv6

Synopsis

stat protocol icmpv6 [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display icmpv6 protocol statistics

protocol ip

stat protocol ip

Synopsis

stat protocol ip [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display IP protocol statistics

protocol udp

stat protocol udp

Synopsis

stat protocol udp [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display UDP protocol statistics

protocol httpBand

[set | unset | show]

set protocol httpBand

Synopsis

set protocol httpBand [-reqBandSize <integer>] [-respBandSize <integer>]

Description

Set band size for HTTP request/response band statistics.

Parameters

reqBandSize

Band size for HTTP request band statistics. Default value: 100 Minimum value: 50

respBandSize

Band size for HTTP response band statistics. Default value: 1024 Minimum value: 50

Example

set protocol httpBand -reqBandSize 200 -respBandSize 2048

Top

unset protocol httpBand

Synopsis

unset protocol httpBand [-reqBandSize] [-respBandSize]

Description

Use this command to remove protocol httpBand settings.Refer to the set protocol httpBand command for meanings of the arguments.

Top

show protocol httpBand

Synopsis

show protocol httpBand -type (REQUEST | RESPONSE)

Description

Display HTTP request/response band statistics.

Parameters

type

Specify whether to display request/response band statistics. Possible values: REQUEST, RESPONSE

Top

Responder Commands

This group of commands can be used to perform operations on the following entities:

- responder policy
- responder action
- responder policylabel
- responder global
- responder param
- responder htmlpage

responder policy

[add | rm | set | unset | show | rename | stat]

add responder policy

Synopsis

add responder policy <name> <rule> <action> [<undefAction>] [-comment <string>] [-logAction <string>] [-appflowAction <string>]

Description

Add a responder policy.

Parameters

name

Name of the responder policy

rule

Expression to be used by responder policy. It has to be a boolean PI rule expression.

action

Responder action to be used by the policy.

undefAction

Responder action to be taken in the case of UNDEF event during policy evaluation. Should be NOOP, RESET or DROP.

comment

Comments associated with this responder policy.

logAction

The log action associated with the responder policy

appflowAction

The appflow action associated with the ES4NS responder policy

Example

i) add responder policy pol9 "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_respondwith

Top

rm responder policy

Synopsis

rm responder policy <name>

Description

Remove a responder policy.

Parameters

name

Name of the responder policy to be removed.

Example

rm responder policy pol9

Top

set responder policy

Synopsis

set responder policy <name> [-rule <expression>] [-action <string>] [-undefAction <string>] [-comment <string>] [-logAction <string>] [-appflowAction <string>]

Description

Set a new rule/action for existing unbound responder policy.

Parameters

name

Name of the responder policy

rule

Expression to be used by responder policy. It has to be a boolean PI rule expression.

action

Responder action to be used by the policy.

undefAction

Responder action to be taken in the case of UNDEF event during policy evaluation. Should be NOOP, RESET or DROP.

comment

Comments associated with this responder policy.

logAction

The log action associated with the responder policy

appflowAction

The appflow action associated with the ES4NS responder policy

Example

set responder policy pol9 -rule "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

Top

unset responder policy

Synopsis

unset responder policy <name> [-undefAction] [-comment] [-logAction] [-appflowAction]

Description

Unset undefAction for existing responder policy..Refer to the set responder policy command for meanings of the arguments.

Example

unset responder policy respol9 -undefAction

Top

show responder policy

Synopsis

show responder policy [<name>] show responder policy stats - alias for 'stat responder policy'

Description

Display all the configured responder policies.

Parameters

name

Name of the responder policy.

Example

show responder policy

Top

rename responder policy

Synopsis

rename responder policy <name>@ <newName>@

Description

Rename a responder policy.

Parameters

name

The name of the responder policy.

newName

The new name of the responder policy.

Example

rename responder policy oldname newname

Top

stat responder policy

Synopsis

stat responder policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display responder policy statistics.

Parameters

name

The name of the responder policy for which statistics will be displayed. If not given statistics are shown for all responder policies.

Top

responder action

[add | rm | set | unset | show | rename]

add responder action

Synopsis

add responder action <name> <type> (<target> | <htmlpage>) [-bypassSafetyCheck (YES | NO)] [-comment <string>]

Description

Creates a responder action. The action thus created can be associated with responder policy by using "add responder policy" command. The system has following built-in action entities: NOOP - the no-op action. RESET - reset the current client and server connection. DROP - drop packets when rate exceeds the rate-limiting threshold

Parameters

name

Name of the responder action to be added.

type

Type of responder action. It can be: (respondwith|redirect). For each action type the <target> is as defined below. o RESPONDWITH: Send the specified response. <target> = SNIT expression to be sent as the response. <htmlpage> = HTML page to be sent as the response. o REDIRECT: Generates an 'HTTP Redirect' to a specified URL. <target> = where to redirect to. o SQLRESPONSE_OK: Generates an OK response. <target> = Message for SQL OK Packet. o SQLRESPONSE_ERROR: Generates an ERROR response. <target> = Message for SQL ERROR Packet. Possible values: noop, respondwith, redirect, respondwithhtmlpage, sqlresponse_ok, sqlresponse_error

target

Expression specifying what to respond with. Maximum length of the input expression is 8191 bytes. Maximum size of string that can be used inside the expression is 255 bytes. Multiple string literals can be concatenated using +. For action type SQLRESPONSE_* the maximum length of target string is 511 bytes.

htmlpage

Name of the html page. htmlpage has to be imported via the 'import responder htmlpage' command.

bypassSafetyCheck

Bypass the safety check and allow unsafe expressions Possible values: YES, NO Default value: NO

comment

Comments associated with this responder action.

Example

1) add responder action act1 respondwith "\\"HTTP/1.1 200 OK\\r\\n\\r\\n\\""
2) add responder action resp respondwithhtmlpage my-responder-page,
3) add responder action redir_action redirect '"http://backupsite2.com" + HTTP.REQ.URL' -bypassSafetyChec

Top

rm responder action

Synopsis

rm responder action <name>

Description

Remove a configured responder action.

Parameters

name

Name of the responder action.

Example

rm responder action act_before

Top

set responder action

Synopsis

set responder action <name> [-target <string> [-bypassSafetyCheck (YES | NO)]] [-htmlpage <string>] [-comment <string>]

Description

Modify a responder action.

Parameters

name

Name of the responder action to be added.

target

Expression specifying what to respond with. Maximum length of the input expression is 8191 bytes. Maximum size of string that can be used inside the expression is 255 bytes. Multiple string literals can be concatenated using +. For action type SQLRESPONSE_* the maximum length of target string is 511 bytes.

htmlpage

Name of the html page. htmlpage has to be imported via the 'import responder htmlpage' command.

comment

Comments associated with this responder action.

Example

1. set responder action act_responder -target 'HTTP.REQ.HEADER(MYURL)' -bypassSafetyCheck YES/,
2. set responder action act_responder -htmlpage my-local-file

Top

unset responder action

Synopsis

unset responder action <name> -comment

Description

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

Top

show responder action

Synopsis

show responder action [<name>]

Description

Display configured responder action(s).

Parameters

name

Name of the responder action.

Example

1. show responder action
2. show responder action act_insert

Top

rename responder action

Synopsis

rename responder action <name>@ <newName>@

Description

Rename a responder action.

Parameters

name

The name of the responder action.

newName

The new name of the responder action.

Example

rename responder action oldname newname

Top

responder policylabel

[add | rm | bind | unbind | show | stat | rename]

add responder policylabel

Synopsis

add responder policylabel <labelName> [-policylabeltype <policylabeltype>]

Description

Add a responder policy label.

Parameters

labelName

Name of the responder policy label.

policylabeltype

The type of the policy label. Default value is HTTP Possible values: HTTP, OTHERTCP, SIP_UDP, MYSQL, MSSQL Default value: NS_PLTMAP_RSP_REQ

Example

add responder policylabel resp_lab

Top

rm responder policylabel

Synopsis

rm responder policylabel <labelName>

Description

Remove a responder policy label.

Parameters

labelName

Name of the responder policy label.

Example

rm responder policylabel resp_lab

Top

bind responder policylabel

Synopsis

bind responder policylabel <labelName> <policyName> <priority> [<gotoPriorityExpression>] [-invoke (<labelType> <labelName>)]

Description

Bind the responder policy to one of the labels.

Parameters

labelName

Name of the responder policy label.

policyName

Name of the policy to be bound to responder policy label.

Example

i) bind responder policylabel resp_lab pol_resp 1 2
ii) bind responder policylabel resp_lab pol_resp 1 2 -invoke vserver CURRENT

Top

unbind responder policylabel

Synopsis

unbind responder policylabel <labelName> <policyName> [-priority <positive_integer>]

Description

Unbind entities from responder label.

Parameters

labelName

Name of the responder policy label.

policyName

The name of the policy to be unbound.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind responder policylabel resp_lab pol_resp

Top

show responder policylabel

Synopsis

show responder policylabel [<labelName>]

Description

Display policy label or policies bound to responder policylabel.

Parameters

labelName

Name of the responder policy label.

Example

i) show responder policylabel resp_lab
ii) show responder policylabel

Top

stat responder policylabel

Synopsis

stat responder policylabel [<labelName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of responder policylabel(s).

Parameters

labelName

The name of the responder policy label for which statistics will be displayed. If not given statistics are shown for all responder policylabels.

Top

rename responder policylabel

Synopsis

rename responder policylabel <labelName>@ <newName>@

Description

Rename a responder policylabel.

Parameters

labelName

The name of the responder policylabel.

newName

The new name of the responder policylabel.

Example

rename responder policylabel oldname newname

Top

responder global

[bind | unbind | show]

bind responder global

Synopsis

bind responder global <policyName> <priority> [<gotoPriorityExpression>] [-type <type>] [-invoke (<labelType> <labelName>)]

Description

Binds the responder policy with given priority

Parameters

policyName

Name of the policy to be bound to responder global.

Example

i) bind responder global pol9 9

Top

unbind responder global

Synopsis

unbind responder global <policyName> [-type <type>] [-priority <positive_integer>]

Description

Unbind entities from responder global.

Parameters

policyName

The name of the policy to be unbound.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind responder global pol9

Top

show responder global

Synopsis

show responder global [-type <type>]

Description

Display the responder global bindings.

Parameters

type

The bindpoint to which policy is bound. Possible values: REQ_OVERRIDE, REQ_DEFAULT, OVERRIDE, DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE, MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT

Example

show responder global

Top

responder param

[set | unset | show]

set responder param

Synopsis

set responder param -undefAction <string>

Description

Set the default responder undef action. If an UNDEF event is triggered during policy evaluation and if the current policy's undefAction is not specified, then this global undefAction value is used. NOOP is the default value of default responder undef action

Parameters

undefAction

can be NOOP, RESET or DROP Default value: "NOOP"

Example

set responder param -undefAction RESET

Top

unset responder param

Synopsis

unset responder param -undefAction

Description

Unset responder params..Refer to the set responder param command for meanings of the arguments.

Example

unset responder param -undefAction

Top

show responder param

Synopsis

show responder param

Description

Display default responder undef action.

Example

show responder param

Top

responder htmlpage

[import | rm | update | show]

import responder htmlpage

Synopsis

import responder htmlpage [<src>] <name> [-comment <string>] [-overwrite]

Description

Downloads the input HTML Page to NetScaler Box with the given object name

Parameters

name

Indicates name of the html page to import/update.

comment

Comments.

overwrite

Overwrites the existing file

Example

import responder htmlpage http://www.example.com/page.html my-responder-page

Top

rm responder htmlpage

Synopsis

rm responder htmlpage <name>

Description

Removes the object imported by import responder htmlpage.

Parameters

name

Indicates name of the html page to import/update.

Example

rm responder htmlpage <name>

Top

update responder htmlpage

Synopsis

update responder htmlpage <name>

Description

Reloads the HTML page of the given object name in responder actions

Parameters

name

Indicates name of the html page to import/update.

Example

update responder htmlpage my-responder-page

Top

show responder htmlpage

Synopsis

show responder htmlpage [<name>]

Description

Displays the object imported by import responder htmlpage.

Parameters

name

Indicates name of the html page to import/update.

Example

show responder htmlpage

Top

Rewrite Commands

This group of commands can be used to perform operations on the following entities:

- rewrite policy
- rewrite action
- rewrite policylabel
- rewrite global
- rewrite param

rewrite policy

[add | rm | set | unset | show | stat | rename]

add rewrite policy

Synopsis

add rewrite policy <name> <rule> <action> [<undefAction>] [-comment <string>] [-logAction <string>]

Description

Add a rewrite policy.

Parameters

name

Name of the rewrite policy

rule

Expression to be used by rewrite policy. It has to be a boolean PI rule expression.

action

Rewrite action to be used by the policy.

undefAction

A rewrite action, to be used by the policy when the rule evaluation turns out to be undefined. The undef action can be NOREWRITE, RESET or DROP

comment

Comments associated with this rewrite policy.

logAction

The log action associated with the rewrite policy

Example

i) add rewrite policy pol9 "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_insert
ii) add rewrite policy pol9 "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_insert NOREWRITE

iii) add rewrite policy pol9 "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_insert RESET
iii) add rewrite policy pol9 "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_insert DROP

Top

rm rewrite policy

Synopsis

rm rewrite policy <name>

Description

Remove a rewrite policy.

Parameters

name

Name of the rewrite policy to be removed.

Example

rm rewrite policy pol9

Top

set rewrite policy

Synopsis

set rewrite policy <name> [-rule <expression>] [-action <string>] [-undefAction <string>] [-comment <string>] [-logAction <string>]

Description

Set a new rule/action/undefAction for existing rewrite policy. The rule flow type can change only if: . action and undefAction(if present) are of NEUTRAL flow type

Parameters

name

Name of the rewrite policy

rule

Expression to be used by rewrite policy. It has to be a boolean PI rule expression.

action

Rewrite action to be used by the policy.

undefAction

A rewrite action, to be used by the policy when the rule evaluation turns out to be undefined. The undef action can be NOREWRITE, RESET or DROP

comment

Comments associated with this rewrite policy.

logAction

The log action associated with the rewrite policy

Example

set rewrite policy pol9 -rule "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

Top

unset rewrite policy

Synopsis

unset rewrite policy <name> [-undefAction] [-comment] [-logAction]

Description

Unset undefAction for existing rewrite policy..Refer to the set rewrite policy command for meanings of the arguments.

Example

unset rewrite policy pol9 -undefAction

Top

show rewrite policy

Synopsis

show rewrite policy [<name>] show rewrite policy stats - alias for 'stat rewrite policy'

Description

Display all the configured rewrite policies.

Parameters

name

Name of the rewrite policy.

Example

show rewrite policy

Top

stat rewrite policy

Synopsis

stat rewrite policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display rewrite policy statistics.

Parameters

name

The name of the rewrite policy for which statistics will be displayed. If not given statistics are shown for all rewrite policies.

Example

stat rewrite policy

Top

rename rewrite policy

Synopsis

rename rewrite policy <name>@ <newName>@

Description

Rename a rewrite policy.

Parameters

name

The name of the rewrite policy.

newName

The new name of the rewrite policy.

Example

rename rewrite policy oldname newname

Top

rewrite action

[add | rm | set | unset | show | rename]

add rewrite action

Synopsis

add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-pattern <expression> | -search <expression>] [-bypassSafetyCheck (YES | NO)] [-refineSearch <string>] [-comment <string>]

Description

Creates a rewrite action. The action thus created can be associated with rewrite policy by using "add rewrite policy" command. The system has three built-in action entities: NOREWRITE - no-op action RESET - reset the current client and server connection DROP - drop packets when rate exceeds the rate-limiting threshold A flow type is implicitly associated with every action.Following 3 flow types are possible: 1. Neutral : the action can be request or response time action 2. Request : the action can only be executed at request time 3. Response : the action can only be executed at response time

Parameters

name

Name of the rewrite action to be added.

type

Type of rewrite action. It can be: (replace|insert_http_header|delete_http_header|corrupt_http_header|insert_before|insert_after|delete|replace_http_res). For each action type the <target> and <string builder expr> are defined below. o INSERT_HTTP_HEADER: Will insert a HTTP header. <target> = header name. <string builder expr> = header value specified as a compound text expression. o INSERT_SIP_HEADER: Will insert a SIP header. <target> = header name. <string builder expr> = header value specified as a compound text expression. o DELETE_HTTP_HEADER: Will delete all occurrence of HTTP header. <target> = header name. o DELETE_SIP_HEADER: Will delete all occurrence of SIP header. <target> = header name. o CORRUPT_HTTP_HEADER: Will corrupt all occurrence of HTTP header. <target> = header name. o CORRUPT_SIP_HEADER: Will corrupt all occurrence of SIP header. <target> = header name. o REPLACE: Will replace the target text reference with the value specified in attr. <target> = Advanced text expression <string builder expr> = Compound text expression o INSERT_BEFORE: Will insert the value specified by attr before the target text reference. <target> = Advanced text expression <string builder expr> = Compound text expression o INSERT_AFTER: Will insert the value specified by attr after the target text reference. <target> = Advanced text expression <string builder expr> = Compound text expression o DELETE: Delete the target text

reference. <target> = Advanced text expression o REPLACE_HTTP_RES: Replace the http response with value specified in target. <target> = Compound text expression o REPLACE_SIP_RES: Replace the SIP response with value specified in target. <target> = Compound text expression o REPLACE_ALL: Replaces all occurrence of the pattern in the text provided in the target with the text provided in the stringBuilderExpr, with a string defined in the -pattern argument or -search argument. For example, you can replace all occurences of abcd with -pattern efgh. <target> = text in a request or a response, for example http.req.body(1000) <stringBuilderExpr> = Compound text expression -pattern <expression> = string constant, for example -pattern efgh or -search text("efgh") o INSERT_BEFORE_ALL: Will insert the value specified by stringBuilderExpr before all the occurrence of pattern in the target text reference. <target> = Advanced text expression <stringBuilderExpr> = Compound text expression -pattern <expression> = string constant or advanced regular expression or -search regex(<regular expression>) or -search text(string constant) o INSERT_AFTER_ALL: Will insert the value specified by stringBuilderExpr after all the occurrence of pattern in the target text reference. <target> = Advanced text expression <stringBuilderExpr> = Compound text expression -pattern <expression> = string constant or advanced regular expression or -search regex(<regular expression>) or -search text(string constant) o DELETE_ALL: Delete all the occurrence of pattern in the target text reference. <target> = Advanced text expression -pattern <expression> = string constant or advanced regular expression or -search regex(<regular expression>) or -search text(string constant) Possible values: noop, delete, insert_http_header, delete_http_header, corrupt_http_header, insert_before, insert_after, replace, replace_http_res, delete_all, replace_all, insert_before_all, insert_after_all, clientless_vpn_encode, clientless_vpn_encode_all, clientless_vpn_decode, clientless_vpn_decode_all, insert_sip_header, delete_sip_header, corrupt_sip_header, replace_sip_res

target

Expression specifying which part of HTTP packet needs to be rewritten.

stringBuilderExpr

Expression specifying new value of the rewritten HTTP packet. Maximum length of the input expression is 8191. Maximum size of string that can be used inside the expression is 1499.

pattern

Pattern to be used for insert_before_all, insert_after_all, replace_all, delete_all action types.

search

search expression takes the followin 5 argumens to use the appropriate methods to search in the specified body or header: 1. text(string) - example: -search text("hello") 2. regex(re<delimiter>regular exp<delimiter>) - example: -search regex(re/^hello/) 3. xpath(xp<delimiter>xpath expression<delimiter>) - example: -search xpath(xp%/a/b%) 4. xpath_json(xp<delimiter>xpath expression<delimiter>) - example: -search xpath_json(xp%/a/b%) xpath_json_search takes xpath expression as argument but operates on json file instead of xml file. 5. patset(patset) - example: -search patset("patset1") search expression are allowed on actions of type 1) replace_all 2) insert_after_all 3) delete_all 4) insert_before_all. search is a super set of pattern. It is advised to use search over pattern.

bypassSafetyCheck

Bypass the safety check and allow unsafe expressions. Possible values: YES, NO Default value: NO

refineSearch

refineSearch expressions specifies how the selected HTTP data can further be refined. These expression always starts with the 'Extend(m,n)' operation. Where 'm' specifies number of bytes to the left of selected data and 'n' specifies number of bytes to the right of selected data. refineSearch expression are only allowed on body based expression and for actions of type 1) replace_all 2) insert_after_all 3) delete_all 4) insert_before_all. This can accelerate search using regular expression. For example if we need to find all the urls from www.zippo.com in a response body. Rather than writing a regular expression to search this url pattern we can search for 'zippo' pattern first and then extend the search space by some bytes and finally check for prefix 'www.zippo.com'. The rewrite command might look like: add rewrite action act1 delete_all 'http.res.body(10000)' -pattern "zippo" -refineSearch "extend(10,10).regex_select(re%<www.zippo.com[^>].*>%)" Maximum length of the input expression is 8191. Maximum size of string that can be used inside the expression is 1499.

comment

Comments associated with this rewrite action.

Example

i) add rewrite action act_insert INSERT_HTTP_HEADER change_req "\\"no change\\""
. This Adds to http header
will add the header change_req: no change.
ii) add rewrite action act_replace REPLACE "HTTP.REQ.URL.PREFIX(1)" "HTTP.REQ.URL.PREFIX(1)+\\"citrix/\\"
. If HTTP.REQ.URL.PREFIX(1) is / the result would be /citrix/
iii) add rewrite action act_before INSERT_BEFORE "HTTP.REQ.HEADER(\\"host\\").VALUE(0)" "\\"india\\""
. If HTTP.REQ.HEADER(\\"host\\").VALUE(0) is netscaler.com the result would be indianetscaler.com
iv) add rewrite action act_after INSERT_AFTER "HTTP.REQ.HEADER(\\"host\\").TYPECAST_LIST_T('.').GET(0)" "
. If HTTP.REQ.HEADER(\\"host\\").VALUE(0) is support.netscaler.com then the result would be support-india
v) add rewrite action act_delete DELETE "HTTP.REQ.HEADER(\\"host\\").VALUE(0)"
will leave the Host header looking like "HOST: ".
vi) add rewrite action act_delete_header DELETE_HTTP_HEADER Host
will delete the Host header. If Host header occurs more than once all occurrence of the header will be delet
vii) add rewrite action act_corrupt_header CORRUPT_HTTP_HEADER Host
will corrupt the Host header. If Host header occurs more than once all occurrence of the header will be corr

Top

rm rewrite action

Synopsis

rm rewrite action <name>

Description

Remove a configured rewrite action.

Parameters

name

Name of the rewrite action.

Example

rm rewrite action act_before

Top

set rewrite action

Synopsis

set rewrite action <name> [-target <string>] [-stringBuilderExpr <string>] [-pattern <expression> | -search <expression>] [-bypassSafetyCheck (YES | NO)] [-refineSearch <string>] [-comment <string>]

Description

Modify rewrite action.

Parameters

name

The name of rewrite action to be modified.

target

Expression specifying which part of the HTTP packet is to be rewritten.

stringBuilderExpr

Expression specifying new value of the rewritten HTTP packet. Maximum length of the input expression is 8191. Maximum size of string that can be used inside the expression is 1499.

pattern

Pattern to be used for insert_before_all, insert_after_all, replace_all, delete_all action types.

search

search expression takes the followin 5 argumens to use the appropriate methods to search in the specified body or header: 1. text(string) - example: -search text("hello") 2. regex(re<delimiter>regular exp<delimiter>) - example: -search regex(re/^hello/) 3. xpath(xp<delimiter>xpath expression<delimiter>) - example: -search xpath(xp%/a/b%) 4. xpath_json(xp<delimiter>xpath expression<delimiter>) - example: -search xpath_json(xp%/a/b%) xpath_json_search takes xpath expression as argument but operates on json file instead of xml file. 5. patset(patset) - example: -search patset("patset1") search expression are allowed on actions of type 1) replace_all 2) insert_after_all 3) delete_all 4) insert_before_all. search is a super set of pattern. It is advised to use search over pattern.

bypassSafetyCheck

Bypass the safety check and allow unsafe expressions. Possible values: YES, NO Default value: NO

refineSearch

refineSearch expressions specifies how the selected HTTP data can further be refined. These expression always starts with the 'Extend(m,n)' operation. Where 'm' specifies number of bytes to the left of selected data and 'n' specifies number of bytes to the right of selected data. refineSearch expression are only allowed on body based expression and for actions of type 1) replace_all 2) insert_after_all 3) delete_all 4) insert_before_all. This can accelerate search using regular expression. For example if we need to find all the urls from www.zippo.com in a response body. Rather than writing a regular expression to search this url pattern we can search for 'zippo' pattern first and then extend the search space by some bytes and finally check for prefix 'www.zippo.com'. The rewrite command might look like: add rewrite action act1 delete_all 'http.res.body(10000)' -pattern "zippo" -refineSearch "extend(10,10).regex_select(re%<www.zippo.com[^>].*>%)" Maximum length of the input expression is 8191. Maximum size of string that can be used inside the expression is 1499.

comment

Comments associated with this rewrite action.

Example

set rewrite action rwact1 -target "HTTP.REQ.HEADER(\\"MyHdr\\")" -stringBuilderExpr "HTTP.REQ.URL.MARK_

Top

unset rewrite action

Synopsis

unset rewrite action <name> [-stringBuilderExpr] [-refineSearch] [-comment]

Description

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

Top

show rewrite action

Synopsis

show rewrite action [<name>]

Description

Display configured rewrite action(s).

Parameters

name

Name of the rewrite action.

Example

1. show rewrite action
2. show rewrite action act_insert

Top

rename rewrite action

Synopsis

rename rewrite action <name>@ <newName>@

Description

Rename a rewrite action.

Parameters

name

The name of the rewrite action.

newName

The new name of the rewrite action.

Example

rename rewrite action oldname newname

Top

rewrite policylabel

[add | rm | bind | unbind | show | stat | rename]

add rewrite policylabel

Synopsis

add rewrite policylabel <labelName> <transform>

Description

Add a rewrite policy label.

Parameters

labelName

Name of the rewrite policy label.

transform

The type of transformations allowed by the policies bound to the label. Possible values: http_req, http_res, othertcp_req, othertcp_res, url, text, clientless_vpn_req, clientless_vpn_res, sipudp_req, sipudp_res

Example

add rewrite policylabel trans_http_url http_req

Top

rm rewrite policylabel

Synopsis

rm rewrite policylabel <labelName>

Description

Remove a rewrite policy label.

Parameters

labelName

Name of the rewrite policy label.

Example

rm rewrite policylabel trans_http_url

Top

bind rewrite policylabel

Synopsis

bind rewrite policylabel <labelName> <policyName> <priority> [<gotoPriorityExpression>] [-invoke (<labelType> <labelName>)]

Description

Bind the rewrite policy to one of the labels.

Parameters

labelName

Name of the rewrite policy label.

policyName

The rewrite policy name.

Example

i) bind rewrite policylabel trans_http_url pol_1 1 2 -invoke reqvserver CURRENT
ii) bind rewrite policylabel trans_http_url pol_2 2

Top

unbind rewrite policylabel

Synopsis

unbind rewrite policylabel <labelName> <policyName> [-priority <positive_integer>]

Description

Unbind entities from rewrite label.

Parameters

labelName

Name of the rewrite policy label.

policyName

The rewrite policy name.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind rewrite policylabel trans_http_url pol_1

Top

show rewrite policylabel

Synopsis

show rewrite policylabel [<labelName>]

Description

Display policy label or policies bound to rewrite policylabel.

Parameters

labelName

Name of the rewrite policy label.

Example

i) show rewrite policylabel trans_http_url
ii) show rewrite policylabel

Top

stat rewrite policylabel

Synopsis

stat rewrite policylabel [<labelName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of rewrite policylabel(s).

Parameters

labelName

The name of the rewrite policy label for which statistics will be displayed. If not given statistics are shown for all rewrite policylabels.

Top

rename rewrite policylabel

Synopsis

rename rewrite policylabel <labelName>@ <newName>@

Description

Rename a rewrite policy label.

Parameters

labelName

The name of the rewrite policylabel.

newName

The new name of the rewrite policylabel.

Example

rename rewrite policylabel oldname newname

Top

rewrite global

[bind | unbind | show]

bind rewrite global

Synopsis

bind rewrite global <policyName> <priority> [<gotoPriorityExpression>] [-type <type>] [-invoke (<labelType> <labelName>)]

Description

Bind the rewrite policy to one of the two global lists of rewrite policies. A policy becomes active only after it is bound. All HTTP traffic will be evaluated against these two policy banks. There is a request time policy bank and a response time policy bank. The flow type of the policy implicitly determines which bank it gets bound to. Each bank of policies is an ordered list ordered by policies priority values. Policy Bank Evaluation The goal of evaluation is to traverse the ordered list of policies in the bank, find out which policies match and build a result set that will contain the actions of all the matching policies. While evaluating a policy if any advanced expression cannot be evaluated then UNDEF processing will get triggered. There are also other scenarios during policy traversal when UNDEF processing can get triggered. If an UNDEF event occurs while processing a policy, then (i) policy bank traversal ends, (ii) the result set of actions that was built so far is wiped out (iii) the current policy's undefAction is put in the result set and the evaluation ends.

Parameters

policyName

The rewrite policy name.

Example

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

Top

unbind rewrite global

Synopsis

unbind rewrite global <policyName> [-type <type>] [-priority <positive_integer>]

Description

Unbind entities from rewrite global.

Parameters

policyName

The rewrite policy name.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind rewrite global pol9

Top

show rewrite global

Synopsis

show rewrite global [-type <type>]

Description

Display the rewrite global bindings.

Parameters

type

The bindpoint to which to policy is bound. Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, OTHERTCP_RES_OVERRIDE, OTHERTCP_RES_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, SIPUDP_RES_OVERRIDE, SIPUDP_RES_DEFAULT

Example

show rewrite global

Top

rewrite param

[set | unset | show]

set rewrite param

Synopsis

set rewrite param -undefAction <string>

Description

Set the default rewrite undef action. If an UNDEF event is triggered during policy evaluation and if the current policy.s undefAction is not specified, then this global undefAction value is used. NOREWRITE is the default value of default rewrite undef action

Parameters

undefAction

can be NOREWRITE, RESET or DROP Default value: "NOREWRITE"

Example

set rewrite param -undefAction RESET

Top

unset rewrite param

Synopsis

unset rewrite param -undefAction

Description

Unset rewrite params..Refer to the set rewrite param command for meanings of the arguments.

Example

unset rewrite param -undefAction

Top

show rewrite param

Synopsis

show rewrite param

Description

Display default rewrite undef action.

Example

show rewrite param

Top

Router Commands

vtysh

Synopsis

vtysh

Description

Enters into the Virtual Teletype Shell (VTYSH) prompt, at which you can configure all the dynamic routing protocols. The NetScaler dynamic routing suite is based on ZebOS, the commercial version of GNU Zebra.

SC Commands

This group of commands can be used to perform operations on the following entities:

- sc
- sc policy
- sc stats
- sc parameter

SC

stat sc

Synopsis

stat sc [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display SureConnect statistics.

sc policy

[add | rm | set | unset | show | stat]

add sc policy

Synopsis

add sc policy <name> [-url <URL> | -rule <expression>] [-delay <usecs>] [-maxConn <positive_integer>] [-action <action> (<altContentSvcName> <altContentPath>)]

Description

Add the SureConnect policy.

Parameters

name

The name of the SureConnect policy.

url

The URL name. The system matches the incoming client request against the URL you enter here. If the incoming request does not match any of the configured URLs or the rules that have been configured, then SureConnect does not trigger.

rule

The rule that the system matches with the incoming request. The system matches the incoming request against the rules you enter here. Before matching against the configured rules, the system matches the requests with any of the configured URLs. Thus, URLs have a higher precedence over rules. If the incoming request does not match any of the configured URLs or the rules that have been configured, then SureConnect does not trigger. Expression logic is expression names, separated by the logical operators || and && , and possibly grouped using parenthesis. If the expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes.The following are valid expression logic: ns_ext_cgi||ns_ext_asp ns_non_get && (ns_header_cookie||ns_header_pragma)

delay

The delay threshold in microseconds for the configured URL or the rule. If the delay statistics gathered for the configured URL or rule exceeds the configured delay, then SureConnect is triggered on the incoming request which matched the corresponding delay. Minimum value: 1 Maximum value: 599999999

maxConn

The maximum number of concurrent connections that can be open for the configured URL or rule. You can enter this argument as any integer value greater than zero. Minimum value: 1 Maximum value: 4294967294

action

The action to be taken when the thresholds are met. The valid options are ACS , NS and NOACTION . ACS - Specifies that alternate content is to be served from altContSvcName with the path altContPath . NS - Specifies that alternate content is to be served from the system. See the set sc parameter command to customize the response served from the system. NOACTION - Specifies that no alternate content is to be served. However, delay statistics are still collected for the configured URLs. If the - maxconn argument is specified, the number of connections is limited to that specified value for that configured URL or rule (alternate content will not served even if the - maxconn threshold is met). Possible values: ACS, NS, NOACTION

altContentSvcName

The alternate content service name used in the ACS action.

altContentPath

The alternate content path for the ACS action.

Example

```
add sc policy scpol_ns -delay 1000000 -url /delay.asp -action NS

add policy expression exp_acs "url == /mc_acs.asp"
add service svc_acs 10.110.100.253 http 80
add scpolicy scpol_acs -maxconn 10 -rule exp_acs -action ACS svc_acs /altcont.htm
```

Top

rm sc policy

Synopsis

rm sc policy <name>

Description

Remove the SureConnect policy.

Parameters

name

The name of the SureConnect policy.

Example

rm sc policy scpol_ns
rm sc policy scpol_acs

Top

set sc policy

Synopsis

set sc policy <name> [-url <URL> | -rule <expression>] [-delay <usecs>] [-maxConn <positive_integer>] [-action <action> (<altContentSvcName> <altContentPath>)]

Description

Set the delay and maxConn parameters for the specified SureConnect policy.

Parameters

name

The name of the SureConnect policy.

url

The URL name. The system matches the incoming client request against the URL you enter here. If the incoming request does not match any of the configured URLs or the rules that have been configured, then SureConnect does not trigger.

rule

The rule that the system matches with the incoming request. The system matches the incoming request against the rules you enter here. Before matching against the configured rules, the system matches the requests with any of the configured URLs. Thus, URLs have a higher precedence over rules. If the incoming request does not match any of the configured URLs or the rules that have been configured, then SureConnect does not trigger. Expression logic is expression names, separated by the logical operators || and && , and possibly grouped using parenthesis. If the expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes.The following are valid expression logic: ns_ext_cgi||ns_ext_asp ns_non_get && (ns_header_cookie||ns_header_pragma)

delay

The delay threshold in microseconds for the configured URL or the rule. Minimum value: 1 Maximum value: 599999999

maxConn

The maximum number of concurrent connections that can be open for the configured URL or rule. Minimum value: 1 Maximum value: 4294967294

action

The action to be taken when the thresholds are met. The valid options are ACS , NS and NOACTION . ACS - Specifies that alternate content is to be served from altContSvcName with the path altContPath . NS - Specifies that alternate content is to be served from the system. See the set sc parameter command to customize the response served from the system. NOACTION - Specifies that no alternate content is to be served. However, delay statistics are still collected for the configured URLs. If the - maxconn argument is specified, the number of connections is limited to that specified value for that configured URL or rule (alternate content will not served even if the - maxconn threshold is met). Possible values: ACS, NS, NOACTION

Example

set sc policy scpol_ns -delay 2000000
set sc policy scpol_acs -maxconn 100

Top

unset sc policy

Synopsis

unset sc policy <name> [-delay] [-maxConn]

Description

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

Top

show sc policy

Synopsis

show sc policy [<name>]

Description

Display all of the Configured SureConnect policies.

Parameters

name

The name of the SureConnect policy.

Example

```
> show sc policy
        2 monitored Sure Connect Policies:
1)      Name: scpol_ns
        RULE: exp1
        Delay: 1000000 microsecs
        Alternate Content from NS
2)      Name: scpol_acs
        RULE: exp_acs
        Max Conn: 10
        Alternate Content from ACS, svc_acs        /delay/alcont.htm
 Done
```

Top

stat sc policy

Synopsis

stat sc policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display SureConnect policy statistics.

Parameters

name

The name of the SC policy for which statistics will be displayed. If not given stati stics are shown for all SC policies.

Top

sc stats

show sc stats

Synopsis

show sc stats - alias for 'stat sc'

Description

show sc stats is an alias for stat sc

sc parameter

[set | unset | show]

set sc parameter

Synopsis

set sc parameter [-sessionLife <secs>] [-vsr <input_filename>]

Description

set the SureConnect parameters.

Parameters

sessionLife

The time between the first time and next time the sureconnect alternet window display.The SureConnect alternate content window is displayed only once during a session. For the same browser accessing a configured URL.The value is in seconds. Default value: 300 Minimum value: 1 Maximum value: 4294967294

vsr

The file containing the customized response that is to be displayed with ACTION as NS in the SureConnect policy. Default value: "DEFAULT"

Example

set sc parameter -sessionlife 200 -vsr /etc/vsr.htm

Top

unset sc parameter

Synopsis

unset sc parameter [-sessionLife] [-vsr]

Description

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

Top

show sc parameter

Synopsis

show sc parameter

Description

Display the SureConnect parameters set through the use of the ###set sc parameter### command.

Example

```
> show sc parameter
    Sure Connect Parameters:
    Sessionlife: 300
    Vsr: DEFAULT
 Done
```

Top

SNMP Commands

This group of commands can be used to perform operations on the following entities:

- snmp
- snmp community
- snmp manager
- snmp trap
- snmp group
- snmp view
- snmp user
- snmp oid
- snmp stats
- snmp alarm
- snmp mib
- snmp engineId
- snmp option

snmp

stat snmp

Synopsis

stat snmp [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display the statistics related to SNMP.

Example

stat snmp

snmp community

[add | rm | show]

add snmp community

Synopsis

add snmp community <communityName> <permissions>

Description

Add an SNMP community. An SNMP community is a password (string) used to authenticate SNMP queries from SNMP managers. You can associate it with any of the following SNMP query types on the NetScaler appliance: - GET - GET NEXT - ALL - GET BULK You can associate one or more community strings with each query type. For example, if you associate two community strings, such as Example and Test, with the query type GET NEXT, the NetScaler appliance considers only those GET NEXT SNMP query packets that contain Example or Test as the community string.

Parameters

communityName

The SNMP community string. Can consist of 1 to 31 characters that include letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

permissions

The SNMP V1 or V2 query-type privilege that you want to associate with this SNMP community. Possible values: GET, GET_NEXT, GET_BULK, ALL

Example

add snmp community public ALL
add snmp community a#12ab GET_BULK

Top

rm snmp community

Synopsis

rm snmp community <communityName>

Description

Remove an SNMP community from the NetScaler appliance. After you remove the SNMP community, the appliance does not respond to any SNMP queries that contain that community string.

Parameters

communityName

The name of the SNMP community that you want to remove from the NetScaler appliance.

Example

rm snmp community public

Top

show snmp community

Synopsis

show snmp community [<communityName>]

Description

Display the SNMP v1 or v2 query type privileges, such as GET, GET NEXT, ALL, or GET BULK, set for all SNMP communities, or for the specified SNMP community. To display the settings of all the SNMP communities, run the command without any parameters. To display the settings of a particular SNMP community, specify the name of the SNMP community.

Parameters

communityName

The name of the SNMP community whose SNMP v1 or v2 query type privilege setting, such as GET, GET NEXT, ALL, or GET BULK, you want the NetScaler appliance to display. This parameter is required for identifying the community.

Example

show snmp community

Top

snmp manager

[add | rm | set | unset | show]

add snmp manager

Synopsis

add snmp manager <IPAddress> ... [-netmask <netmask>] [-domainResolveRetry <integer>]

Description

Add an SNMP manager to query the NetScaler appliance. The added manager complies with SNMP version 1, version 2, and version 3. If you do not configure at least one SNMP manager, the NetScaler appliance accepts and responds to SNMP queries from all hosts on the network. If you add one or more SNMP managers on the NetScaler appliance, the appliance does not accept SNMP queries from any hosts except the SNMP managers. You can add up to a maximum of 100 IP based SNMP managers or networks and a maximum of 5 host-name based SNMP managers.

Parameters

IPAddress

The IPv4 or network address or the host name of the SNMP manager that you want to add to the NetScaler appliance. Can be any of the following: - IPv4 address of the SNMP manager. - IPv4 network address. The NetScaler appliance accepts and responds to SNMP queries from any device on this network. - Associated host-name of an SNMP manager that has an IPv4 address. If you specify a host-name, you must add a DNS name server that resolves the host-name of the SNMP manager to its IP address. You can add up to a maximum of 100 IP based SNMP managers or networks and a maximum of 5 host-name-based SNMP managers.

netmask

The subnet mask associated with the IPv4 network address specified by the IPAddress parameter. If the IPAddress parameter specifies a specific host, which is IP address or host name of the SNMP manager, accept the default value of 255.255.255.255 for the netmask parameter. Default value: 0xFFFFFFFF

domainResolveRetry

The amount of time, in seconds, for which the NetScaler appliance waits before sending another DNS query to resolve the host-name of the SNMP manager if the last query failed. After a query succeeds, the appliance waits for the TTL time. This parameter is only valid for host-name based SNMP managers. Minimum value: 5 Maximum value: 20939

Example

```
add snmp manager 192.168.1.20 192.168.2.42
add snmp manager 192.168.2.16 -netmask 255.255.255.240
add snmp manager hostnamemanager.com
```

Top

rm snmp manager

Synopsis

rm snmp manager <IPAddress> ... [-netmask <netmask>]

Description

Remove an SNMP manager from the list of managers that are allowed to access the NetScaler appliance.

Parameters

IPAddress

The IPv4 or network address or the host name of the SNMP manager that you want to remove from the NetScaler appliance.

netmask

The subnet mask associated with the SNMP manager entry. If the IPAddress parameter specifies a specific host, which is IP address or host name of the SNMP manager, the subnet mask is 255.255.255.255. Default value: 0xFFFFFFFF

Example

```
rm snmp manager 192.168.1.20
rm snmp manager 192.168.2.16 -netmask 255.255.255.240
rm snmp manager hostnamemanager.com
```

Top

set snmp manager

Synopsis

set snmp manager <IPAddress> [-netmask <netmask>] [-domainResolveRetry <integer>]

Description

Modify the domain resolve retry parameter of any host-name based SNMP managers specified on the NetScaler appliance.

Parameters

IPAddress

The host name of the SNMP manager for which you want to modify the domain resolve retry parameter.

netmask

The subnet mask associated with the SNMP manager entry. If the IPAddress parameter specifies a specific host, which is IP address or host name of the SNMP manager, the subnet mask is 255.255.255.255. Default value: 0xFFFFFFFF

domainResolveRetry

The amount of time, in seconds, for which the NetScaler appliance waits before sending another DNS query to resolve the host-name of the SNMP manager if the last query failed. After a query succeeds, the appliance waits for the TTL time. This parameter is only valid for host-name based SNMP managers. Minimum value: 5 Maximum value: 20939

Example

set snmp manager www.example.com -domainResolveRetry 7

Top

unset snmp manager

Synopsis

unset snmp manager <IPAddress> -netmask <netmask> -domainResolveRetry

Description

Use this command to remove snmp manager settings.Refer to the set snmp manager command for meanings of the arguments.

Top

show snmp manager

Synopsis

show snmp manager [<IPAddress> [-netmask <netmask>]]

Description

Display the configuration details of SNMP managers on the NetScaler appliance. The SNMP managers can be IPv4 or network address or host-name based. IPv4 or network-address based managers are listed by the following respective settings: - IP address - Subnet mask Host-name based SNMP manager are listed by the following respective setting: - Host name - Resolve-retry - Resolved-IP address For IPv4 or network-address based managers, resolved-IP address and host name are irrelevant. For a host-name based SNMP manager, IP address is irrelevant.

Parameters

IPAddress

The IPv4 or network address or the host name of the SNMP manager. This parameter is required for identifying the SNMP manager entry.

Example

show snmp manager

Top

snmp trap

[add | rm | set | unset | show]

add snmp trap

Synopsis

add snmp trap <trapClass> <trapDestination> ... [-version (V1 | V2)] [-destPort <port>] [-communityName <string>] [-srcIP <ip_addr|ipv6_addr>] [-severity <severity>]

Description

Add an SNMP trap listener. You can configure the NetScaler appliance to generate asynchronous events (trap messages) to report abnormal conditions. The trap messages are sent to a remote device (trap listener) to help administrators monitor the appliance and respond promptly to any issues. The NetScaler appliance provides a set of condition entities called SNMP alarms. When the condition in any SNMP alarm is met, the appliance sends an SNMP trap message to the configured trap listener. For example, if the LOGIN-FAILURE alarm is enabled, a trap message is sent whenever an attempt to log on to the NetScaler appliance fails.

Parameters

trapClass

The type of trap messages that you want the NetScaler appliance to send to this trap listener. There are two types: Generic. Send standard system SNMP traps messages, such as authenticationfailure, linkDown, linkUp, and, coldStart traps, to the trap listener. Specific. Send enterprise specific trap messages to the trap listener. The MIB file of the NetScaler appliance contains the definitions of all the enterprise specific traps. For more information about the enterprise specific traps, see the SNMP OID reference guide for this release of the NetScaler software. Possible values: generic, specific

trapDestination

The IPv4 or the IPv6 address of the trap listener to which you want the NetScaler appliance to send the SNMP trap messages.

version

The SNMP version, which determines the format of trap messages received by this trap listener. Possible values: V1, V2 Default value: TRAP_VERSION_2

destPort

The UDP port of this trap listener to which the NetScaler appliance send the SNMP trap messages. You must specify the same port number on the trap listener device. Otherwise, the trap listener drops the trap messages. Default value: 162 Minimum value: 1 Maximum value: 65534

communityName

A password (string) sent with the traps messages, which is used to authenticate the trap messages on the trap listener. Can consist of 1 to 31 characters that include letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You must specify the same community string on the trap listener device. Otherwise, the trap listener drops the trap messages. Default value: "public"

srcIP

The IPv4 or IPv6 address that the NetScaler appliance inserts as the source IP address in all SNMP trap messages that it sends to this trap listener. For a trap listener that has an IPv4 address, you can set the source IP to either a mapped IP (MIP) address or a subnet IP (SNIP) address configured on the NetScaler appliance. By default, the appliance uses the NSIP address as the source IP address. For a trap listener that has an IPv6 address, you can set the source IP address to any subnet IPv6 (SNIP6) address configured on the appliance. By default, the appliance uses the NSIP6 address as the source IP address.

severity

The severity level at or above which the NetScaler appliance sends trap messages to this trap listener. Following are the severity levels defined on the NetScaler appliance, in increasing order of severity. - Informational - Warning - Minor - Major - Critical For example, if you set the severity level as Minor, all trap messages with a severity level of Minor, Major, or Critical are sent to the trap listener. This parameter can only be set for specific trap listeners. By default, all levels of generated SNMP traps messages are sent to a trap listener. Important: Trap messages are not assigned severity levels unless you specify severity levels when configuring SNMP alarms. For example, if you specify a severity level as Warning for the SNMP alarm named LOGIN-FAILURE, a trap message generated as a result of login failure is assigned the Warning severity level. Possible values: Critical, Major, Minor, Warning, Informational Default value: SNMP_SEV_UNKNOWN

Top

rm snmp trap

Synopsis

rm snmp trap <trapClass> <trapDestination> ...

Description

Remove a trap listener entry from the NetScaler appliance.

Parameters

trapClass

The trap type specified in the trap listener entry that you want to remove. Possible values: generic, specific

trapDestination

The IP address of the trap listener specified in the trap listener entry that you want to remove.

Top

set snmp trap

Synopsis

set snmp trap <trapClass> <trapDestination> [-destPort <port>] [-version (V1 | V2)] [-communityName <string>] [-srcIP <ip_addr|ipv6_addr>] [-severity <severity>]

Description

Modify certain parameters for configured trap listeners.

Parameters

trapClass

The type of trap specified in the trap listener entry that you want to modify. This parameter is required for identifying the trap listener entry and cannot be modified. Possible values: generic, specific

trapDestination

The IP address of the trap listener specified in the trap listener that you want to modify. This parameter is required for identifying the trap listener entry and cannot be modified.

destPort

The UDP port of this trap listener to which the NetScaler appliance send the SNMP trap messages. You must specify the same port number on the trap listener device. Otherwise, the trap listener drops the trap messages. Default value: 162 Minimum value: 1 Maximum value: 65534

version

The SNMP version, which determines the format of trap messages received by this trap listener. Possible values: V1, V2 Default value: TRAP_VERSION_2

communityName

A password (string) sent with the traps messages, which is used to authenticate the trap messages on the trap listener. Can consist of 1 to 31 characters that include letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You must specify the same community string on the trap listener device. Otherwise, the trap listener drops the trap messages. Default value: "public"

srcIP

The IPv4 or IPv6 address that the NetScaler appliance inserts as the source IP address in all SNMP trap messages that it sends to this trap listener. For a trap listener that has an IPv4 address, you can set the source IP to either a mapped IP (MIP) address or a subnet IP (SNIP) address configured on the NetScaler appliance. By default, the appliance uses the NSIP address as the source IP address. For a trap listener that has an IPv6 address, you can set the source IP address to any subnet IPv6 (SNIP6) address configured on the appliance. By default, the appliance uses the NSIP6 address as the source IP address.

severity

The minimum severity of the alarms to be sent to the trap destination. Possible values: Critical, Major, Minor, Warning, Informational Default value: SNMP_SEV_UNKNOWN

Example

set snmp trap generic 192.168.3.4 -version V1

Top

unset snmp trap

Synopsis

unset snmp trap <trapClass> <trapDestination> [-destPort] [-version] [-communityName] [-srcIP] [-severity]

Description

Reset certain parameters of a trap listener entry to the default settings..Refer to the set snmp trap command for meanings of the arguments.

Example

unset snmp trap generic 192.168.3.4 -version

Top

show snmp trap

Synopsis

show snmp trap [<trapClass> <trapDestination>]

Description

Display the settings of all trap listeners or of the specified trap listener. To display the settings of all the trap listeners, run the command without any parameters. To display the settings of a particular trap listener, specify the trapClass (trap type) and trapDestination (IP address) of the trap listener.

Parameters

trapClass

The trap type specified in the trap listener entry whose details you want the NetScaler appliance to display. This parameter is required for identifying the trap listener entry. Possible values: generic, specific

Example

show snmp trap

Top

snmp group

[add | rm | set | show]

add snmp group

Synopsis

add snmp group <name> <securityLevel> -readViewName <string>

Description

Add an SNMP user group on the NetScaler appliance. SNMP groups are logical aggregations of SNMP users. SNMP groups are used to implement access control and define the security levels for the users. You can add a maximum of 1000 SNMP groups to the NetScaler appliance.

Parameters

name

A name for the SNMP group. Can begin and consist of 1 to 31 characters that include letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the SNMP group.

securityLevel

The security level of the group. The following options are available: noAuthNoPriv. Neither authentication nor encryption is required for the communication between the SNMP user belonging to this group and the NetScaler appliance. authNoPriv. Authetication is required but no encryption for the communication between the SNMP user belonging to this group and the NetScaler appliance. You must set an authentication algorithm while configuring the SNMP users that belong to this group. authPriv. Authetication as well as encryption is required for the communication between the SNMP user belonging to this group and the NetScaler appliance. You must set an authentication and an encryption algorithm while configuring the SNMP users that belong to this group. Possible values: noAuthNoPriv, authNoPriv, authPriv

readViewName

The name of the configured SNMP view that you want to bind to this SNMP group. An SNMP user bound to this group can access the subtrees that are bound to this SNMP view as type INCLUDED but cannot access the ones that are type EXCLUDED. If the NetScaler appliance has multiple SNMP view entries with the same name, all such entries are associated with the SNMP group.

Top

rm snmp group

Synopsis

rm snmp group <name> <securityLevel>

Description

Remove an SNMP group entry from the NetScaler appliance. The appliance can have multiple SNMP groups with the same name, differentiated by the securityLevel parameter setting. Therefore, to identify an SNMP group entry that you want to remove, you have to specify both the name and security level of the SNMP group.

Parameters

name

The name of the SNMP group that you want to remove from the NetScaler appliance.

securityLevel

The security level of the SNMP group that you want to remove from the NetScaler appliance. Possible values: noAuthNoPriv, authNoPriv, authPriv

Top

set snmp group

Synopsis

set snmp group <name> <securityLevel> -readViewName <string>

Description

Modify certain parameters of an SNMPv3 group entry on the NetScaler appliance.

Parameters

name

The name specified in the SNMP group entry that you want to modify. This parameter is required for identifying the SNMP group and cannot be modified.

securityLevel

The security level of the group. The following options are available: noAuthNoPriv. Neither authentication nor encryption is required for the communication between the SNMP user belonging to this group and the NetScaler appliance. authNoPriv. Authetication is required but no encryption for the communication between the SNMP user belonging to this group and the NetScaler appliance. You must set an authentication algorithm while configuring the SNMP users that belong to this group. authPriv. Authetication as well as encryption is required for the communication between the SNMP user belonging to this group and the NetScaler appliance. You must set an authentication and an encryption algorithm while configuring the SNMP users that belong to this group. Possible values: noAuthNoPriv, authNoPriv, authPriv

readViewName

The name of the configured SNMP view that you want to bind to this SNMP group. An SNMP user bound to this group can access the subtrees that are bound to this SNMP view as type INCLUDED but cannot access the ones that are type EXCLUDED. If the NetScaler appliance has multiple SNMP view entries with the same name, all such entries are associated with the SNMP group.

Top

show snmp group

Synopsis

show snmp group [<name> <securityLevel>]

Description

Display the settings of all SNMP groups or of the specified SNMP group. To display the settings of all the SNMP groups, run the command without any parameters. To display the settings of a particular SNMP group, specify the name of the SNMP group and securityLevel. The NetScaler appliance can have multiple SNMP groups with the same name differentiated by the securityLevel (security level) parameter setting.

Parameters

name

The name of the SNMP group whose details you want the NetScaler appliance to display. This parameter is required for identifying the SNMP group.

securityLevel

The security level type specified for the SNMP group whose details you want the NetScaler appliance to display. This parameter is required for identifying the SNMP group. Possible values: noAuthNoPriv, authNoPriv, authPriv

Top

snmp view

[add | rm | set | show]

add snmp view

Synopsis

add snmp view <name> <subtree> -type (included | excluded)

Description

Use this command to add an snmp view.

Parameters

name

A name for the SNMP view. Can begin and consist of 1 to 31 characters that include letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the SNMP view.

subtree

A particular branch (subtree) of the MIB tree that you want to associate with this SNMP view. You must specify the subtree as an SNMP OID.

type

Include or exclude the subtree, specified in the subtree parameter, to or from this view. This setting can be useful when you have included a subtree, such as A, in an SNMP view and you want to exclude a specific subtree of A, such as B, from the SNMP view. Possible values: included, excluded

Top

rm snmp view

Synopsis

rm snmp view <name> <subtree>

Description

Remove an SNMP view entry from the NetScaler appliance. The appliance can have multiple SNMP views with the same name, differentiated by the subtree parameter setting. Therefore, to identify an SNMP group subtree that you want to remove, you have to specify both the name and subtree of the SNMP view.

Parameters

name

The name of the SNMP view that you want to remove from the NetScaler appliance.

subtree

The MIB subtree of the SNMP view entry that you want to remove from the NetScaler appliance.

Top

set snmp view

Synopsis

set snmp view <name> <subtree> -type (included | excluded)

Description

Modify the type parameter of an SNMP view configured on the NetScaler appliance.

Parameters

name

The name specified in the SNMP view entry for which you want to modify the type parameter. This parameter is required for identifying the SNMP view entry and cannot be modified.

subtree

The subtree of the MIB tree specified in the SNMP view entry for which you want to modify the type parameter. This parameter is required for identifying the SNMP view entry and cannot be modified.

type

Include or exclude the subtree, specified in the subtree parameter, to or from this view. This setting can be useful when you have included a subtree, such as A, in an SNMP view and you want to exclude a specific subtree of A, such as B, from the SNMP view. Possible values: included, excluded

Top

show snmp view

Synopsis

show snmp view [<name> [<subtree>]]

Description

Display the settings of all SNMP views or of the specified SNMP view. To display the settings of all the SNMP views, run the command without any parameters. To display the settings of a particular SNMP view, specify the name of the SNMP view and subtree (the associated subtree of the MIB). The NetScaler appliance can have multiple SNMP views with the same name, differentiated by the subtree parameter settings.

Parameters

name

The name of the SNMP view whose details you want the NetScaler appliance to display. This parameter is required for identifying the SNMP view.

Top

snmp user

[add | rm | set | unset | show]

add snmp user

Synopsis

add snmp user <name> -group <string> [-authType (MD5 | SHA) {-authPasswd } [-privType (DES | AES) {-privPasswd }]]

Description

Add an SNMPv3 user who can send SNMP queries to the NetScaler appliance. You can add a maximum of 1000 SNMP users.

Parameters

name

A name for the SNMP user. Can begin and consist of 1 to 31 characters that include letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

group

The name of the configured SNMP group to which you want to bind this SNMP user. The access rights (bound SNMP views) and security level set for this group are associated to this user.

authType

The authentication algorithm used by the NetScaler appliance and the SNMP user for authenticating the communication between them. You must set the same authentication algorithm while configuring the SNMP user in the SNMP manager. Possible values: MD5, SHA

privType

The encryption algorithm used by the NetScaler appliance and the SNMP user for encrypting the communication between them. You must set the same encryption algorithm while configuring the SNMP user in the SNMP manager. Possible values: DES, AES

Top

rm snmp user

Synopsis

rm snmp user <name>

Description

Remove an SNMP user entry from the NetScaler appliance.

Parameters

name

The name of the SNMP user that you want to remove from the NetScaler appliance.

Top

set snmp user

Synopsis

set snmp user <name> [-group <string>] [-authType (MD5 | SHA) {-authPasswd }] [-privType (DES | AES) {-privPasswd }]

Description

Modify certain parameters of an SNMPv3 user entry on the NetScaler appliance.

Parameters

name

The name specified in the SNMP user entry that you want to modify. This parameter is required for identifying the SNMP user and cannot be modified.

group

The name of the configured SNMP group to which you want to bind this SNMP user. The access rights (bound SNMP views) and security level set for this group are associated to this user.

authType

The authentication algorithm used by the NetScaler appliance and the SNMP user for authenticating the communication between them. You must set the same authentication algorithm while configuring the SNMP user in the SNMP manager. Possible values: MD5, SHA

privType

The encryption algorithm used by the NetScaler appliance and the SNMP user for encrypting the communication between them. You must set the same encryption algorithm while configuring the SNMP user in the SNMP manager. Possible values: DES, AES

Top

unset snmp user

Synopsis

unset snmp user <name> (-authType | -privType) [-authPasswd] [-privPasswd]

Description

Reset certain parameters of an SNMPv3 user entry to their default settings..Refer to the set snmp user command for meanings of the arguments.

Top

show snmp user

Synopsis

show snmp user [<name>]

Description

Display the settings of all SNMP users or of the specified SNMP user. To display the settings of all the SNMP users, run the command without any parameters. To display the settings of a particular SNMP user, specify the name of the SNMP user.

Parameters

name

The name of the SNMP user whose details you want the NetScaler appliance to display. This parameter is required for identifying the SNMP user.

Top

snmp oid

show snmp oid

Synopsis

show snmp oid <entityType> [<name>]

Description

Display the corresponding SNMP OIDs for the virtual servers, services, and service groups configured on the NetScaler appliance. To display the SNMP OID of all entities of a particular type, such as virtual servers, run the command with only that entity type specified. To display the SNMP of a particular entity, specify the entity type and the entity name.

Parameters

entityType

The type of entity whose SNMP OIDs you want the NetScaler appliance to display. Possible values: VSERVER, SERVICE, SERVICEGROUP

name

The name of the entity whose SNMP OID you want the NetScaler appliance to display.

Example

show snmp oid VSERVER vs1

snmp stats

show snmp stats

Synopsis

show snmp stats - alias for 'stat snmp'

Description

show snmp stats is an alias for stat snmp

snmp alarm

[set | unset | enable | disable | show]

set snmp alarm

Synopsis

set snmp alarm <trapName> [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-time <secs>] [-state (ENABLED | DISABLED)] [-severity <severity>] [-logging (ENABLED | DISABLED)]

Description

The NetScaler appliance provides a set of condition entities called SNMP alarms. When the condition in any SNMP alarm is met, the appliance generates SNMP trap messages that are sent to the configured trap listeners. This mechanism helps administrators monitor the NetScaler appliance and respond promptly to any issues. For example, when the LOGIN-FAILURE alarm is enabled, a trap message is generated and sent to the trap listener whenever an attempt to log on to NetScaler appliance fails. The SNMP alarms are either event based or threshold based. For each configured threshold based alarm, an SNMP trap message is sent when the value exceeds the specified high threshold. When the value falls below the normal threshold, another SNMP trap is sent to indicate a return-to-normal state. The NetScaler appliance supports the following user configurable alarms:

HA-STATE-CHANGE: Change to primary/secondary

CPU-USAGE: Individual CPU usage

AVERAGE-CPU: Average CPU usage

MGMT-CPU: Management CPU usage

ENTITY-STATE: Entity state change

SYNFLOOD: Global unacknowledged SYN count

MEMORY: Memory usage

VSERVER-REQRATE: Vserver specific request rate

SERVICE-REQRATE: Service specific request rate

ENTITY-RXRATE: Entity specific Rx bytes per sec

ENTITY-TXRATE: Entity specific Tx bytes per sec

ENTITY-SYNFLOOD: Entity specific unacknowledged SYN count

CONFIG-CHANGE: System configuration changed

SERVICE-MAXCLIENTS: Service hit max-client limit

CONFIG-SAVE: System configuration was saved

SERVICEGROUP-MEMBER-REQRATE: Request rate on a service group member

SERVICEGROUP-MEMBER-MAXCLIENTS: Service group member hits max-client

MONITOR-RTO-THRESHOLD: Monitor probe response timeout

LOGIN-FAILURE: GUI/CLI/API login failure

SSL-CERT-EXPIRY: Certificate expiry

FAN-SPEED-LOW: Low fan speed

VOLTAGE-LOW: Low voltage

VOLTAGE-HIGH: High Voltage

TEMPERATURE-HIGH: High temperature

CPU-TEMPERATURE-HIGH: High CPU temperature

POWER-SUPPLY-FAILURE: Power supply failure

DISK-USAGE-HIGH: High disk usage

INTERFACE-THROUGHPUT-LOW: Low Interface throughput

MON_PROBE_FAILED: Monitor probe failure

HA-VERSION-MISMATCH: HA netscaler's OS version mismatch

HA-SYNC-FAILURE: HA config synchronization failure

HA-NO-HEARTBEATS: No HA heartbeats

HA-BAD-SECONDARY-STATE: Secondary state DOWN/UNKNOWN/STAY SECONDARY

INTERFACE-BW-USAGE: System aggregate BW usage

RATE-LIMIT-THRESHOLD-EXCEEDED: Client exceed rate-limit threshold

ENTITY-NAME-CHANGE: Entity name change

HA-PROP-FAILURE: HA config propagation failure

IP-CONFLICT: IP conflict

PF-RL-RATE-THRESHOLD: Platform rate limit in Mbps

PF-RL-PPS-THRESHOLD: Platform packets per second limit

PF-RL-RATE-PKTS-DROPPED: Packet Drops due to platform rate limit

PF-RL-PPS-PKTS-DROPPED: Packet Drops due to platform packet per sec limit

APPFW-START-URL: AppFirewall Start URL violation

APPFW-DENY-URL: AppFirewall Deny URL violation

APPFW-REFERER-HEADER: AppFirewall Referer Header violation

APPFW-CSRF-TAG: AppFirewall CSRF Tag violation

APPFW-COOKIE: AppFirewall Cookie violation

APPFW-FIELD-CONSISTENCY: AppFirewall Field Consistency violation

APPFW-BUFFER-OVERFLOW: AppFirewall Buffer Overflow violation

APPFW-FIELD-FORMAT: AppFirewall Field Format violation

APPFW-SAFE-COMMERCE: AppFirewall Safe Commerce violation

APPFW-SAFE-OBJECT: AppFirewall Safe Object violation

APPFW-POLICY-HIT: AppFirewall Policy Hit

APPFW-XSS: AppFirewall Cross Site Scripting violation

APPFW-XML-XSS: AppFirewall XML Cross Site Scripting violation

APPFW-SQL: AppFirewall SQL violation

APPFW-XML-SQL: AppFirewall XML SQL violation

APPFW-XML-ATTACHMENT: AppFirewall XML Attachment violation

APPFW-XML-DOS: AppFirewall XML DoS violation

APPFW-XML-VALIDATION: AppFirewall XML Validation violation

APPFW-XML-WSI: AppFirewall XML WSI violation

APPFW-XML-SCHEMA-COMPILE: AppFirewall XML Schema Compile violation

APPFW-XML-SOAP-FAULT: AppFirewall XML Soap Fault violation

DNSKEY-EXPIRY: DNSKEY expiry

DATASTREAM-RATE-LIMIT-HIT: DataStream Rate Limit Hit

HA-LICENSE-MISMATCH: HA netscaler's license mismatch

SSL-CARD-FAILED: SSL Card Failed

SSL-CARD-NORMAL: SSL Card Normal

WARM-RESTART-EVENT: Warm Restart Event Occurred

HARD-DISK-DRIVE-ERRORS: Hard Disk Drive Errors

COMPACT-FLASH-ERRORS: Compact Flash Errors

CALLHOME-UPLOAD-EVENT: Attempt to upload Show Tech Support Archive

1024KEY-EXCHANGE-RATE: 1024 Key Exchange Rate

2048KEY-EXCHANGE-RATE: 2048 Key Exchange Rate

4096KEY-EXCHANGE-RATE: 4096 Key Exchange Rate

SSL-CUR-SESSION-INUSE: SSL Current Sessions In Use

CLUSTER-NODE-HEALTH: Cluster Node Health State Change

CLUSTER-NODE-QUORUM: Cluster Node View has Quorum

CLUSTER-VERSION-MISMATCH: Cluster Node Version Mismatch

CLUSTER-CCO-CHANGE: Cluster Configuration Coordinator Change

CLUSTER-OVS-CHANGE: Cluster Operational View Set Change

CLUSTER-SYNC-FAILURE: Cluster Config Synchronization Failure

CLUSTER-PROP-FAILURE: Cluster Config Propagation Failure

For the purposes of this command, entity includes vservers and services.

Note: - The NetScaler appliance sends these trap messages only to those trap listeners that are configured as 'Specific'. - Thresholds for SERVICE-MAXCLIENTS should be set with the set service <name> -maxClients <n> command. To configure the NetScaler appliance to generate enterprise specific trap messages, you must enable and configure alarms. Then, you specify the SPECIFIC trap listeners to which the NetScaler sends the generated trap messages.

Parameters

trapName

The name of the SNMP alarm. This parameter is required for identifying the SNMP alarm and cannot be modified.

Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, MGMT-CPU-USAGE, SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE,

INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED, ENTITY-NAME-CHANGE, HA-PROP-FAILURE, IP-CONFLICT, PF-RL-RATE-THRESHOLD, PF-RL-PPS-THRESHOLD, PF-RL-RATE-PKTS-DROPPED, PF-RL-PPS-PKTS-DROPPED, APPFW-START-URL, APPFW-DENY-URL, APPFW-REFERER-HEADER, APPFW-CSRF-TAG, APPFW-COOKIE, APPFW-FIELD-CONSISTENCY, APPFW-BUFFER-OVERFLOW, APPFW-FIELD-FORMAT, APPFW-SAFE-COMMERCE, APPFW-SAFE-OBJECT, APPFW-POLICY-HIT, APPFW-XSS, APPFW-XML-XSS, APPFW-SQL, APPFW-XML-SQL, APPFW-XML-ATTACHMENT, APPFW-XML-DOS, APPFW-XML-VALIDATION, APPFW-XML-WSI, APPFW-XML-SCHEMA-COMPILE, APPFW-XML-SOAP-FAULT, DNSKEY-EXPIRY, DATASTREAM-RATE-LIMIT-HIT, HA-LICENSE-MISMATCH, SSL-CARD-FAILED, SSL-CARD-NORMAL, WARM-RESTART-EVENT, HARD-DISK-DRIVE-ERRORS, COMPACT-FLASH-ERRORS, CALLHOME-UPLOAD-EVENT, 1024KEY-EXCHANGE-RATE, 2048KEY-EXCHANGE-RATE, 4096KEY-EXCHANGE-RATE, SSL-CUR-SESSION-INUSE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-VERSION-MISMATCH, CLUSTER-CCO-CHANGE, CLUSTER-OVS-CHANGE, CLUSTER-SYNC-FAILURE, CLUSTER-PROP-FAILURE

thresholdValue

A value for the high threshold. The NetScaler appliance generates an SNMP trap message when the value of the respective entity is greater than or equal to the specified high threshold value.

Minimum value: 1

time

The interval, in seconds, at which the NetScaler appliance generates SNMP trap messages when the conditions specified in the SNMP alarm are met. This parameter can be specified for the following SNMP alarms: SYNFLOOD, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, APPFW, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM and CLUSTER-VERSION-MISMATCH.

Default value: 1

state

The current state of the SNMP alarm. The NetScaler appliance generates trap messages only for SNMP alarms that are enabled. Some alarms are enabled by default, but you can disable them.

Possible values: ENABLED, DISABLED

Default value: ENABLED

severity

The severity level assigned to trap messages generated by this alarm. The severity levels defined on the NetScaler appliance are, in increasing order of severity, Informational, Warning, Minor, Major, and Critical. For example, if you set a Warning severity level for the SNMP alarm named LOGIN-FAILURE, the trap messages generated when a login attempt fails are assigned the Warning severity level. The default is no severity level, which means that the NetScaler appliance does not assign any severity level to the generated SNMP traps messages. This parameter is useful when you want the NetScaler appliance to send trap messages to a trap listener on the basis of severity level. Trap messages with a severity level lower than the specified level (in the trap listener entry)

are not sent. For example, if you set the severity level as Minor for a trap listener, all trap messages assigned severity level equal to or greater than Minor (Minor, Major, and Critical) are sent to the trap listener.

Possible values: Critical, Major, Minor, Warning, Informational

Default value: SNMP_SEV_UNKNOWN

logging

The logging status of the alarm. When logging is enabled, the NetScaler appliance logs every trap messages that is generated for this alarm.

Possible values: ENABLED, DISABLED

Default value: ENABLED

Example

set snmp alarm VSERVER-REQRATE -thresholdValue 10000 -normalValue 100

Top

unset snmp alarm

Synopsis

unset snmp alarm <trapName> [-thresholdValue] [-normalValue] [-time] [-state] [-severity] [-logging]

Description

Reset certain parameters of an SNMP alarm to their default settings..Refer to the set snmp alarm command for meanings of the arguments.

Example

unset snmp alarm VSERVER-REQRATE

Top

enable snmp alarm

Synopsis

enable snmp alarm <trapName> ...

Description

Enable an SNMP alarm. The NetScaler appliance generates trap messages only for SNMP alarms that are enabled. Some alarms are enabled by default, but you can disable them.

Parameters

trapName

The name of the SNMP alarm that you want to enable. This parameter is required for identifying the SNMP alarm.

Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, MGMT-CPU-USAGE, SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED, ENTITY-NAME-CHANGE, HA-PROP-FAILURE, IP-CONFLICT, PF-RL-RATE-THRESHOLD, PF-RL-PPS-THRESHOLD, PF-RL-RATE-PKTS-DROPPED, PF-RL-PPS-PKTS-DROPPED, APPFW-START-URL, APPFW-DENY-URL, APPFW-REFERER-HEADER, APPFW-CSRF-TAG, APPFW-COOKIE, APPFW-FIELD-CONSISTENCY, APPFW-BUFFER-OVERFLOW, APPFW-FIELD-FORMAT, APPFW-SAFE-COMMERCE, APPFW-SAFE-OBJECT, APPFW-POLICY-HIT, APPFW-XSS, APPFW-XML-XSS, APPFW-SQL, APPFW-XML-SQL, APPFW-XML-ATTACHMENT, APPFW-XML-DOS, APPFW-XML-VALIDATION, APPFW-XML-WSI, APPFW-XML-SCHEMA-COMPILE, APPFW-XML-SOAP-FAULT, DNSKEY-EXPIRY, DATASTREAM-RATE-LIMIT-HIT, HA-LICENSE-MISMATCH, SSL-CARD-FAILED, SSL-CARD-NORMAL, WARM-RESTART-EVENT, HARD-DISK-DRIVE-ERRORS, COMPACT-FLASH-ERRORS, CALLHOME-UPLOAD-EVENT, 1024KEY-EXCHANGE-RATE, 2048KEY-EXCHANGE-RATE, 4096KEY-EXCHANGE-RATE, SSL-CUR-SESSION-INUSE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-VERSION-MISMATCH, CLUSTER-CCO-CHANGE, CLUSTER-OVS-CHANGE, CLUSTER-SYNC-FAILURE, CLUSTER-PROP-FAILURE

Example

```
enable snmp alarm VSERVER-REQRATE
enable snmp alarm CPU SYNFLOOD
```

Top

disable snmp alarm

Synopsis

disable snmp alarm <trapName> ...

Description

Disable an SNMP alarm. The NetScaler appliance does not generate trap messages for SNMP alarms that are disabled. Some alarms are enabled by default, but you can disable the same.

Parameters

trapName

The name of the SNMP alarm that you want to disable. This parameter is required for identifying the SNMP alarm.

Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, MGMT-CPU-USAGE, SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED, ENTITY-NAME-CHANGE, HA-PROP-FAILURE, IP-CONFLICT, PF-RL-RATE-THRESHOLD, PF-RL-PPS-THRESHOLD, PF-RL-RATE-PKTS-DROPPED, PF-RL-PPS-PKTS-DROPPED, APPFW-START-URL, APPFW-DENY-URL, APPFW-REFERER-HEADER, APPFW-CSRF-TAG, APPFW-COOKIE, APPFW-FIELD-CONSISTENCY, APPFW-BUFFER-OVERFLOW, APPFW-FIELD-FORMAT, APPFW-SAFE-COMMERCE, APPFW-SAFE-OBJECT, APPFW-POLICY-HIT, APPFW-XSS, APPFW-XML-XSS, APPFW-SQL, APPFW-XML-SQL, APPFW-XML-ATTACHMENT, APPFW-XML-DOS, APPFW-XML-VALIDATION, APPFW-XML-WSI, APPFW-XML-SCHEMA-COMPILE, APPFW-XML-SOAP-FAULT, DNSKEY-EXPIRY, DATASTREAM-RATE-LIMIT-HIT, HA-LICENSE-MISMATCH, SSL-CARD-FAILED, SSL-CARD-NORMAL, WARM-RESTART-EVENT, HARD-DISK-DRIVE-ERRORS, COMPACT-FLASH-ERRORS, CALLHOME-UPLOAD-EVENT, 1024KEY-EXCHANGE-RATE, 2048KEY-EXCHANGE-RATE, 4096KEY-EXCHANGE-RATE, SSL-CUR-SESSION-INUSE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-VERSION-MISMATCH, CLUSTER-CCO-CHANGE, CLUSTER-OVS-CHANGE, CLUSTER-SYNC-FAILURE, CLUSTER-PROP-FAILURE

Example

```
disable snmp alarm VSERVER-REQRATE
disable snmp alarm CPU SYNFLOOD
```

Top

show snmp alarm

Synopsis

show snmp alarm [<trapName>]

Description

Display the settings of all SNMP alarms or of the specified SNMP alarm. To display the settings of all the SNMP alarms, run the command without any parameters. To display the settings of a particular SNMP alarm, specify the trapName (alarm name) of the SNMP alarm.

Parameters

trapName

The name of the SNMP alarm whose details you want the NetScaler appliance to display. This parameter is required for identifying the SNMP alarm.

Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, MGMT-CPU-USAGE, SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED, ENTITY-NAME-CHANGE, HA-PROP-FAILURE, IP-CONFLICT, PF-RL-RATE-THRESHOLD, PF-RL-PPS-THRESHOLD, PF-RL-RATE-PKTS-DROPPED, PF-RL-PPS-PKTS-DROPPED, APPFW-START-URL, APPFW-DENY-URL, APPFW-REFERER-HEADER, APPFW-CSRF-TAG, APPFW-COOKIE, APPFW-FIELD-CONSISTENCY, APPFW-BUFFER-OVERFLOW, APPFW-FIELD-FORMAT, APPFW-SAFE-COMMERCE, APPFW-SAFE-OBJECT, APPFW-POLICY-HIT, APPFW-XSS, APPFW-XML-XSS, APPFW-SQL, APPFW-XML-SQL, APPFW-XML-ATTACHMENT, APPFW-XML-DOS, APPFW-XML-VALIDATION, APPFW-XML-WSI, APPFW-XML-SCHEMA-COMPILE, APPFW-XML-SOAP-FAULT, DNSKEY-EXPIRY, DATASTREAM-RATE-LIMIT-HIT, HA-LICENSE-MISMATCH, SSL-CARD-FAILED, SSL-CARD-NORMAL, WARM-RESTART-EVENT, HARD-DISK-DRIVE-ERRORS, COMPACT-FLASH-ERRORS, CALLHOME-UPLOAD-EVENT, 1024KEY-EXCHANGE-RATE, 2048KEY-EXCHANGE-RATE, 4096KEY-EXCHANGE-RATE, SSL-CUR-SESSION-INUSE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-VERSION-MISMATCH, CLUSTER-CCO-CHANGE, CLUSTER-OVS-CHANGE, CLUSTER-SYNC-FAILURE, CLUSTER-PROP-FAILURE

Top

snmp mib

[set | unset | show]

set snmp mib

Synopsis

set snmp mib [-contact <string>] [-name <string>] [-location <string>] [-customID <string>]

Description

Configure the SNMP agent of the NetScaler appliance with information that identifies the appliance, such as the name of the administrator for this NetScaler appliance, a name for the appliance, and the location of the appliance. SNMP managers can query the NetScaler appliance for this information.

Parameters

contact

The name of the administrator for this NetScaler appliance. Along with the name, you can include information on how to contact this person, such as a phone number or an email address. Can begin and consist of 1 to 127 characters that include letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_). Default value: "WebMaster (default)"

name

A name for this NetScaler appliance. Can begin and consist of 1 to 127 characters that include letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the NetScaler appliance. Default value: "NetScaler"

location

The physical location of the NetScaler appliance. For example, you can specify building name, lab number, and rack number. Can begin and consist of 1 to 127 characters that include letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. Default value: "POP (default)"

customID

A custom identification number for the NetScaler appliance. Can begin and consist of 1 to 127 characters that include letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a custom identification that helps identify the NetScaler appliance. Default

value: "Default"

Top

unset snmp mib

Synopsis

unset snmp mib [-contact] [-name] [-location] [-customID]

Description

Use this command to remove snmp mib settings.Refer to the set snmp mib command for meanings of the arguments.

Top

show snmp mib

Synopsis

show snmp mib

Description

Display the information that has been configured on the SNMP agent for the purpose of identifying the NetScaler appliance, such as the name of the appliance, administrator, and location.

Example

show snmp mib

Top

snmp engineId

[set | unset | show]

set snmp engineId

Synopsis

set snmp engineId <engineID>

Description

Modify the SNMPv3 engine identification (ID) on the NetScaler appliance. The SNMPv3 engine has an identification (ID) that uniquely identifies it on the NetScaler appliance. The ID is used in the communication between the SNMPv3 user and the SNMPv3 engine of the NetScaler appliance. The engine ID is pre-configured by Citrix and is based on the MAC address of one of its interfaces. It is not necessary to override the engine ID. However, you can change the engine ID. Note: Changing the ID SNMPv3 engine invalidates the current SNMP users. You have to reconfigure the SNMP users in the SNMP managers.

Parameters

engineID

The unique identification for the SNMPv3 engine. Engine ID should be a hexadecimal value with a minimum length of 10 hex characters.

Top

unset snmp engineId

Synopsis

unset snmp engineId

Description

Reset the SNMPv3 engine identification (ID) on the NetScaler appliance to its default setting. The NetScaler appliance derives the engine ID from the MAC address of one of its interfaces. Note: Changing the ID SNMPv3 engine invalidates the current SNMP users. You have to reconfigure the SNMP users in the SNMP managers..Refer to the set snmp engineId command for meanings of the arguments.

Top

show snmp engineId

Synopsis

show snmp engineId

Description

Display the engine ID of the SNMP agent of the NetScaler appliance.

Top

snmp option

[set | unset | show]

set snmp option

Synopsis

set snmp option [-snmpset (ENABLED | DISABLED)] [-snmpTrapLogging (ENABLED | DISABLED)]

Description

Enable or disable the SNMP options for SNMP SET and SNMP trap logging.

Parameters

snmpset

Accept SNMP SET requests sent to the NetScaler appliance, and allow SNMP managers to write values to MIB objects that are configured for write access. Possible values: ENABLED, DISABLED Default value: DISABLED

snmpTrapLogging

Enable the NetScaler appliance to log any SNMP trap events (for SNMP alarms in which logging is enabled) even when no trap listeners are configured. With the default setting, SNMP trap events are logged if at least one trap listener is configured on the appliance. Possible values: ENABLED, DISABLED Default value: DISABLED

Top

unset snmp option

Synopsis

unset snmp option [-snmpset] [-snmpTrapLogging]

Description

Use this command to remove snmp option settings.Refer to the set snmp option command for meanings of the arguments.

Top

show snmp option

Synopsis

show snmp option

Description

Displays the settings for the following SNMP options for SNMP SET and SNMP trap Logging.

Top

SSL Commands

This group of commands can be used to perform operations on the following entities:

- ssl
- ssl fipsKey
- ssl wrapkey
- ssl certKey
- ssl ciphersuite
- ssl cipher
- ssl crl
- ssl action
- ssl policy
- ssl policylabel
- ssl ocspResponder
- ssl rsakey
- ssl pkcs12
- ssl pkcs8
- ssl dhParam
- ssl dsaKey
- ssl certLink
- ssl certReq
- ssl cert
- ssl stats
- ssl parameter
- ssl fips
- ssl service
- ssl serviceGroup

- ssl vserver
- ssl fipsSIMTarget
- ssl fipsSIMSource
- ssl global

ssl

stat ssl

Synopsis

stat ssl [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display ssl statistics.

ssl fipsKey

[create | rm | show | import | export]

create ssl fipsKey

Synopsis

create ssl fipsKey <fipsKeyName> -modulus <positive_integer> [-exponent (3 | F4)]

Description

Generate a FIPS key within the Hardware Security Module (HSM)-FIPS card.

Parameters

fipsKeyName

The object name for the FIPS key.

modulus

The modulus of the key to be created. The modulus value should be a multiple of 64. Minimum value: 1024 Maximum value: 4096

exponent

The exponent value for the key to be created. 3 : Hex value 0x3 F4 : Hex value 0x10001 Possible values: 3, F4 Default value: 3

Example

create fipskey fips1 -modulus 1024 -exp f4

Top

rm ssl fipsKey

Synopsis

rm ssl fipsKey <fipsKeyName> ...

Description

Remove the specified FIPS key(s) from the system.

Parameters

fipsKeyName

The name of the FIPS key(s) to be removed from the system.

Example

rm fipskey fips1

Top

show ssl fipsKey

Synopsis

show ssl fipsKey [<fipsKeyName>]

Description

Display the information on the FIPS keys configured on the system. If no FIPS key name is specified then the command will list all the FIPS keys configured in the system. If a FIPS key name is specified, the command will display the details of the FIPS key.

Parameters

fipsKeyName

The name of the FIPS key.

Example

1) An example of output of show ssl fipskey command is as follows:
show fipskey
2 FIPS keys:
1) FIPS Key Name: fips1
2) FIPS Key Name: fips2

2) An example of output of show fipskey command with FIPS key name specified is as follows:
show fipskey fips1
FIPS Key Name: fips1 Modulus: 1024 Public Exponent: 3 (Hex: 0x3)

Top

import ssl fipsKey

Synopsis

import ssl fipsKey <fipsKeyName> -key <string> [-inform <inform>] [-wrapKeyName <string>] [-iv <string>] [-exponent (3 | F4)]

Description

Import a key into the Hardware Security Module (HSM) -FIPS card. You can also use this command to import a FIPS key from another System's FIPS system (example Primary system), or for importing a non-FIPS key from an external Web server (Apache/IIS).

Parameters

fipsKeyName

The object name for the FIPS key being imported.

key

The path to the key file. The default input path for the key is /nsconfig/ssl/.

inform

The input format of the key file. SIM: Secure Information Management. This is used when a FIPS key is transferred from one FIPS system to other. DER: Distinguished Encoding Rule. This is used when a non-FIPS key is to be imported inside a FIPS system. The non-FIPS key has to be converted to PKCS#8 form using the CLI command "convert pkcs8". Possible values: SIM, DER, PEM Default value: FORMAT_SIM

wrapKeyName

The object name of the wrapkey to use for importing the key. The wrapkey is created using the CLI command "create ssl wrapkey". This is required if the key being imported is a non-FIPS key.

iv

The Initialization Vector (IV) to use for importing the key. This is required if the key being imported is a non-FIPS key.

exponent

The exponent value for the key to be imported. 3 : Hex value 0x3 F4 : Hex value 0x10001 Possible values: 3, F4 Default value: 3

Example

1) import fipskey fips1 -key /nsconfig/ssl/fipskey.sim
The above example imports a FIPS key stored in the file fipskey.sim in the system.

2) import fipskey fips2 -key /nsconfig/ssl/key.der -inform DER -wrapKeyName wrapkey1 -iv wrap123
The above example imports a non-FIPS key stored in the file key.der in the system.

Top

export ssl fipsKey

Synopsis

export ssl fipsKey <fipsKeyName> -key <string>

Description

Export a FIPS key from one system to another or to backup the FIPS key in a secure manner. The exported key is secured using a strong asymmetric key encryption methods.

Parameters

fipsKeyName

The name of the FIPS key to be exported.

key

The path and file name to store the exported key. The default output path for the key is /nsconfig/ssl/.

Example

export fipskey fips1 -key /nsconfig/ssl/fips1.key

Top

ssl wrapkey

[create | rm | show]

create ssl wrapkey

Synopsis

create ssl wrapkey <wrapKeyName> {-password } {-salt }

Description

Generate a wrap key.

Parameters

wrapKeyName

The object name for the wrap key.

password

The password string for the wrap key.

salt

The salt string for the wrap key.

Example

create wrapkey wrap1 -password wrapkey123 -salt wrapsalt123

Top

rm ssl wrapkey

Synopsis

rm ssl wrapkey <wrapKeyName> ...

Description

Remove the specified wrapkey(s) from the system.

Parameters

wrapKeyName

The name of the wrapkey(s) to be removed from the system.

Example

rm wrapkey wrap1

Top

show ssl wrapkey

Synopsis

show ssl wrapkey

Description

Display the wrap keys.

Example

An example of output of 'show wrapkey' command is as shown below:
sh wrapkey
1 WRAP key:
1) WRAP Key Name: wrap1

Top

ssl certKey

[add | rm | set | unset | bind | unbind | link | unlink | show | update]

add ssl certKey

Synopsis

add ssl certKey <certkeyName> -cert <string> [(-key <string> [-password]) | -fipsKey <string>] [-inform (DER | PEM)] [-expiryMonitor (ENABLED | DISABLED) [-notificationPeriod <positive_integer>]] [-bundle (YES | NO)]

Description

Add a certificate-key pair object. Notes: 1) For server certificate-key pair, use both -cert and -key arguments. 2) The command ###bind ssl certkey###, used for binding a certificate-key pair to an SSL virtual server, fails if the certificate-key pair does not include the private key. 3) In an HA configuration, the certificate should be located as specified in the -cert <string> parameter, on both the primary and secondary nodes. If the optional parameter -key is used, the key must be located as specified in the -key <string> parameter.

Parameters

certkeyName

The name of the certificate and private-key pair.

cert

The file name and path for the X509 certificate file. The certificate file should be present on the system device (HDD). The default input path for the certificate file is /nsconfig/ssl/.

key

The file name and path for the private-key file. The private-key file should be present on the system device (HDD). The default input path for the key file is /nsconfig/ssl/. Notes: 1) This argument is optional when adding a Certificate-Authority (CA) certificate file. In this case the CA's private-key will not be available to the user. 2) The System's FIPS system does not support external keys (non-FIPS keys). On a System's FIPS system, you will not be able to load keys from a local storage device such as a hard disc or flash memory.

fipsKey

The name of the FIPS key. The FIPS key is created inside the FIPS HSM (Hardware Security Module). This is applicable only to the SSL FIPS system.

inform

The input format of the certificate and the private-key files. The two formats supported by the system are: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

passplain

This is mostly used for API purpose.The pass-phrase that was used to encrypt the private-key. This option can be used to load encrypted private-keys. The maximum length of the pass-phrase supported is 32 characters. Note: Password protected private key is supported only for the PEM format.

expiryMonitor

Alert before the certificate is about to expire. Possible values: ENABLED, DISABLED

notificationPeriod

Number of days in advance when an alert needs to be generated for a certificate which is about to expire. Minimum value: 10 Maximum value: 100

bundle

Option to add certificate bundle. Possible values: YES, NO Default value: NO

Example

1) add ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /nsconfig/ssl/pkey.pem
The above command loads a certificate and private key file.
2) add ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /nsconfig/ssl/pkey.pem -password
Password: ********
The above command loads a certificate and private key file. Here the private key file is an encrypted key.
3) add ssl certkey fipscert -cert /nsconfig/ssl/cert.pem -fipskey fips1024
The above command loads a certificate and associates it with the corresponding FIPS key that resides within

Top

rm ssl certKey

Synopsis

rm ssl certKey <certkeyName> ...

Description

Remove the specified certificate-key pair from the system.

Parameters

certkeyName

The name of the certificate-key pair. Note: The certificate-key pair is removed only when it is not referenced by any other object. The reference count is updated when the certificate-key pair is bound to an SSL virtual server (using the ###bind ssl certkey### command) or linked to another certificate-key pair (using the ###link ssl certkey### command).

Example

1) rm ssl certkey siteAcertkey
The above command removes the certificate-key pair siteAcertkey from the system.

Top

set ssl certKey

Synopsis

set ssl certKey <certkeyName> [-expiryMonitor (ENABLED | DISABLED) [-notificationPeriod <positive_integer>]]

Description

Change attributes of a certificate-key pair object.

Parameters

certkeyName

The name of the certificate and private-key pair.

expiryMonitor

Alert before the certificate is about to expire. Possible values: ENABLED, DISABLED

Top

unset ssl certKey

Synopsis

unset ssl certKey <certkeyName> [-expiryMonitor] [-notificationPeriod]

Description

Use this command to remove ssl certKey settings.Refer to the set ssl certKey command for meanings of the arguments.

Top

bind ssl certKey

Synopsis

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <positive_integer>]

Description

Bind a certificate-key pair to an SSL virtual server or an SSL service

Parameters

certkeyName

The object name for the certificate-key pair.

ocspResponder

The name of the OCSP responder to be associated with the CA certificate.

vServerName

The name of the SSL virtual server name to which the certificate-key pair needs to be bound.

serviceName

The name of the SSL service to which the certificate-key pair needs to be bound. Use the ###add service### command to create this service.

serviceGroupName

The name of the SSL service group to which the certificate-key pair needs to be bound. Use the "add servicegroup" command to create this service.

CA

If this option is specified, it indicates that the certificate-key pair being bound to the SSL virtual server is a CA certificate. If this option is not specified, the certificate-key pair is bound as a normal server certificate. Note: In case of a normal server certificate, the certificate-key pair should consist of both the certificate and the private-key.

Example

1) bind ssl certkey cacert -ocspResponder ocsp_ca -priority 1
In the above example, the CA certificate cacert is bound with the OCSP responder ocsp_ca with priority 1, w

Top

unbind ssl certKey

Synopsis

unbind ssl certKey <certkeyName> -ocspResponder <string>

Description

Unbind the certificate-key pair from the specified SSL vserver or SSL service. Use the "bind ssl certkey " command to bind the certificate-key pair to the specified SSL vserver or SSL service.

Parameters

certkeyName

The object name for the certificate-key pair.

ocspResponder

OCSP responders bound to this certkey

vServerName

The name of the SSL virtual server.

serviceName

The name of the SSL service

serviceGroupName

The name of the service group.

CA

The certificate-key pair being unbound is a Certificate Authority (CA) certificate. If you choose this option, the certificate-key pair is unbound from the list of CA certificates that were bound to the specified SSL virtual server or SSL service.

Example

1) unbind ssl certkey sslvip siteAcertkey
In the above example, the server certificate siteAcertkey is unbound from the SSL virtual server.
2) unbind ssl certkey sslvip CAcertkey -CA
In the above example, the CA certificate CAcertkey is unbound from the SSL virtual server.

Top

link ssl certKey

Synopsis

link ssl certKey <certkeyName> <linkCertKeyName>

Description

Link a certificate-key pair to its Certificate Authority (CA) certificate-key pair. Note: The two certificate-key pairs are linked only if the certificate specified in the certKeyName parameter is issued by the Certificate-Authority specified in the linkCertKeyName parameter.

Parameters

certkeyName

The certificate-key name that is to be bound to its issuer certificate-key pair.

linkCertKeyName

The name of the Certificate-Authority.

Example

1) link ssl certkey siteAcertkey CAcertkey
In the above example, the certificate-key siteAcertkey is bound to its issuer certificate-key pair CAcertkey.

Top

unlink ssl certKey

Synopsis

unlink ssl certKey <certkeyName>

Description

Unlink the certificate-key name from its Certificate-Authority (CA) certificate-key pair.

Parameters

certkeyName

The certificate-key object name that has to be unlinked from the CA certificate. The CA certificate name is taken internally.

Example

1) unlink ssl certkey siteAcertkey
The above example unlinks the certificate 'siteAcertkey' from its Certificate-Authority (CA) certificate.

Top

show ssl certKey

Synopsis

show ssl certKey [<certkeyName>]

Description

Display the information pertaining to the certificate-key pairs configured on the system: 1) If no argument is specified, the command will display all the certificate-key pairs configured on the system. 2) If the certKeyName argument is specified, the command will display the details of the certificate.

Parameters

certkeyName

The certificate-key pair object name.

Example

1) An example of the output of the show ssl certkey command is shown below:
2 configured certkeys:
1) Name: siteAcertkey
Cert Path: /nsconfig/ssl/siteA-cert.pem
Key Path: /nsconfig/ssl/siteA-key.pem
Format: PEM
Status: Valid
2) Name: cert1
Cert Path: /nsconfig/ssl/server_cert.pem
Key Path: /nsconfig/ssl/server_key.pem
Format: PEM
Status: Valid

2) An example of the output of the show ssl certkey siteAcertkey command is shown below:
Name: siteAcertkey Status: Valid
Version: 3
Serial Number: 02
Signature Algorithm: md5WithRSAEncryption
Issuer: /C=US/ST=CA/L=Santa Clara/O=siteA/OU=Tech

Validity
Not Before: Nov 11 14:58:18 2001 GMT
Not After: Aug 7 14:58:18 2004 GMT
Subject: /C=US/ST-CA/L=San Jose/O=CA/OU=Security
Public Key Algorithm: rsaEncryption
Public Key size: 1024

Top

update ssl certKey

Synopsis

update ssl certKey <certkeyName> [-cert <string>] [(-key <string> [-password]) | -fipsKey <string>] [-inform (DER | PEM)] [-noDomainCheck]

Description

Update a certificate-key pair object. Notes: 1) In a HA configuration, the certificate should be located as specified in the -cert <string> parameter, on both the primary and secondary nodes. If the optional parameter -key is used, the key must be located as specified in the -key <string> parameter.

Parameters

certkeyName

The name of the certificate and private-key pair.

cert

The file name and path for the X509 certificate file. The certificate file should be present on the system device (HDD). The default input path for the certificate file is /nsconfig/ssl/.

key

The file name and path for the private-key file. The private-key file should be present on the system device (HDD). The default input path for the key file is /nsconfig/ssl/.

fipsKey

The name of the FIPS key. The FIPS key is created inside the FIPS HSM (Hardware Security Module). This is applicable only to the SSL FIPS system.

inform

The input format of the certificate and the private-key files. The two formats supported by the system are: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

passplain

This is mostly used for API purpose.The pass-phrase that was used to encrypt the private-key. This option can be used to load encrypted private-keys. The maximum length of the pass-phrase supported is 32 characters. Note: Password protected private key is supported only for the PEM format.

noDomainCheck

Specify this option to override the check for matching domain names during certificate update operation

Example

1) update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /nsconfig/ssl/pkey.pem
The above command updates a certificate and private key file.
2) update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /nsconfig/ssl/pkey.pem -password
Password: ********
The above command updates a certificate and private key file. Here the private key file is an encrypted key
3) update ssl certkey mydomaincert
The above command updates the certificate using the same parameters (-cert path/-key path) that it was ac

Top

ssl ciphersuite

show ssl ciphersuite

Synopsis

show ssl ciphersuite [<cipherName>]

Description

Display the details of a cipher, cipher-group, or cipher-alias defined on the system. If no argument is specified, the command displays all the predefined cipher-aliases and user-defined cipher-groups on the system. If a cipher name is specified, the details of the cipher are displayed. If a user defined cipher-group name is specified, all the individual ciphers in the group are displayed along with the individual cipher description. If a system predefined cipher-alias name is specified, all the individual ciphers in the alias are displayed along with the individual cipher description.

Parameters

cipherName

Cipher name.

Example

1) An example of the output of the show ssl cipher SSL3-RC4-MD5 command is as follows:
Cipher Name: SSL3-RC4-MD5
Description: SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
2) This example displays the details of individual ciphers in the system predefinedcipher-alias: SSLv2 (the co
8 configured cipher(s)in alias
1) Cipher Name: SSL2-RC4-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
2) Cipher Name: SSL2-EXP-RC4-MD5
Description: SSLv2 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
3) Cipher Name: SSL2-RC2-CBC-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
4) Cipher Name: SSL2-EXP-RC2-CBC-MD5
Description: SSLv2 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
5) Cipher Name: SSL2-DES-CBC-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5
6) Cipher Name: SSL2-DES-CBC3-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5
7) Cipher Name: SSL2-RC4-64-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=RC4(64) Mac=MD5

ssl cipher

add ssl cipher

Synopsis

add ssl cipher <cipherGroupName>

Description

Create a user-defined cipher group or to add ciphers to an existing group. The cipher group can be used to set the cipher-suite of an SSL virtual server.

Parameters

cipherGroupName

The name of the user-defined cipher group. If the cipher group does not exist on the system, a new group is created with the specified name. The ciphers are added to this group. If a group identified by cipherGroupName already exists on the system, the ciphers are added to it.

cipherAliasName/cipherName/cipherGroupName

The individual cipher name(s), a user-defined cipher group, or a system predefined cipher alias that will be added to the predefined cipher alias that will be added to the group cipherGroupName. If a cipher alias or a cipher group is specified, all the individual ciphers in the cipher alias or group will be added to the user-defined cipher group.

Example

1) add ssl cipher mygroup SSL2-RC4-MD5 SSL2-EXP-RC4-MD5
The above command creates a new cipher-group by the name: mygroup, with the two ciphers SSL2-RC4-M
If a cipher-group by the name: mygroup already exists in system, then the two ciphers is added to the list of

2) add ssl cipher mygroup HIGH MEDIUM
The above command creates a new cipher-group by the name: mygroup, with the ciphers from the cipher
If a cipher-group by the name, mygroup, already exists in system, then the ciphers from the two aliases is ac

Top

bind ssl cipher

Synopsis

bind ssl cipher [<cipherGroupName>@] [-cipherName <string>]

Description

Change the default cipher-suite defined for an SSL virtual server. By default, the predefined cipher alias on the system is bound to all SSL virtual servers. The DEFAULT alias contains all ciphers with encryption strength >=128bit. Note: To view the individual ciphers in the alias DEFAULT, use the show ssl cipher DEFAULT CLI command

Parameters

cipherGroupName

The name of the user-defined cipher group. If the cipher group does not exist on the system, a new group is created with the specified name. The ciphers are added to this group. If a group identified by cipherGroupName already exists on the system, the ciphers are added to it.

vServerName

The name of the SSL virtual server to which the cipher-suite is to be bound.

serviceName

The name of the SSL service name to which the cipher-suite is to be bound.

serviceGroupName

The name of the SSL service name to which the cipher-suite is to be bound.

cipherOperation

The operation that is performed when adding the cipher-suite. Possible cipher operations are: ADD - Appends the given cipher-suite to the existing one configured for the virtual server. REM - Removes the given cipher-suite from the existing one configured for the virtual server. ORD - Overrides the current configured cipher-suite for the virtual server with the given cipher-suite. Possible values: ADD, REM, ORD Default value: 6

cipherAliasName/cipherName/cipherGroupName

A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.

cipherName

A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.

Example

1) bind ssl cipher sslvip ADD SSL3-RC4-SHA
The above example appends the cipher SSL3-RC4-SHA to the cipher-suite already configured for the SSL virtu
2) bind ssl cipher sslvip REM NULL
The above example removes the ciphers identified by the system's predefined cipher-alias -NULL from the ci
3) bind ssl cipher sslvip ORD HIGH
The above example overrides the existing cipher-suite configured for the SSL virtual server with ciphers, hav

Note: The individual ciphers contained in a system predefined cipher-alias can beviewed by using the followi

Top

show ssl cipher

Synopsis

show ssl cipher [<cipherGroupName>]

Description

Display the details of a cipher, cipher-group, or cipher-alias defined on the system. If no argument is specified, the command displays all the predefined cipher-aliases and user-defined cipher-groups on the system. If a cipher name is specified, the details of the cipher are displayed. If a user defined cipher-group name is specified, all the individual ciphers in the group are displayed along with the individual cipher description. If a system predefined cipher-alias name is specified, all the individual ciphers in the alias are displayed along with the individual cipher description.

Parameters

cipherGroupName

The name of cipher group/alias/individual cipher name

Example

1) An example of the output of the show ssl cipher SSL3-RC4-MD5 command is as follows:
Cipher Name: SSL3-RC4-MD5
Description: SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
2) This example displays the details of individual ciphers in the system predefinedcipher-alias: SSLv2 (the co
8 configured cipher(s)in alias
1) Cipher Name: SSL2-RC4-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
2) Cipher Name: SSL2-EXP-RC4-MD5
Description: SSLv2 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
3) Cipher Name: SSL2-RC2-CBC-MD5
Description: SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
4) Cipher Name: SSL2-EXP-RC2-CBC-MD5
Description: SSLv2 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export

```
5) Cipher Name: SSL2-DES-CBC-MD5
   Description: SSLv2 Kx=RSA      Au=RSA  Enc=DES(56)   Mac=MD5
6) Cipher Name: SSL2-DES-CBC3-MD5
   Description: SSLv2 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=MD5
7) Cipher Name: SSL2-RC4-64-MD5
   Description: SSLv2 Kx=RSA      Au=RSA  Enc=RC4(64)   Mac=MD5
```

Top

rm ssl cipher

Synopsis

rm ssl cipher <cipherGroupName>

Description

Remove cipher(s) from a user-defined cipher group. It can also remove an entire cipher group from the system. If there is no cipherName included with the cipherGroupName, the cipher group specified by cipherGroupName is deleted. If there is a cipherName included, the specified cipher(s) are removed from the cipher group.

Parameters

cipherGroupName

The user defined cipher group on the system.

cipherName

The cipher(s) to be removed from the cipher group.

Example

1) rm ssl cipher mygroup SSL2-RC4-MD5
The above example removes the cipher SSL2-RC4-MD5 from the cipher group mygroup.
2) rm ssl cipher mygroup
The above example will remove the cipher group 'mygroup' from the system.

Top

unbind ssl cipher

Synopsis

unbind ssl cipher <cipherGroupName> [-cipherName <string> ...]

Description

Remove cipher(s) from a user-defined cipher group. It can also remove an entire cipher group from the system. If there is no cipherName included with the cipherGroupName, the cipher group specified by cipherGroupName is deleted. If there is a cipherName included, the specified cipher(s) are removed from the cipher group.

Parameters

cipherGroupName

The user defined cipher group on the system.

cipherName

The cipher(s) to be removed from the cipher group.

Example

1) rm ssl cipher mygroup SSL2-RC4-MD5
The above example removes the cipher SSL2-RC4-MD5 from the cipher group mygroup.
2) rm ssl cipher mygroup
The above example will remove the cipher group 'mygroup' from the system.

Top

ssl crl

[add | create | rm | set | unset | show]

add ssl crl

Synopsis

add ssl crl <crlName> <crlPath> [-inform (DER | PEM)] [-refresh (ENABLED | DISABLED)] [-CAcert <string>] [-method (HTTP | LDAP)] [-server <ip_addr|ipv6_addr|*> | -url <URL>] [-port <port>] [-baseDN <string>] [-scope (Base | One)] [-interval <interval>] [-day <integer>] [-time <HH:MM>] [-bindDN <string>] {-password } [-binary (YES | NO)]

Description

Add a Certificate Revocation List (CRL) object. Note: In an HA configuration, the CRL on both the primary and secondary nodes must be present in the location specified by <crlPath>.

Parameters

crlName

The object name for the CRL.

crlPath

The file name and path for the CRL file. The default input path for the CRL is /var/netscaler/ssl/.

inform

The input format of the CRL file. PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

refresh

Enables or disables the auto refresh feature for the CRL identified by the crlName Possible values: ENABLED, DISABLED

CAcert

The corresponding CA certificate that has issued the CRL. This is the System object identifying the CA certificate that is loaded in System. Note: This is a mandatory field when the "-refresh" option is enabled. The CA certificate needs to be installed before loading the CRL.

method

The method for CRL refresh - HTTP or LDAP. Possible values: HTTP, LDAP

server

The IP address of the LDAP server from which the CRLs are to be fetched.

url

URI of the CRL Distribution Point.

port

The port for the LDAP server. Minimum value: 1

baseDN

The baseDN attribute used by LDAP search to query for the attribute certificateRevocationList. Note: It is recommended to use the baseDN attribute over the Issuer Name from the CA certificate for the CRL, if the Issuer-Name fields does not exactly match the LDAP directory structure's DN.

scope

Extent of the search operation on the LDAP server. Base: Exactly the same level as basedn One : One level below basedn Possible values: Base, One Default value: NSAPI_ONESCOPE

interval

The CRL refresh interval. The valid values are monthly, weekly, and daily. This along with the -days and -time option will identify the exact time/time-interval for CRL refresh. -interval NONE can be used to reset previously set interval settings. Possible values: MONTHLY, WEEKLY, DAILY, NONE

day

The purpose of this option varies with the usage of the -interval option. If the -interval option has been set to MONTHLY, the -days option can be used to set a particular day of the month (1-30/31/28) on which the CRL needs to be refreshed. If the -interval option has been set to WEEKLY, the -days option can be used to set a particular day of the week, i.e. 0...6 (Sun=0,Sat=6) on which the CRL needs to be refreshed. The system handles the valid number of days in a Month or Week, if the input value for the corresponding -day option is set incorrectly. If the -interval option has been set to DAILY, the -days parameter is not used. If the -days option is used without the -interval option, it specifies the number of days after which the refresh is to be done. Maximum value: 31

time

Time duration when the crl is to be refreshed w.r.t hours or minutes.

bindDN

The bindDN to be used to access the CRL object in the LDAP repository. This is required if the access to the LDAP repository is restricted, i.e. anonymous access is not allowed.

password

The password to be used to access the CRL object in the LDAP repository. This is required if the access to the LDAP repository is restricted i.e. anonymous access is not allowed.

binary

Set the LDAP based CRL retrieval mode to binary. Possible values: YES, NO Default value: NO

Example

1) add ssl certkey CAcert -cert /nsconfig/ssl/ca_cert.pem
add ssl crl crl_file /var/netscaler/ssl/crl.pem -cacert CAcert
The above command adds a CRL from local storage system (HDD) with no refresh set.
2) add ssl certkey CAcert -cert /nsconfig/ssl/ca_cert.pem
add ssl crl crl_file /var/netscaler/ssl/crl_new.pem -cacert Cacert -refresh ENABLED -server 10.102.1.100 -p
The above command adds a CRL to the system by fetching the CRL from the LDAP server and setting the refr

Top

create ssl crl

Synopsis

create ssl crl <CAcertFile> <CAkeyFile> <indexFile> (-revoke <input_filename> | -genCRL <output_filename>) {-password }

Description

Revoke a certificate or list of certificates or generate a CRL for the list of certificates that are revoked.

Parameters

CAcertFile

Path to the CA certificate file. The default input path for the CA certificate is /nsconfig/ssl/. Maximum value: 63

CAkeyFile

Path to the CA key file. The default input path for the CA key is /nsconfig/ssl/. Maximum value: 63

indexFile

This file contains the serial number of all the certificates that are revoked. This file is created the first time. New certificate revocation will be added to it subsequently. The default input path for the index file is /nsconfig/ssl/. Maximum value: 63

revoke

The certificate file to be revoked. The default input path for the certificate(s) is /nsconfig/ssl/. Maximum value: 63

genCRL

The CRL file to be created. The list of certificates that have been revoked is obtained from the index file. The default output path for the CRL file is /var/netscaler/ssl/. Maximum value: 63

password

The password for the CA key file. Maximum value: 31

Example

1) create crl /nsconfig/ssl/cacert.pem /nsconfig/ssl/cakey.pem /nsconfig/ssl/index.txt -gencrl /var/netsca

Top

rm ssl crl

Synopsis

rm ssl crl <crlName> ...

Description

Remove the specified CRL object from the system.

Parameters

crlName

The name of the CRL object to be removed from the system.

Example

1) rm ssl crl ca_crl
The above CLI command to delete the CRL object ca_crl from the system is.

Top

set ssl crl

Synopsis

set ssl crl <crlName> [-refresh (ENABLED | DISABLED)] [-CAcert <string>] [-server <ip_addr|ipv6_addr|*> | -url <URL>] [-method (HTTP | LDAP)] [-port <port>] [-baseDN <string>] [-scope (Base | One)] [-interval <interval>] [-day <integer>] [-time <HH:MM>] [-bindDN <string>] {-password } [-binary (YES | NO)]

Description

Enable the automatic refresh option on a CRL and set different refresh parameters.

Parameters

crlName

The object name for the CRL.

refresh

The state of the auto refresh feature for the CRL. Possible values: ENABLED, DISABLED

CAcert

The corresponding CA certificate that has issued the CRL. This is the System object identifying the CA certificate that is loaded in System.

server

The IP address of the LDAP server from which the CRLs are to be fetched.

method

The method for CRL refresh. Possible values: HTTP, LDAP

port

The port of the LDAP server. Minimum value: 1

baseDN

The baseDN attribute used by LDAP search to query for the attribute certificateRevocationList. Note: It is recommended to use the baseDN attribute over the Issuer Name from the CA certificate for the CRL, if the Issuer-Name fields does not exactly match the LDAP directory structure's DN.

scope

Extent of the search operation on the LDAP server. Base: Exactly the same level as basedn One : One level below basedn Possible values: Base, One Default value: NSAPI_ONESCOPE

interval

The CRL refresh interval. This option, when used in conjunction with the -days and -time option, can identify the exact time/time-interval for the CRL refresh. -interval NONE can be used to reset previously set interval settings. -interval NOW can be used to force a instantaneous CRL refresh. This is a one time operation. Possible values: MONTHLY, WEEKLY, DAILY, NOW, NONE

day

The purpose of this option varies with the usage of the -interval option. If the -interval option has been set to MONTHLY, the -days option can be used to set a particular day of the month (1-30/31/28) on which the CRL needs to be refreshed. If the -interval option has been set to WEEKLY, the -days option can be used to set a particular day of the week, i.e. 1...7 (Sun=1,Sat=7) on which the CRL needs to be refreshed. Sytem handles the valid number of days in a Month or Week, if the input value for the corresponding -day option is set incorrectly. For -interval daily, the -days parameter is not used. If -days is used without the -interval option, it specifies the number of days after which the refresh is to be performed. Maximum value: 31

time

Time duration when the crl is to be refreshed w.r.t hours or minutes.

bindDN

The bindDN to be used to access the CRL object in the LDAP repository. This is required if the access to the LDAP repository is restricted, i.e. anonymous access is not allowed.

password

The password to be is used to access the CRL object in the LDAP repository. This is required if the access to the LDAP repository is restricted, i.e. anonymous access is not allowed.

binary

Set the LDAP based CRL retrieval mode to binary. Possible values: YES, NO Default value: NO

Example

1) set ssl crl crl_file -refresh ENABLE -interval MONTHLY -days 10 -time 12:00
The above example sets the CRL refresh to every Month, on date=10, and time=12:00hrs.
2) set ssl crl crl_file -refresh ENABLE -interval WEEKLY -days 1 -time 00:10
The above example sets the CRL refresh every Week, on weekday=Monday, and at time 10 past midnight.
3) set ssl crl crl_file -refresh ENABLE -interval DAILY -days 1 -time 12:00
The above example sets the CRL refresh every Day, at 12:00hrs.
4) set ssl crl crl_file -refresh ENABLE -days 10
The above example sets the CRL refresh after every 10 days.
Note: The CRL will be refreshed after every 10 days. The time for CRL refresh will be 00:00 hrs.
5) set ssl crl crl_file -refresh ENABLE -time 01:00
The above example sets the CRL refresh after every 1 hour.
6) set ssl crl crl_file -refresh ENABLE -interval NOW
The above example sets the CRL refresh instantaneously.

Top

unset ssl crl

Synopsis

unset ssl crl <crlName> [-refresh] [-CAcert] [-server] [-method] [-url] [-port] [-baseDN] [-scope] [-interval] [-day] [-time] [-bindDN] [-password] [-binary]

Description

Use this command to remove ssl crl settings.Refer to the set ssl crl command for meanings of the arguments.

Top

show ssl crl

Synopsis

show ssl crl [<crlName>]

Description

Display the information pertaining to the Certificate Revocation Lists (CRL) configured on the system: If the crlName argument is specified, the command displays the details of the CRL. If the crlName argument is not specified, the command displays all the CRLs.

Parameters

crlName

The CRL object name.

Example

1) An example output of the show ssl crl command is as follows:
1 configured CRL(s)
1 Name: ca_crl
CRL Path: /var/netscaler/ssl/cr1.der
Format: DER Cacert: ca_cert
Refresh: DISABLED

2) An example of the output of the show ssl crl ca_crl command is as follows:
Name: ca_crl Status: Valid, Days to expiration: 21
CRL Path: /var/netscaler/ssl/cr1.der
Format: DER CAcert: ca_cert

```
Refresh: DISABLED
Version: 1
Signature Algorithm: md5WithRSAEncryption
Issuer: /C=US/ST=CA/L=santa clara /O=CA/OU=security
Last_update:Dec 21 09:47:16 2001 GMT
Next_update:Jan 20 09:47:16 2002 GMT
Revoked Certificates:
   Serial Number: 01
   Revocation Date:Dec 21 09:47:02 2001 GMT
   Serial Number: 02
   Revocation Date:Dec 21 09:47:02 2001 GMT
```

Top

ssl action

[add | rm | show]

add ssl action

Synopsis

add ssl action <name> [-clientAuth (DOCLIENTAUTH | NOCLIENTAUTH)] [-clientCert (ENABLED | DISABLED) -certHeader <string>] [-clientCertSerialNumber (ENABLED | DISABLED) -certSerialHeader <string>] [-clientCertSubject (ENABLED | DISABLED) -certSubjectHeader <string>] [-clientCertHash (ENABLED | DISABLED) -certHashHeader <string>] [-clientCertIssuer (ENABLED | DISABLED) -certIssuerHeader <string>] [-sessionID (ENABLED | DISABLED) -sessionIDHeader <string>] [-cipher (ENABLED | DISABLED) -cipherHeader <string>] [-clientCertNotBefore (ENABLED | DISABLED) -certNotBeforeHeader <string>] [-clientCertNotAfter (ENABLED | DISABLED) -certNotAfterHeader <string>] [-OWASupport (ENABLED | DISABLED)]

Description

Create a new SSL action.

Parameters

name

The name for the new SSL action.

clientAuth

Set action to do client certificate authentication or no authentication. DOCLIENTAUTH: Perform client certificate authentication. NOCLIENTAUTH: No client certificate authentication. Possible values: DOCLIENTAUTH, NOCLIENTAUTH

clientCert

The state of insertion of the client certificate in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

clientCertSerialNumber

The state of insertion of the client certificate's Serial Number in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

clientCertSubject

The state of insertion of the client certificate's Subject Name in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

clientCertHash

The state of insertion of the client certificate's hash (signature) in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

clientCertIssuer

The state of insertion of the client certificate's Issuer Name in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

sessionID

The state of insertion of the Session-ID in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

cipher

The state of insertion of the cipher details in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

clientCertNotBefore

The state of insertion of the client certificate's Not-Before date in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

clientCertNotAfter

The state of insertion of the client certificate's Not-After in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

OWASupport

The state of Outlook Web-Access support. If the system is in front of an Outlook Web Access (OWA) server, a special header field, 'FRONT-END-HTTPS: ON', needs to be inserted in the HTTP requests going to the OWA server. Note: This parameter is required as the SSL requests (HTTPS) arrives at the back-end Exchange-2000 server on the configured HTTP port (80) instead of arriving at the front-end Exchange 2000 server. Possible values: ENABLED, DISABLED

Example

```
add ssl action certInsert_act -clientCert ENABLED -certHeader CERT
```

Top

rm ssl action

Synopsis

rm ssl action <name>

Description

Remove the specified SSL action.

Parameters

name

The name of the SSL action.

Example

rm ssl action certInsert_act

Top

show ssl action

Synopsis

show ssl action [<name>]

Description

Display the SSL actions.

Parameters

name

The name of the SSL action.

Example

show ssl action
1 Configured SSL action:
1) Name: certInsert_act
Data Insertion Action:
Cert Header: ENABLED Cert Tag: CERT

Top

ssl policy

[add | rm | set | unset | show]

add ssl policy

Synopsis

add ssl policy <name> -rule <expression> [-action <string>] [-undefAction <string>] [-comment <string>]

Description

Add an SSL policy.

Parameters

name

The name for the new SSL policy.

rule

The expression that sets the condition for application of the SSL policy.

reqAction

The name of the action to be performed on the request. Refer to 'add ssl action' command to add a new action. Builtin actions like NOOP, RESET, DROP, CLIENTAUTH and NOCLIENTAUTH are also allowed.

action

The name of the action to be performed on the request. Refer to "add ssl action" command to add a new action. This is a mandatory argument. Actions like NOOP, RESET, DROP, CLIENTAUTH and NOCLIENTAUTH are also allowed.

undefAction

Action to be used by the policy when the rule evaluation turns out to be undefined. The undef action can be NOOP, RESET or DROP

comment

Comments associated with this policy.

Example

add ssl action certInsert_act -clientCert ENABLED -certHeader CERT
add ssl policy certInsert_pol -rule 'HTTP.REQ.URL.STARTSWITH("/secure/")' -reqAction certInsert_act
The above example adds an SSL policy to do Client certificate insertion into the HTTP requests for any web-c

Top

rm ssl policy

Synopsis

rm ssl policy <name>

Description

Remove an SSL policy.

Parameters

name

The name of the SSL policy.

Example

rm ssl policy certInsert_pol

Top

set ssl policy

Synopsis

set ssl policy <name> [-rule <expression>] [-action <string>] [-undefAction <string>] [-comment <string>]

Description

Set a new rule/action/undefAction for existing SSL policy. The rule flow type can change only if: . action and undefAction(if present) are of NEUTRAL flow type

Parameters

name

Name of the SSL policy

rule

Expression to be used by SSL policy. It has to be a boolean PI rule expression.

action

The name of the action to be performed on the request. Refer to "add ssl action" command to add a new action. This is a mandatory argument. Actions like NOOP, RESET, DROP, CLIENTAUTH and NOCLIENTAUTH are also allowed.

undefAction

A SSL action, to be used by the policy when the rule evaluation turns out to be undefined. The undef action can be NOREWRITE, RESET or DROP

comment

Comments associated with this SSL policy.

Example

set ssl policy pol1 -rule "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

Top

unset ssl policy

Synopsis

unset ssl policy <name> [-undefAction] [-comment]

Description

Unset ssl policy arguments.Refer to the set ssl policy command for meanings of the arguments.

Example

unset ssl policy pol1 -undefAction

Top

show ssl policy

Synopsis

show ssl policy [<name>]

Description

Display the created SSL policies.

Parameters

name

The name of the SSL policy.

Example

```
show ssl policy
1 SSL policy:
1)      Name: certInsert_pol    Rule: URL == /*
       Action: certInsert_act      Hits: 0
```

Top

ssl policylabel

[add | rm | bind | unbind | show]

add ssl policylabel

Synopsis

add ssl policylabel <labelName> -type (CONTROL | DATA)

Description

Create a SSL policy label.

Parameters

labelName

The name of the SSL policy label to be created.

type

Specifies when policies bound to this policy label will be evaluated. Possible values: CONTROL, DATA

Example

add ssl policylabel ssl_pol_label -type REQ

Top

rm ssl policylabel

Synopsis

rm ssl policylabel <labelName>

Description

Remove a SSL policy label.

Parameters

labelName

The name of the SSL policy label to be removed.

Example

rm ssl policylabel ssl_pol_label

Top

bind ssl policylabel

Synopsis

bind ssl policylabel <labelName> <policyName> <priority> [<gotoPriorityExpression>] [-invoke (<labelType> <labelName>)]

Description

Bind an SSL policy to a SSL policy label.

Parameters

labelName

Name of the SSL policy label.

policyName

The SSL policy name.

Example

bind ssl policylabel ssl_pol_label -policyName ssl_pol -priority 1

Top

unbind ssl policylabel

Synopsis

unbind ssl policylabel <labelName> <policyName> [-priority <positive_integer>]

Description

Unbind an SSL policy from a SSL policy label.

Parameters

labelName

Name of the SSL policy label.

policyName

The SSL policy name.

Example

unbind ssl policylabel ssl_pol_label ssl_pol

Top

show ssl policylabel

Synopsis

show ssl policylabel [<labelName>]

Description

Display all SSL policy labels or all policies bound to a SSL policy label.

Parameters

labelName

The name of the SSL policy label.

Example

i) show ssl policylabel ssl_pol_label
ii) show ssl policylabel

Top

ssl ocspResponder

[add | rm | set | unset | show]

add ssl ocspResponder

Synopsis

add ssl ocspResponder <name> -url <URL> [-cache (ENABLED | DISABLED) [-cacheTimeout <positive_integer>]] [-batchingDepth <positive_integer>] [-batchingDelay <positive_integer>] [-resptimeout <positive_integer>] [-responderCert <string> | -trustResponder] [-producedAtTimeSkew <positive_integer>] [-signingCert <string>] [-useNonce (YES | NO)] [-insertClientCert (YES | NO)]

Description

Add an OCSP responder object.

Parameters

name

The name of the OCSP responder.

url

The URL of the OCSP responder.

cache

Enable or disable caching of OCSP responses. Possible values: ENABLED, DISABLED

cacheTimeout

Optional OCSP cache time out in minutes. If omitted, the timeout provided in the OCSP response will be used. Default value: 1 Minimum value: 1 Maximum value: 1440

batchingDepth

Maximum number of client certificates to batch together into one OCSP request; a value of 1 makes each request separate and immediate. Minimum value: 1 Maximum value: 8

batchingDelay

Maximum time, in mS, to wait to accumulate OCSP requests to batch. If batching depth is 1, this argument has no effect. Maximum value: 10000

resptimeout

Maximum time, in mS, to wait for an OCSP response before giving up. Defaults to 2000 mS. Total waiting time is also dependent on batching delay as the sum of these two values will give you the total waiting time. If batching is disabled, timeout is completely governed by this parameter. Maximum value: 120000

producedAtTimeSkew

Amount of time, in seconds, that the NetScaler clock and the clock of the OCSP responder can differ for checking the producedAt time in the response. Default is 300 seconds (5 minutes). Default value: 300 Maximum value: 86400

signingCert

The certificate used to optionally sign OCSP requests. If omitted, requests will not be signed.

useNonce

Add a nonce to the OCSP request. Possible values: YES, NO

insertClientCert

Include the client cert in the OCSP request. Possible values: YES, NO

Example

1) add ssl ocspResponder -url http://ocsp.example.com -producedAtTimeSkew 0
The above command will only allow responses that were generated in the same second to be used. That is,
2) add ssl ocspResponder -url http://ocsp.example.com -producedAtTimeSkew 300
This command will allow responses to vary up to five minutes plus or minus. That is, if the response has a pr

Top

rm ssl ocspResponder

Synopsis

rm ssl ocspResponder <name> ...

Description

Remove the specified OCSP responder from the system.

Parameters

name

The name of the certificate-key pair. Note: The OCSP responder is removed only when it is not referenced by any other object.

Example

1) rm ssl ocspResponder o1
The above command removes the OCSP responder o1 from the system.

Top

set ssl ocspResponder

Synopsis

set ssl ocspResponder <name> [-url <URL>] [-cache (ENABLED | DISABLED)] [-cacheTimeout <positive_integer>] [-batchingDepth <positive_integer>] [-batchingDelay <positive_integer>] [-resptimeout <positive_integer>] [-responderCert <string> | -trustResponder] [-producedAtTimeSkew <positive_integer>] [-signingCert <string>] [-useNonce (YES | NO)] [-insertClientCert (YES | NO)]

Description

Set an OCSP responder object's properties.

Parameters

name

The name of the OCSP responder.

url

The URL of the OCSP responder.

cache

Enable or disable caching of OCSP responses. Possible values: ENABLED, DISABLED

cacheTimeout

Optional OCSP cache time out in minutes. If omitted, the timeout provided in the OCSP response will be used. Default value: 1 Minimum value: 1 Maximum value: 1440

batchingDepth

Maximum number of client certificates to batch together into one OCSP request; a value of 1 makes each request separate and immediate. Minimum value: 1 Maximum value: 8

batchingDelay

Maximum time, in mS, to wait to accumulate OCSP requests to batch. If batching depth is 1, this argument has no effect. Maximum value: 10000

resptimeout

Maximum time, in mS, to wait for an OCSP response before giving up. Defaults to 2000 mS. If this is set to 0, NetScaler will wait for an indefinite amount of time. Maximum value: 120000

producedAtTimeSkew

Amount of time, in seconds, that the NetScaler clock and the clock of the OCSP responder can differ for checking the producedAt time in the response. Default is 300 seconds (5 minutes). Default value: 300 Maximum value: 86400

signingCert

The certificate used to optionally sign OCSP requests. If omitted, requests will not be signed.

useNonce

Add a nonce to the OCSP request. Protects against replay attacks. Possible values: YES, NO

insertClientCert

Include the client cert in the OCSP request. Possible values: YES, NO

Example

1) add ssl ocspResponder -url http://ocsp.example.com -producedAtTimeSkew 0
The above command will only allow responses that were generated in the same second to be used. That is,
2) add ssl ocspResponder -url http://ocsp.example.com -producedAtTimeSkew 300
This command will allow responses to vary up to five minutes plus or minus. That is, if the response has a pr

Top

unset ssl ocspResponder

Synopsis

unset ssl ocspResponder <name> [-trustResponder] [-insertClientCert (YES | NO)] [-cache] [-cacheTimeout] [-batchingDepth] [-batchingDelay] [-resptimeout] [-responderCert] [-producedAtTimeSkew] [-signingCert] [-useNonce]

Description

Unset an OCSP responder object's properties..Refer to the set ssl ocspResponder command for meanings of the arguments.

Top

show ssl ocspResponder

Synopsis

show ssl ocspResponder [<name>]

Description

Add an OCSP responder object.

Parameters

name

The name of the OCSP responder.

Top

ssl rsakey

create ssl rsakey

Synopsis

create ssl rsakey <keyFile> <bits> [-exponent (3 | F4)] [-keyform (DER | PEM)] [-des | -des3] {-password }

Description

Generate an RSA key.

Parameters

keyFile

The file in which the generated RSA key is stored. The default output path for the key file is /nsconfig/ssl/. Maximum value: 63

bits

The bit value (key length) for the RSA key. Minimum value: 512 Maximum value: 4096

exponent

The public exponent value for the RSA key. The supported values are F4 (Hex: 0x10001) or 3 (Hex: 0x3). Possible values: 3, F4 Default value: FIPSEXP_F4

keyform

The format for the key file: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

des

Encrypt the generated RSA key using DES algorithm. You will be prompted to enter the pass-phrase (password) that will be used to encrypt the key.

des3

Encrypt the generated RSA key using the Triple-DES algorithm. You will be prompted to enter the pass-phrase (password) that will be used to encrypt the key.

password

The pass-phrase to use for encryption if '-des' or '-des3' option is selected. Maximum value: 31

Example

create ssl rsakey /nsconfig/ssl/rsa1024.pem 1024 -exp F4

ssl pkcs12

convert ssl pkcs12

Synopsis

convert ssl pkcs12 <outfile> [-import [-pkcs12File <input_filename>] [-des | -des3]] [-export [-certFile <input_filename>] [-keyFile <input_filename>]] {-password } {-PEMPassPhrase }

Description

Convert the end-user certificate (Client-certificate/Server-Certificate) from PEM encoding format to PKCS#12 format. These certificates can then be distributed and installed in browsers as Client certificates.

Parameters

outfile

The output file to be generated. If the -import option is used, this file will be used to store the certificate and the private-key in PEM format. If the -export option is used, the certificate and private-key will be stored in the PKCS12 format. The default output path for the file is /nsconfig/ssl/. Maximum value: 63

import

Convert the certificate and private-key from PKCS12 format to PEM format.

export

Convert the certificate and private-key from PEM format to PKCS12 format. Note: During the export operation, you will be prompted to enter the 'Export password'

Example

1) convert ssl pkcs12 /nsconfig/ssl/client_certkey.p12 -export -cert /nsconfig/ssl/client_certcert.pem -k
The above example CLI command converts the PEM encoded certificate and key file to PKCS#12.
2) convert ssl pkcs12 /nsconfig/ssl/client_certkey.pem -import -pkcs12 /nsconfig/ssl/client_certcertkey.p1
The above example CLI command converts the PKCS12 file to PEM format.
3) convert ssl pkcs12 /nsconfig/ssl/client_certkey.pem -import -pkcs12 /nsconfig/ssl/client_certcertkey.p
The above example CLI command converts the PKCS12 file to PEM format, with encrypted key.

Note: The -des option will encrypt the output key using DES algorithm. User will be prompted to enter the

ssl pkcs8

convert ssl pkcs8

Synopsis

convert ssl pkcs8 <pkcs8File> <keyFile> [-keyform (DER | PEM)] {-password }

Description

Convert a PEM or DER encoded key file to PKCS#8 format before importing it into the System's FIPS system.

Parameters

pkcs8File

The name of the output file where the PKCS8 format key file will be stored. The default output path for the PKCS8 file is /nsconfig/ssl/. Maximum value: 63

keyFile

The input key file. The default input path for the key file is /nsconfig/ssl/. Maximum value: 63

keyform

The format of the keyFile. PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

password

The password if the key is encrypted. Valid for PEM encoded files only. Maximum value: 31

Example

convert ssl pkcs8 /nsconfig/ssl/key.pk8 /nsconfig/ssl/key.pem

ssl dhParam

create ssl dhParam

Synopsis

create ssl dhParam <dhFile> [<bits>] [-gen (2 | 5)]

Description

Generate the Diffie-Hellman (DH) parameters.

Parameters

dhFile

The name of the output file where the generated DH parameter is stored. Maximum value: 63

bits

The bit value for the DH parameters.Maximum bit value allowed is 2048. Minimum value: 512 Maximum value: 2048

gen

The DH generator value (g) to be used. Possible values: 2, 5 Default value: 2

Example

1) create ssl dhparam /nsconfig/ssl/dh1024.pem 1024 -gen 5

ssl dsaKey

create ssl dsaKey

Synopsis

create ssl dsaKey <keyFile> <bits> [-keyform (DER | PEM)] [-des | -des3] {-password }

Description

Generate a DSA key.

Parameters

keyFile

The name of the output file where the generated DSA key is stored. The default output path for the DH file is /nsconfig/ssl/. Maximum value: 63

bits

The bit value (key length) for the DSA key. Minimum value: 512 Maximum value: 2048

keyform

The format of the key file: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule. Possible values: DER, PEM Default value: FORMAT_PEM

des

Encrypt the generated DSA key using the DES algorithm. It prompts you to enter the pass-phrase (password) that is used to encrypt the key.

des3

Encrypt the generated DSA key using Triple-DES algorithm. You will be prompted to enter the pass-phrase (password) that is used to encrypt the key.

password

The pass-phrase to use for encryption if '-des' or '-des3' option is selected. Maximum value: 31

Example

create ssl dsakey /nsconfig/ssl/dsa1024.pem 1024

ssl certLink

show ssl certLink

Synopsis

show ssl certLink

Description

Display all the linked certificate-key pairs in the system.

Example

The following shows an example of the output of the show ssl certlink command:
linked certificate:
1) Cert Name: siteAcertkey CA Cert Name: CAcertkey

ssl certReq

create ssl certReq

Synopsis

create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName <string>) [-keyform (DER | PEM) {-PEMPassPhrase }] -countryName <string> -stateName <string> -organizationName <string> [-organizationUnitName <string>] [-localityName <string>] [-commonName <string>] [-emailAddress <string>] {-challengePassword } [-companyName <string>]

Description

Generate a new Certificate Signing Request (CSR). The generated CSR can be sent to a Certificate-Authority (CA) to obtain an X509 certificate for the user domain (web site).

Parameters

reqFile

The file name where the generated Certificate Signing Requests are stored. The default output path for the CSR file is /nsconfig/ssl/. Maximum value: 63

keyFile

The key file name to be used. The key can be an RSA or a DSA key. The default input path for the key file is /nsconfig/ssl/. Maximum value: 63

fipsKeyName

The FIPS key name to be used. FIPS keys are created inside the FIPS HSM (Hardware Security Module). This is applicable only to the SSL FIPS system.

keyform

The format for the input key file specified in the keyFileName: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

countryName

Country Name - Two letter ISO code for your country. For example, US for United States.

stateName

State or Province Name - Full name for the state or province where your organization is located. Maximum characters allowed are 63. Do not abbreviate.

organizationName

Organization Name - Name of the organization. The organization name (corporation, limited partnership, university, or government agency) must be registered with some authority at the national, state, or city level. Use the legal name under which the organization is registered. Maximum characters allowed are 63. Do not abbreviate the organization name and do not use the following characters in the name: < > ~ ! @ # 0 ^ * / ( )?.

organizationUnitName

Organization Unit Name - Division or Section name in the organization that will use the certificate. Maximum characters allowed are 63.

localityName

Locality Name - Name of the city or town in which your organization's head office is located.Maximum characters allowed are 127.

commonName

Common Name - Fully qualified domain name for the company/Web site. The common name is the fully qualified domain name (FQDN) for the company/Web site. The common name must match the name used by DNS servers to do a DNS lookup of your server (for example, www.mywebsite.com <http://www.mywebsite.com>). Most browsers use this information for authenticating the server's certificate during the SSL handshake. If the server name does not match the common name as given in the server certificate, the browsers will terminate the SSL handshake or prompt the user with a warning message. The maximum characters allowed are 63. CAUTION: Do not use wildcard characters such as * or ? and do not use an IP address as the common name. The common name should be without the protocol specifier <http://> or <https://>.

emailAddress

Challenge Password - The contact person's E-mail address.

challengePassword

Challenge Password - Challenge password for this certificate.

companyName

Optional Company Name - Additional name of the company/web-site.

Example

create ssl certreq /nsconfig/ssl/csr.pem -keyFile /nsconfig/ssl/rsa1024.pem

ssl cert

create ssl cert

Synopsis

create ssl cert <certFile> <reqFile> <certType> [-keyFile <input_filename>] [-keyform (DER | PEM) {-PEMPassPhrase }] [-days <positive_integer>] [-certForm (DER | PEM)] [-CAcert <input_filename>] [-CAcertForm (DER | PEM)] [-CAkey <input_filename>] [-CAkeyForm (DER | PEM)] [-CAserial <output_filename>]

Description

Generate a signed X509 Certificate.

Parameters

certFile

The name of the generated certificate file. The default path of the certificate file is /nsconfig/ssl/. Maximum value: 63

reqFile

The Certificate Signing Request (CSR) file that is used to generate the certificate. This file is created using the "create ssl certreq" command or an existing CSR. The default input path for the CSR file is /nsconfig/ssl/. Maximum value: 63

certType

The type of the certificate to be generated. ROOT_CERT : The certificate generated will be a self-signed Root-CA certificate. For this, you need to specify the -keyfile parameter. The generated Root-CA certificate can be used for signing end-user certificates (Client/Server) or to create Intermediate-CA certificates. INTM_CERT : The certificate generated will be an Intermediate-CA certificate. For this, you need to specify the following parameters: -CAcert , -CAkey, and -CAserial. NOTE: The three parameters are also mandatory for the CLNT_CERT or SRVR_CERT certificate types. CLNT_CERT : The certificate generated will be an end-user client certificate. This can be used in a Client-Authentication setup. SRVR_CERT : The certificate generated will be an end-user Server certificate. This can be used as an SSL server certificate on the backend SSL servers for an SSL backend-encryption setup with the system. NOTE: Avoid using the Server certificate (generated above) for a front-end SSL virtual server (or SSL service) on a system or on any frontend SSL server if the certificate is signed by System. The same is true with System generated Intermediate-CA or Root-CA certificate. The reason being, the System generated CA certificates will not be present in browsers (such as IE, Netscape, and other browsers) by default. So during the SSL handshake the Server Certificate verification will fail. Browsers generally display a warning message and prompt the user to either continue with the SSL handshake or terminate it. If the System

generated CA certificates are installed in the browsers as trusted CA certificates, the SSL handshake will proceed without any errors or warnings. Possible values: ROOT_CERT, INTM_CERT, CLNT_CERT, SRVR_CERT

keyFile

The input keyFile to sign the certificate being generated. This keyFile is created using the "create ssl rsakey" or "create ssl dsakey" commands, or an existing RSA/DSA key. This file is required only when creating a self-signed Root-CA certificate. The default input path for the keyFile is /nsconfig/ssl/. Note: If the input key specified is an encrypted key, the user will be prompted to enter the PEM pass-phrase that was used for encrypting the key. Maximum value: 63

keyform

The format for the input key file: PEM : Privacy Enhanced Mail DER : Distinguished Encoding Rule. Possible values: DER, PEM Default value: FORMAT_PEM

days

The number of days for which the certificate will be valid. The certificate is valid from the time and day (system time) of the creation, to the number of days specified in the -days field.The maximum value allowed is 3650 Default value: 365 Minimum value: 1 Maximum value: 3650

certForm

The output certificate format: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

CAcert

The CA certificate file that will issue and sign the Intermediate-CA certificate or the end-user certificates (Client/Server). The default input path for the CA certificate file is /nsconfig/ssl/. Maximum value: 63

CAcertForm

The format of the input CA certificate file: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

CAkey

The CA key file that will be used to sign the Intermediate-CA certificate or the end-user certificates (Client/Server). The default input path for the CA key file is /nsconfig/ssl/. Note: If the CA key file is password protected, the user will be prompted to enter the pass-phrase used for encrypting the key. Maximum value: 63

CAkeyForm

The format of the input CA key file: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

CAserial

The Serial number file maintained for the CA certificate. This will contain the serial number of the next certificate to be issued/signed by the CA (-CAcert). If the specified file does not exist, a new file will be created. The default input path for the CAserial file name is /nsconfig/ssl/. Note: Specify the proper path of the existing serial file; else a new serial file will be created. This may change the certificate serial numbers assigned by the CA certificate to each of the certificate it signs. Maximum value: 63

Example

1) create ssl cert /nsconfig/ssl/root_cert.pem /nsconfig/ssl/root_csr.pem ROOT_CERT -keyFile /nsconfig/ssl
The above example creates a self signed Root-CA certificate.
2) create ssl cert /nsconfig/ssl/server_cert.pem /nsconfig/ssl/server_csr.pem SRVR_CERT -CAcert /nsconfig
The above example creates a Server certificate which is signed by the Root-CA certificate: root_cert.pem

ssl stats

show ssl stats

Synopsis

show ssl stats - alias for 'stat ssl'

Description

show ssl stats is an alias for stat ssl

ssl parameter

[set | unset | show]

set ssl parameter

Synopsis

set ssl parameter [-quantumSize <quantumSize>] [-crlMemorySizeMB <positive_integer>] [-strictCAChecks (YES | NO)] [-sslTriggerTimeout <positive_integer>] [-sendCloseNotify (YES | NO)] [-encryptTriggerPktCount <positive_integer>] [-denySSLReneg <denySSLReneg>] [-insertionEncoding (Unicode | UTF-8)] [-ocspCacheSize <positive_integer>] [-pushFlag <positive_integer>] [-dropReqWithNoHostHeader (YES | NO)] [-pushEncTriggerTimeout <positive_integer>] [-undefActionControl <string>] [-undefActionData <string>]

Parameters

quantumSize

SSL quantum size configures the amount of data to be collected before we push the data to the crypto hardware for encryption. Setting the right quantum size based on the application requirements will help to better utilize the crypto resources. For example, in case of large downloads, larger quantum size is beneficial. Possible values: 4096, 8192, 16384 Default value: 8192

crlMemorySizeMB

Memory size to use for CRLs. Set the maximum system memory size, the CRL(s) can consume. This setting will not reserve the memory for CRL, but will set the max limit all CRL(s) loaded in the system can consume. Default value: 256 Minimum value: 10 Maximum value: 1024

strictCAChecks

Enable strict CA certificate checks. Possible values: YES, NO Default value: NO

sslTriggerTimeout

Encryption trigger timer. Set the encryption trigger timeout for transactions, which are not trackable by Netscaler. NetScaler will use this setting to accumulate data received from the server for the configured time period before pushing it to the crypto hardware for encryption Default value: 100 Minimum value: 1 Maximum value: 200

sendCloseNotify

Enable sending SSL Close-Notify at the end of a transaction Possible values: YES, NO Default value: YES

encryptTriggerPktCount

Number of queued packets that force encryption to occur. Set the maximum number of packets to accumulate before triggering encryption to the crypto hardware. Default setting is 45 packets. This setting can be used for non-trackable transactions which generates small size packets from server to NetScaler. Default value: 45 Minimum value: 10 Maximum value: 50

denySSLReneg

SSL Renegotiation setting NO: Allow SSL renegotiation to work. FRONTEND_CLIENT: Deny SSL renegotiation initiated by the client. FRONTEND_CLIENTSERVER: Deny SSL renegotiation initiated by the client and by NS (during policy-based clientAuth). NONSECURE. Deny nonsecure SSL renegotiation. This option will only allow clients which support RFC 5746. ALL: Deny SSL renegotiation for above two cases and for server initiated renegotiation on the backend side. Possible values: NO, FRONTEND_CLIENT, FRONTEND_CLIENTSERVER, ALL, NONSECURE Default value: NO

insertionEncoding

Encoding method used to insert Subject/Issuer in HTTP Request to backend servers. Possible values: Unicode, UTF-8 Default value: UNICODE_INSERTION

ocspCacheSize

Size, per packet engine, in megabytes of the OCSP cache. The actual maximum value for this value is clamped at 10% of packet engine memory. Maximum packet engine memory is 4GB; thus, if you have enough memory to give all packet engines 4GB of memory, the maximum value here would be approximately 410 MB. Default value: 10 Maximum value: 512

pushFlag

PUSH insertion cotnrol flags (Can be ORed): 0 auto, 0x1 = every decrypted record, 0x2 = every encrypted record Maximum value: 3

dropReqWithNoHostHeader

Host header check for SNI enabled sessions. If this check is enabled and if the HTTP request does not contain the Host header for SNI enabled session, then the request will be dropped Possible values: YES, NO Default value: NO

pushEncTriggerTimeout

PUSH encryption trigger timer Default value: 1 Minimum value: 1 Maximum value: 200

undefActionControl

Name of undef action. It can be SSL control builtin action like CLIENTAUTH, NOCLIENTAUTH or an action like NOOP, RESET, DROP. Default value: "CLIENTAUTH"

undefActionData

Name of undef action. It can be NOOP, RESET or DROP Default value: "NOOP"

Top

unset ssl parameter

Synopsis

unset ssl parameter [-quantumSize] [-crlMemorySizeMB] [-strictCAChecks] [-sslTriggerTimeout] [-sendCloseNotify] [-encryptTriggerPktCount] [-denySSLReneg] [-insertionEncoding] [-ocspCacheSize] [-pushFlag] [-dropReqWithNoHostHeader] [-pushEncTriggerTimeout] [-undefActionControl] [-undefActionData]

Description

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

Top

show ssl parameter

Synopsis

show ssl parameter

Description

Display ssl advanced parameters.

Top

ssl fips

[set | unset | reset | show | update]

set ssl fips

Synopsis

set ssl fips -initHSM Level-2 [-hsmLabel <string>]

Description

Initialize the Hardware Security Module (HSM) or the FIPS card and set a new Security Officer password and User password. CAUTION: This command will erase all data on the FIPS card. You will be prompted before proceeding with the command execution. Save the current configuration after executing this command.

Parameters

initHSM

The FIPS initialization level. Possible values: Level-2

soPassword

The Hardware Security Module's (HSM) Security Officer password.

oldSoPassword

The old Security Officer password. This is used for authentication.

userPassword

The Hardware Security Module's (HSM) User password.

hsmLabel

The label to identify the Hardware Security Module (HSM).

Example

1) set fips -initHSM Level-2 fipsso123 oldfipsso123 fipuser123 -hsmLabel FIPS-140-2
>This command will erase all data on the FIPS card. You must save the configuration (saveconfig) after execu

The above command initializes the FIPS card to FIPS-140-2 Level-2 and sets the HSM's Security Officer and Us

Top

unset ssl fips

Synopsis

unset ssl fips -hsmLabel

Description

Use this command to remove ssl fips settings.Refer to the set ssl fips command for meanings of the arguments.

Top

reset ssl fips

Synopsis

reset ssl fips

Description

Reset the FIPS card to default password for SO and User accounts. Note: This command can be used only if the FIPS card has been locked due to three or more unsuccessful login attempts

Example

reset fips

Top

show ssl fips

Synopsis

show ssl fips

Description

Display the information on the FIPS card.

Example

An example of the output for show ssl fips command is as follows:

```
FIPS HSM Info:
    HSM Label            : FIPS1
    Initialization       : FIPS-140-2 Level-2
    HSM Serial Number    : 238180016
    Firmware Version     : 4.3.0
    Total Flash Memory   : 1900428
    Free Flash Memory    : 1899720
    Total SRAM Memory    : 26210216
    Free SRAM Memory     : 17857232
```

Top

update ssl fips

Synopsis

update ssl fips -fipsFW 4.6.1

Description

Update the FIPS firmware. Note: Only compatible firmware version upgrade is allowed, e.g 4.6.0 to 4.6.1

Parameters

fipsFW

The FIPS firmware update. Possible values: 4.6.1

Example

update ssl fips -fipsFW 4.6.1

Top

ssl service

[set | unset | bind | unbind | show]

set ssl service

Synopsis

set ssl service <serviceName>@ [-dh (ENABLED | DISABLED) -dhFile <string>] [-dhCount <positive_integer>] [-eRSA (ENABLED | DISABLED) [-eRSACount <positive_integer>]] [-sessReuse (ENABLED | DISABLED) [-sessTimeout <positive_integer>]] [-cipherRedirect (ENABLED | DISABLED) [-cipherURL <URL>]] [-sslv2Redirect (ENABLED | DISABLED) [-sslv2URL <URL>]] [-clientAuth (ENABLED | DISABLED) [-clientCert (Mandatory | Optional)]] [-sslRedirect (ENABLED | DISABLED)] [-redirectPortRewrite (ENABLED | DISABLED)] [-nonFipsCiphers (ENABLED | DISABLED)] [-ssl2 (ENABLED | DISABLED)] [-ssl3 (ENABLED | DISABLED)] [-tls1 (ENABLED | DISABLED)] [-SNIEnable (ENABLED | DISABLED)] [-serverAuth (ENABLED | DISABLED)] [-pushEncTrigger <pushEncTrigger>] [-sendCloseNotify (YES | NO)]

Description

Set the Advance SSL Configurations for an SSL service.

Parameters

serviceName

The SSL service name for which the advance configurations are to be set.

dh

The state of Diffie-Hellman (DH) key exchange support for the SSL service. Possible values: ENABLED, DISABLED Default value: DISABLED

dhCount

The refresh count for regeneration of DH public-key and private-key from the DH parameter. Zero means infinite usage (no refresh). Option '-dh' has to be enabled Maximum value: 65534

eRSA

The state of Ephemeral RSA key exchange support for the SSL service. Ephemeral RSA is used for export ciphers. Possible values: ENABLED, DISABLED Default value: ENABLED

sessReuse

The state of session reuse support for the SSL service. Possible values: ENABLED, DISABLED Default value: ENABLED

cipherRedirect

The state of Cipher Redirect feature. Cipher Redirect feature can be used to provide more readable information to SSL clients about mismatch in ciphers between the client and the SSL vserver. Possible values: ENABLED, DISABLED Default value: DISABLED

sslv2Redirect

The state of SSLv2 Redirect feature . SSLv2 Redirect feature can be used to provide more readable information to SSL client about non-support of SSLv2 protocol on the SSL vserver. Possible values: ENABLED, DISABLED Default value: DISABLED

clientAuth

The state of Client-Authentication support for the SSL service. Possible values: ENABLED, DISABLED Default value: DISABLED

sslRedirect

The state of HTTPS redirects for the SSL service. This is required for the proper functioning of the redirect messages from the server. The redirect message from the server provides the new location for the moved object. This is contained in the HTTP header field: Location, e.g. Location: http://www.moved.org/here.html For the SSL session, if the client browser receives this message, the browser will try to connect to the new location. This will break the secure SSL session, as the object has moved from a secure site (https://) to an un-secure one (http://). Generally browsers flash a warning message on the screen and prompt the user, either to continue or disconnect. The above feature, when enabled will automatically convert all such http:// redirect message to https://. This will not break the client SSL session. Note: The set ssl service command can be used for configuring a front-end SSL service for service based SSL Off-Loading, or a backend SSL service for backend-encryption setup. Some of the command options are not applicable while configuring a backend service. System will not report an error if these options are used for a backend SSL service. These are: [-dh (ENABLED|DISABLED) (-dhFile < file_name >)] [(-dhCount <pos_int>)] [-eRSA (ENABLED|DISABLED)] [(-eRSACount <pos_int>)] [-cipherRedirect (ENABLED | DISABLED) [-cipherURL <URL>]] [-sslv2Redirect (ENABLED | DISABLED) [-sslv2URL <URL>]] [-clientAuth (ENABLED | DISABLED) [-clientCert (Mandatory | Optional)]] [-sslRedirect (ENABLED | DISABLED)] [-ssl2 (ENABLED|DISABLED)]. Possible values: ENABLED, DISABLED Default value: DISABLED

redirectPortRewrite

The state of the port in rewrite while performing HTTPS redirect. Possible values: ENABLED, DISABLED Default value: DISABLED

nonFipsCiphers

The state of usage of non FIPS approved ciphers. Valid only for an SSL service bound with a FIPS key and certificate. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl2

The state of SSLv2 protocol support for the SSL service. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl3

The state of SSLv3 protocol support for the SSL service. Possible values: ENABLED, DISABLED Default value: ENABLED

tls1

The state of TLSv1 protocol support for the SSL service. Possible values: ENABLED, DISABLED Default value: ENABLED

SNIEnable

The state of SNI Extension. Server Name Indication (SNI) helps to enable SSL encryption on multiple subdomains if the domains are controlled by the same organization and share the same second-level domain name. State of SNI feature on service Possible values: ENABLED, DISABLED Default value: DISABLED

serverAuth

The state of Server-Authentication support for the SSL service. Possible values: ENABLED, DISABLED Default value: DISABLED

pushEncTrigger

PUSH packet triggering encryption Always - Any PUSH packet triggers encryption Ignore - Ignore PUSH packet for triggering encryption Merge - For consecutive sequence of PUSH packets, last PUSH packet triggers encryption Timer - PUSH packet triggering encryption delayed by timer period defined in 'set ssl parameter' Possible values: Always, Merge, Ignore, Timer

sendCloseNotify

Enable sending SSL Close-Notify at the end of a transaction Possible values: YES, NO Default value: YES

Example

1) set ssl service sslsvc -dh ENABLED -dhFile /nsconfig/ssl/dh1024.pem -dhCount 500
The above example sets the DH parameters for the SSL service 'sslsvc'.
2. set ssl service sslsvc -ssl2 DISABLED
The above example disables the support for SSLv2 protocol for the SSL service 'sslsvc'.

Top

unset ssl service

Synopsis

unset ssl service <serviceName>@ [-dh] [-dhFile] [-dhCount] [-eRSA] [-eRSACount] [-sessReuse] [-sessTimeout] [-cipherRedirect] [-cipherURL] [-sslv2Redirect] [-sslv2URL] [-clientAuth] [-clientCert] [-sslRedirect] [-redirectPortRewrite] [-nonFipsCiphers] [-ssl2] [-ssl3] [-tls1] [-SNIEnable] [-serverAuth] [-sendCloseNotify]

Description

Use this command to remove ssl service settings.Refer to the set ssl service command for meanings of the arguments.

Top

bind ssl service

Synopsis

bind ssl service <serviceName>@ ((-policyName <string> [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-invoke (<labelType> <labelName>)]) | ((-certkeyName <string> [(-CA [-crlCheck (Mandatory | Optional) | -ocspCheck (Mandatory | Optional)]) | -SNICert]) | -cipherName <string>))

Description

Bind a SSL certkey or a SSL policy to a SSL service.

Parameters

serviceName

The name of the SSL service to which the SSL policy needs to be bound.

policyName

The name of the SSL policy.

certkeyName

The name of the CertKey

cipherName

A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.

Example

bind ssl service ssl_svc -policyName certInsert_pol -priority 10

Top

unbind ssl service

Synopsis

unbind ssl service <serviceName>@ ((-policyName <string> [-priority <positive_integer>]) | ((-certkeyName <string> [(-CA [-crlCheck (Mandatory | Optional)]) | -SNICert]) | -cipherName <string>))

Description

Unbind a SSL policy from a SSL service.

Parameters

serviceName

The name of the SSL service from which the SSL policy needs to be unbound.

policyName

The name of the SSL policy.

certkeyName

The certificate key pair binding.

cipherName

A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.

Example

unbind ssl service ssl_svc -policyName certInsert_pol

Top

show ssl service

Synopsis

show ssl service [<serviceName>] [-cipherDetails]

Description

View the advanced SSL settings for an SSL service.

Parameters

serviceName

The name of the SSL service.

cipherDetails

Details of the individual ciphers bound to the SSL service. Select this flag value to display the details of the individual ciphers bound to the SSL service.

Example

An example of output of show ssl service command is as shown below
show ssl service svc1

```
Advanced SSL configuration for Back-end SSL Service svc1:
DH: DISABLED
Ephemeral RSA: ENABLED          Refresh Count: 0
Session Reuse: ENABLED          Timeout: 300 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
Server Auth: DISABLED
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)      Cipher Name: ALL
Description: Predefined Cipher Alias
```

Top

ssl serviceGroup

[set | unset | bind | unbind | show]

set ssl serviceGroup

Synopsis

set ssl serviceGroup <serviceGroupName>@ [-sessReuse (ENABLED | DISABLED) [-sessTimeout <positive_integer>]] [-nonFipsCiphers (ENABLED | DISABLED)] [-ssl3 (ENABLED | DISABLED)] [-tls1 (ENABLED | DISABLED)] [-serverAuth (ENABLED | DISABLED)] [-sendCloseNotify (YES | NO)]

Description

Set the Advance SSL Configurations for a SSL service group.

Parameters

serviceGroupName

The SSL service group name for which the advance configurations are to be set.

sessReuse

The state of session reuse support for the SSL service group. Possible values: ENABLED, DISABLED Default value: ENABLED

nonFipsCiphers

The state of usage of non FIPS approved ciphers. Valid only for an SSL service group bound with a FIPS key and certificate. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl3

The state of SSLv3 protocol support for the SSL service group. Possible values: ENABLED, DISABLED Default value: ENABLED

tls1

The state of TLSv1 protocol support for the SSL service group. Possible values: ENABLED, DISABLED Default value: ENABLED

serverAuth

The state of Server-Authentication support for the SSL service group. Possible values: ENABLED, DISABLED Default value: DISABLED

sendCloseNotify

Enable sending SSL Close-Notify at the end of a transaction Possible values: YES, NO Default value: YES

Example

1) set ssl servicegroup svcg1 -sessReuse DISABLED
The above example disables session reuse for the service group 'svcg1'.

Top

unset ssl serviceGroup

Synopsis

unset ssl serviceGroup <serviceGroupName>@ [-sessReuse] [-sessTimeout] [-nonFipsCiphers] [-ssl3] [-tls1] [-serverAuth] [-sendCloseNotify]

Description

Use this command to remove ssl serviceGroup settings.Refer to the set ssl serviceGroup command for meanings of the arguments.

Top

bind ssl serviceGroup

Synopsis

bind ssl serviceGroup <serviceGroupName>@ ((-certkeyName <string> [(-CA [-crlCheck (Mandatory | Optional) | -ocspCheck (Mandatory | Optional)]) | -SNICert]) | -cipherName <string>)

Description

Bind a SSL certkey or a SSL policy to a SSL service.

Parameters

serviceGroupName

The name of the SSL service to which the SSL policy needs to be bound.

certkeyName

The name of the CertKey

cipherName

A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.

Example

bind ssl service ssl_svc -policyName certInsert_pol -priority 10

Top

unbind ssl serviceGroup

Synopsis

unbind ssl serviceGroup <serviceGroupName>@ ((-certkeyName <string> [(-CA [-crlCheck (Mandatory | Optional)]) | -SNICert]) | -cipherName <string>)

Description

Unbind a SSL policy from a SSL service.

Parameters

serviceGroupName

The name of the SSL service from which the SSL policy needs to be unbound.

certkeyName

The name of the certificate bound to the SSL service group.

cipherName

A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.

Example

unbind ssl service ssl_svc -policyName certInsert_pol

Top

show ssl serviceGroup

Synopsis

show ssl serviceGroup [<serviceGroupName>] [-cipherDetails]

Description

View the advanced SSL settings for an SSL service group.

Parameters

serviceGroupName

The name of the SSL service group.

cipherDetails

Display the details of the individual ciphers bound to the SSL service group.

Example

An example of output of show ssl servicegroup command is as shown below
show ssl servicegroup ssl_svcg

```
Advanced SSL configuration for Back-end SSL Service Group ssl_svcg:
Session Reuse: ENABLED          Timeout: 300 seconds
Server Auth: DISABLED
Non FIPS Ciphers: DISABLED
SSLv3: ENABLED  TLSv1: ENABLED

1)   Cipher Name: ALL
     Description: Predefined Cipher Alias
```

Top

ssl vserver

[set | unset | bind | unbind | show]

set ssl vserver

Synopsis

set ssl vserver <vServerName>@ [-clearTextPort <port>] [-dh (ENABLED | DISABLED) -dhFile <string>] [-dhCount <positive_integer>] [-eRSA (ENABLED | DISABLED) [-eRSACount <positive_integer>]] [-sessReuse (ENABLED | DISABLED) [-sessTimeout <positive_integer>]] [-cipherRedirect (ENABLED | DISABLED) [-cipherURL <URL>]] [-sslv2Redirect (ENABLED | DISABLED) [-sslv2URL <URL>]] [-clientAuth (ENABLED | DISABLED) [-clientCert (Mandatory | Optional)]] [-sslRedirect (ENABLED | DISABLED)] [-redirectPortRewrite (ENABLED | DISABLED)] [-nonFipsCiphers (ENABLED | DISABLED)] [-ssl2 (ENABLED | DISABLED)] [-ssl3 (ENABLED | DISABLED)] [-tls1 (ENABLED | DISABLED)] [-SNIEnable (ENABLED | DISABLED)] [-pushEncTrigger <pushEncTrigger>] [-sendCloseNotify (YES | NO)]

Description

Set Advance SSL Configurations for an SSL virtual server.

Parameters

vServerName

The name of the SSL virtual server.

clearTextPort

The port on the back-end web-servers where the clear-text data is sent by system. Use this setting for the wildcard IP based SSL Acceleration configuration (*:443).

dh

The state of DH key exchange support for the specified SSL virtual server. Possible values: ENABLED, DISABLED Default value: DISABLED

dhCount

The refresh count for the re-generation of DH public-key and private-key from the DH parameter. Zero means infinite usage (no refresh). Note: The '-dh' argument must be enabled if this argument is specified. Maximum value: 65534

eRSA

The state of Ephemeral RSA key exchange support for the SSL virtual server. Ephemeral RSA is used for export ciphers Possible values: ENABLED, DISABLED Default value: DISABLED

sessReuse

The state of session re-use support for the SSL virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

cipherRedirect

The state of Cipher Redirect feature.Cipher Redirect feature can be used to provide more readable information to SSL clients about mismatch in ciphers between the client and the SSL vserver. Possible values: ENABLED, DISABLED Default value: DISABLED

sslv2Redirect

The state of SSLv2 Redirect feature.SSLv2 Redirect feature can be used to provide more readable information to SSL client about non-support of SSLv2 protocol on the SSL vserver. Possible values: ENABLED, DISABLED Default value: DISABLED

clientAuth

The state of Client-Authentication support for the SSL virtual server. Possible values: ENABLED, DISABLED Default value: DISABLED

sslRedirect

The state of HTTPS redirects for the SSL virtual server. This is required for proper working of the redirect messages from the web server. The redirect message from the server gives the new location for the moved object. This is contained in the HTTP header field: Location (for example, Location: http://www.moved.org/here.html). For an SSL session, if the client browser receives this message, the browser will try to connect to the new location. This will break the secure SSL session, as the object has moved from a secure site (https://) to an unsecured one (http://). Browsers usually flash a warning message on the screen and prompt the user to either continue or disconnect. When the above feature is enabled, all such http:// redirect messages are automatically converted to https://. This does not break the client SSL session. Possible values: ENABLED, DISABLED Default value: DISABLED

redirectPortRewrite

The state of port in rewrite while performing HTTPS redirect. When this setting is ENABLED on a SSL virtual server, the NetScaler rewrites the port by using the port settings of the content switching virtual server. Possible values: ENABLED, DISABLED Default value: DISABLED

nonFipsCiphers

The state of usage of non FIPS approved ciphers. Valid only for an SSL vserver bound with a FIPS key and certificate. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl2

The state of SSLv2 protocol support for the SSL virtual server. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl3

The state of SSLv3 protocol support for the SSL virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

tls1

The state of TLSv1 protocol support for the SSL virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

SNIEnable

state of SNI feature on virtual server Possible values: ENABLED, DISABLED Default value: DISABLED

pushEncTrigger

PUSH packet triggering encryption Always - Any PUSH packet triggers encryption Ignore - Ignore PUSH packet for triggering encryption Merge - For consecutive sequence of PUSH packets, last PUSH packet triggers encryption Timer - PUSH packet triggering encryption delayed by timer period defined in 'set ssl parameter' Possible values: Always, Merge, Ignore, Timer

sendCloseNotify

Enable sending SSL Close-Notify at the end of a transaction Possible values: YES, NO Default value: YES

Example

1) set ssl vserver sslvip -dh ENABLED -dhFile /siteA/dh1024.pem -dhCount 500
The above example set the DH parameters for the SSL virtual server 'sslvip'.
3) set ssl vserver sslvip -ssl2 DISABLED
The above example disables the support for SSLv2 protocol for the SSL virtual server 'sslvip'.

Top

unset ssl vserver

Synopsis

unset ssl vserver <vServerName>@ [-clearTextPort] [-dh] [-dhFile] [-dhCount] [-eRSA] [-eRSACount] [-sessReuse] [-sessTimeout] [-cipherRedirect] [-cipherURL] [-sslv2Redirect] [-sslv2URL] [-clientAuth] [-clientCert] [-sslRedirect] [-redirectPortRewrite] [-nonFipsCiphers] [-ssl2] [-ssl3] [-tls1] [-SNIEnable] [-sendCloseNotify]

Description

Use this command to remove ssl vserver settings.Refer to the set ssl vserver command for meanings of the arguments.

Top

bind ssl vserver

Synopsis

bind ssl vserver <vServerName>@ ((-policyName <string> [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-invoke (<labelType> <labelName>)]) | ((-certkeyName <string> [(-CA [-crlCheck (Mandatory | Optional) | -ocspCheck (Mandatory | Optional)]) | -SNICert]) | -cipherName <string>))

Description

Bind a SSL certkey or a SSL policy to a SSL virtual server.

Parameters

vServerName

The name of the SSL virtual server to which the SSL policy needs to be bound.

policyName

The name of the SSL policy.

certkeyName

The name of the CertKey

cipherName

A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.

Example

1. bind ssl vserver ssl_vip -certkeyName cert1
In the above example the certificate cert1 is bound to the SSL vserver ssl_vip as server certificate.
2. bind ssl vserver ssl_vip -certkeyName cert2 -CA
In the above example the certificate cert2 is bound to the SSL vserver ssl_vip as CA certificate.
3. bind ssl vserver ssl_vip -certkeyName cert3 -CA -ocspCheck Mandatory
In the above example the certificate cert3 is bound to the SSL vserver ssl_vip as CA certificate, with OCSP ch
4. bind ssl vserver ssl_vip -policyName certInsert_pol -priority 10
In the above example the SSL policy certInsert_pol is bound to the SSL vserver ssl_vip with priority 10.

Top

unbind ssl vserver

Synopsis

unbind ssl vserver <vServerName>@ ((-policyName <string> [-priority <positive_integer>]) | ((-certkeyName <string> [-CA | -SNICert]) | -cipherName <string>))

Description

Unbind a SSL policy from a SSL virtual server.

Parameters

vServerName

The name of the SSL virtual server from which the SSL policy needs to be unbound.

policyName

The name of the SSL policy.

certkeyName

The name of the certificate key pair binding.

cipherName

A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.

Example

unbind ssl vserver ssl_vip -policyName certInsert_pol

Top

show ssl vserver

Synopsis

show ssl vserver [<vServerName>] [-cipherDetails]

Description

Display all the SSL specific configurations for an SSL virtual server. This includes information about the Advance SSL configurations, certificate bindings, and cipher-suite configurations.

Parameters

vServerName

The name of the SSL virtual server.

cipherDetails

Details of the individual ciphers bound to the SSL vserver. Select this flag value to display the details of the individual ciphers bound to the SSL vserver.

Example

An example of the output of the show vserver sslvip command is as follows:
sh ssl vserver va1

```
        Advanced SSL configuration for VServer va1:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 0
        Session Reuse: ENABLED          Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

        1 bound certificate:
1)      CertKey Name: buy       Server Certificate

        1 bound CA certificate:
1)      CertKey Name: rtca      CA Certificate

        1)      Cipher Name: DEFAULT
        Description: Predefined Cipher Alias
```

Top

ssl fipsSIMTarget

[enable | init]

enable ssl fipsSIMTarget

Synopsis

enable ssl fipsSIMTarget <keyVector> <sourceSecret>

Description

Enable the target FIPS system to participate in secure exchange of keys with another FIPS system. The command is used for secure transfer of FIPS keys from the Primary system to the Secondary system.

Parameters

keyVector

The file name and path for storing the target FIPS system's key-vector. The default output path for the secret data is /nsconfig/ssl/.

sourceSecret

The file name and path for the source FIPS system's secret data. The default input path for the secret data is /nsconfig/ssl/.

Example

enable fipsSIMtarget /nsconfig/ssl/target.key /nsconfig/ssl/source.secret

Top

init ssl fipsSIMTarget

Synopsis

init ssl fipsSIMTarget <certFile> <keyVector> <targetSecret>

Description

Initialize the target FIPS system for participating in secure exchange of keys with another FIPS system. The command is used for secure transfer of FIPS keys from the primary system to the Secondary system.

Parameters

certFile

The source FIPS system's certificate file name and path. The default input path for the certificate file is /nsconfig/ssl/.

keyVector

The file name and path for storing the target FIPS system's key-vector. The default output path for the key-vector is /nsconfig/ssl/.

targetSecret

The file name and path for storing the target FIPS system's secret data. The default output path for the secret data is /nsconfig/ssl/.

Example

```
init fipsSIMtarget /nsconfig/ssl/source.cert /nsconfig/ssl/target.key /nsconfig/ssl/target.secret
```

Top

ssl fipsSIMSource

[enable | init]

enable ssl fipsSIMSource

Synopsis

enable ssl fipsSIMSource <targetSecret> <sourceSecret>

Description

Enable the source FIPS system for participating in secure exchange of keys with another FIPS system. The command is used for secure transfer of FIPS keys from the Primary system to the Secondary system.

Parameters

targetSecret

The file name and path for the target FIPS system's secret data. The default input path for the secret data is /nsconfig/ssl/.

sourceSecret

The file name and path for storing the source FIPS system's secret data. The default output path for the secret data is /nsconfig/ssl/.

Example

enable fipsSIMsource /nsconfig/ssl/target.secret /nsconfig/ssl/source.secret

Top

init ssl fipsSIMSource

Synopsis

init ssl fipsSIMSource <certFile>

Description

Initialize the source FIPS system for participating in secure exchange of keys with another FIPS system. The command is used for secure transfer of FIPS keys from the primary system to the secondary system.

Parameters

certFile

The file name and path where the source FIPS system's certificate is to be stored. The default output path for the certificate file is /nsconfig/ssl/.

Example

```
init fipsSIMsource /nsconfig/ssl/source.cert
```

Top

ssl global

[bind | unbind | show]

bind ssl global

Synopsis

bind ssl global [-policyName <string>] [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-type <type>] [-invoke (<labelType> <labelName>)]

Description

Bind an SSL policy globally.

Parameters

policyName

The name of the SSL policy.

Example

bind ssl global -policyName certInsert_pol -priority 100

Top

unbind ssl global

Synopsis

unbind ssl global [-policyName <string> [-type <type>] [-priority <positive_integer>]]

Description

Unbind a globally bound SSL policy.

Parameters

policyName

The name of the SSL policy.

Example

unbind ssl global -policyName certInsert_pol

Top

show ssl global

Synopsis

show ssl global [-type <type>]

Description

Display globally bound SSL policies.

Parameters

type

The bindpoint to which policy is bound. Possible values: CONTROL_OVERRIDE, CONTROL_DEFAULT, DATA_OVERRIDE, DATA_DEFAULT

Example

```
show ssl global
      1 Globally Active SSL Policy:
1)    Name: certInsert_pol       Priority: 100
```

Top

Stream Commands

This group of commands can be used to perform operations on the following entities:

- stream selector
- stream identifier
- stream session

stream selector

[add | set | rm | show]

add stream selector

Synopsis

add stream selector <name> <rule> ...

Description

Create stream selectors. A selector is an abstraction for a collection of PIXL expressions.

Parameters

name

The name of stream selector.

rule

The set of PIXL expressions.

Example

add stream selector sel_subnet HTTP.REQ.URL CLIENT.IP.SRC.SUBNET(24)

Top

set stream selector

Synopsis

set stream selector <name> -rule <expression> ...

Description

Change the set of expressions associated with the stream selector.

Parameters

name

The name of stream selector.

rule

The set of PIXL expressions.

Example

set stream sel_subnet HTTP.REQ.URL CLIENT.IP.SRC

Top

rm stream selector

Synopsis

rm stream selector <name>

Description

The command deletes the stream selector.

Parameters

name

The name of stream selector.

Example

rm stream selector sel_subnet

Top

show stream selector

Synopsis

show stream selector [<name>]

Description

Display selectors.

Parameters

name

The name of stream selector.

Example

show ns limitSelector sel_subnet

Top

stream identifier

[add | set | unset | rm | show | stat]

add stream identifier

Synopsis

add stream identifier <name> <selectorName> [-interval <positive_integer>] [-SampleCount <positive_integer>] [-sort <sort>]

Parameters

name

The name of stream identifier.

selectorName

The name of stream selector.

interval

Time interval in minutes for holding on the objects. Default value: 1 Minimum value: 1

SampleCount

Sample count 1 in sample count objects to be sampled. Default value: 1 Minimum value: 1 Maximum value: 65535

sort

Attribute on which the objects will be sorted on which summarized expressions will be performed. Possible values: REQUESTS, CONNECTIONS, RESPTIME, BANDWIDTH, NONE Default value: STREAM_DIMENSION_REQUESTS

Top

set stream identifier

Synopsis

set stream identifier <name> [-selectorName <string>] [-interval <positive_integer>] [-SampleCount <positive_integer>] [-sort <sort>]

Parameters

name

The name of stream identifier.

selectorName

The name of stream selector.

interval

Time interval in minutes for holding on the objects. Default value: 1 Minimum value: 1

SampleCount

Sample count 1 in sample count objects to be sampled. Default value: 1 Minimum value: 1 Maximum value: 65535

sort

Attribute on which the objects will be sorted on which summarized expressions will be performed. Possible values: REQUESTS, CONNECTIONS, RESPTIME, BANDWIDTH, NONE Default value: STREAM_DIMENSION_REQUESTS

Top

unset stream identifier

Synopsis

unset stream identifier <name> [-selectorName] [-interval] [-SampleCount] [-sort]

Description

Use this command to remove stream identifier settings.Refer to the set stream identifier command for meanings of the arguments.

Top

rm stream identifier

Synopsis

rm stream identifier <name>

Parameters

name

The name of stream identifier.

Top

show stream identifier

Synopsis

show stream identifier [<name>]

Parameters

name

The name of stream identifier.

Top

stat stream identifier

Synopsis

stat stream identifier <name> [<pattern> ...] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-sortBy <sortBy> [<sortOrder>]]

Description

Display statistics of a identifier.

Parameters

name

The name of the identifier.

pattern

Pattern for the selector field, ? means field is required, * means field value does not matter, anything else is a regular pattern

Top

stream session

clear stream session

Synopsis

clear stream session <name>

Parameters

name

The name of the identifier.

System Commands

This group of commands can be used to perform operations on the following entities:

- system
- system cmdPolicy
- system user
- system group
- system session
- system cpu
- system memory
- system entitydata
- system entity
- system globaldata
- system counters
- system countergroup
- system eventhistory
- system core
- system dataSource
- system global
- system collectionparam
- system parameter

system

stat system

Synopsis

stat system [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

This command displays system statistics

system cmdPolicy

[add | rm | set | show]

add system cmdPolicy

Synopsis

add system cmdPolicy <policyName> <action> <cmdSpec>

Description

Add a system command Policy to the system.

Parameters

policyName

The name for the command policy.

action

The action the policy need to apply when the cmdSpec pattern matches. Possible values: ALLOW, DENY

cmdSpec

The matching rule that the policy will utilize. This rule is a regular expression which the policy uses to pattern match.

Top

rm system cmdPolicy

Synopsis

rm system cmdPolicy <policyName>

Description

Remove a system command policy.

Parameters

policyName

The name of the policy.

Top

set system cmdPolicy

Synopsis

set system cmdPolicy <policyName> <action> <cmdSpec>

Description

Modify an already configured command Policy.

Parameters

policyName

The name for the command policy.

action

The action the policy need to apply when the cmdSpec pattern matches. Possible values: ALLOW, DENY

cmdSpec

The matching rule that the policy will utilize. This rule is a regular expression which the policy uses to pattern match.

Top

show system cmdPolicy

Synopsis

show system cmdPolicy [<policyName>]

Description

Display configured command policies.

Parameters

policyName

The name of a policy.

Top

system user

[add | rm | set | unset | bind | unbind | show]

add system user

Synopsis

add system user <userName> [-promptString <string>] [-timeout <secs>]

Description

Add a new system user to the system.

Parameters

userName

The name for the system user.

password

The system user's password.

promptString

The system user's prompt.

timeout

CLI session inactivity timeout, in seconds. Timeout cannot have values in between 1 and 9. Maximum value: 100000000

Top

rm system user

Synopsis

rm system user <userName>

Description

Remove a system user.

Parameters

userName

The name of the system user.

Top

set system user

Synopsis

set system user <userName> {-password } [-promptString <string>] [-timeout <secs>]

Description

Set a system user's password.

Parameters

userName

The name for the system user.

password

The system user's password.

promptString

The system user's prompt.

timeout

CLI session inactivity timeout, in seconds. Timeout cannot have values in between 1 and 9. Maximum value: 100000000

Top

unset system user

Synopsis

unset system user <userName> [-promptString] [-timeout]

Description

Use this command to remove system user settings.Refer to the set system user command for meanings of the arguments.

Top

bind system user

Synopsis

bind system user <userName> <policyName> <priority>

Description

Bind the command policy to a system user.

Parameters

userName

The name of the system user.

policyName

The name of the command policy being bound to the system user.

Top

unbind system user

Synopsis

unbind system user <userName> <policyName>

Description

Unbind attributes of a system user.

Parameters

userName

The name of the system user.

policyName

The name of the command policy to be unbound.

Top

show system user

Synopsis

show system user [<userName>]

Description

Display configured system users.

Parameters

userName

The name of a system user.

Top

system group

[add | rm | bind | unbind | show | set | unset]

add system group

Synopsis

add system group <groupName> [-promptString <string>] [-timeout <secs>]

Description

Add a new system group.

Parameters

groupName

The name of system group.

promptString

The system group's prompt.

timeout

CLI session inactivity timeout, in seconds. Timeout cannot have values in between 1 and 9. Maximum value: 100000000

Top

rm system group

Synopsis

rm system group <groupName>

Description

Remove a system group.

Parameters

groupName

The name of the system group.

Top

bind system group

Synopsis

bind system group <groupName> [-userName <string>] [-policyName <string> <priority>]

Description

Bind entities to a system group.

Parameters

groupName

The name of the system group.

userName

The name of a system user to be bound to the group.

policyName

The name of the command policy to be bound to the group.

Top

unbind system group

Synopsis

unbind system group <groupName> [-userName <string>] [-policyName <string>]

Description

Unbind entities from a system group.

Parameters

groupName

The system group name.

userName

The name of a system user to be unbound from the group.

policyName

The command policy to be be unbound from the group.

Top

show system group

Synopsis

show system group [<groupName>]

Description

Display the configured system groups.

Parameters

groupName

The name of the system group.

Top

set system group

Synopsis

set system group <groupName> [-promptString <string>] [-timeout <secs>]

Description

Set attributes of a system group.

Parameters

groupName

The name of system group.

promptString

The system group's prompt.

timeout

CLI session inactivity timeout, in seconds. Timeout cannot have values in between 1 and 9. Maximum value: 100000000

Top

unset system group

Synopsis

unset system group <groupName> [-promptString] [-timeout]

Description

Use this command to remove system group settings.Refer to the set system group command for meanings of the arguments.

Top

system session

[show | kill]

show system session

Synopsis

show system session [<sid>]

Description

Display system sessions. System may reclaim sessions with no active connections before expiry time

Parameters

sid

The session id. Minimum value: 1

Top

kill system session

Synopsis

kill system session (<sid> | -all)

Description

Kill system sessions.

Parameters

sid

The session id. Minimum value: 1

all

Specify this if you want to kill all sessions except self.

Top

system cpu

stat system cpu

Synopsis

stat system cpu [<id>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

This command displays CPU statistics

Parameters

id

Specifies the CPU ID. Default value: 65535 Maximum value: 65534

system memory

stat system memory

Synopsis

stat system memory [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display NetScaler global memory statistics

Example

stat system memory

system entitydata

[rm | show]

rm system entitydata

Synopsis

rm system entitydata [<type>] [<name>] [-allDeleted] [-allInactive] [-dataSource <string>] [-core <integer>]

Parameters

type

Specify the entity type.

name

Specify the entity name.

allDeleted

Specify this if you would like to deleted all deleted entity database.

allInactive

Specify this if you would like to deleted all inactive entity database.

dataSource

Specify data source name.

core

Specify core.

Top

show system entitydata

Synopsis

show system entitydata <type> <name> <counters> [-startTime <string> | (-last <integer> [<unit>])] [-endTime <string>] [-dataSource <string>] [-core <integer>]

Description

Display historical data for global counters.

Parameters

type

Specify the entity type.

name

Specify the entity name.

counters

Specify the counters.

startTime

Specify end time in mmddyyyyhhmm.

endTime

Specify end time in mmddyyyyhhmm.

last

Specify the counters. Default value: 1

dataSource

Specify Data source name.

core

Specify core.

Example

show system entitydata lbvserver v1 totalrequests -last 1 days

Top

system entity

show system entity

Synopsis

show system entity <type> [-dataSource <string>] [-core <integer>]

Description

Display entities in historical data.

Parameters

type

Specify the entity type.

dataSource

Specify Data source name.

core

Specify core.

Example

show system entity lbvserver

system globaldata

show system globaldata

Synopsis

show system globaldata <counters> [<countergroup>] [-startTime <string> | (-last <integer> [<unit>])] [-endTime <string>] [-dataSource <string>] [-core <integer>]

Description

Display historical data for global counters.

Parameters

counters

Specify the counters.

countergroup

Specify the counter group.

startTime

Specify start time in mmddyyyyhhmm.

endTime

Specify end time in mmddyyyyhhmm.

last

Specify the counters. Default value: 1

dataSource

Specify data source name.

core

Specify core.

Example

show system globaldata cpu_usage -last 1 hours

system counters

show system counters

Synopsis

show system counters [<countergroup>] [-dataSource <string>]

Description

Display entities in historical data.

Parameters

countergroup

Specify the group name.

dataSource

Specify Data source name.

system countergroup

show system countergroup

Synopsis

show system countergroup [-dataSource <string>]

Description

Display available counter groups.

Parameters

dataSource

Specify Data source name.

system eventhistory

show system eventhistory

Synopsis

show system eventhistory [-startTime <string> | (-last <integer> [<unit>])] [-endTime <string>] -dataSource <string>

Description

Display events in historical data.

Parameters

startTime

Specify start time in mmddyyyyhhmm.

endTime

Specify end time in mmddyyyyhhmm.

last

Specify the counters. Default value: 1

dataSource

Specify Data source name.

system core

show system core

Synopsis

show system core [-dataSource <string>]

Description

Display entities in historical data.

Parameters

dataSource

Specify Data source name.

system dataSource

show system dataSource

Synopsis

show system dataSource [<dataSource>]

Description

Display entities in historical data.

Parameters

dataSource

Specify Data source name.

system global

[bind | unbind | show]

bind system global

Synopsis

bind system global [<policyName> [-priority <positive_integer>]]

Description

Bind entities to system global.

Parameters

policyName

The name of the command policy to be bound to system global.

Top

unbind system global

Synopsis

unbind system global <policyName>

Description

Unbind entities from system global.

Parameters

policyName

The name of the command policy to be unnbound.

Top

show system global

Synopsis

show system global

Description

Display system global bindings.

Top

system collectionparam

[set | unset | show]

set system collectionparam

Synopsis

set system collectionparam [-communityName <string>] [-dataPath <string>]

Description

Set a collection parameters.

Parameters

dataPath

specify the data path

Top

unset system collectionparam

Synopsis

unset system collectionparam [-communityName] [-dataPath]

Description

Use this command to remove system collectionparam settings.Refer to the set system collectionparam command for meanings of the arguments.

Top

show system collectionparam

Synopsis

show system collectionparam

Description

Display collection parameter

Top

system parameter

[set | unset | show]

set system parameter

Synopsis

set system parameter [-rbaOnResponse (ENABLED | DISABLED)] [-promptString <string>] [-natPcbForceFlushLimit <positive_integer>] [-natPcbRstOnTimeout (ENABLED | DISABLED)] [-timeout <secs>]

Description

Set System parameters.

Parameters

rbaOnResponse

specify whether RBA on response is enabled/disabled Possible values: ENABLED, DISABLED Default value: ENABLED

promptString

The global system CLI prompt.

natPcbForceFlushLimit

force flush if number of NATPCBs above this Default value: 2147483647 Minimum value: 1000

natPcbRstOnTimeout

Send RST to client and server connections when the natpcbs timeout. This avoids the buildup of idle TCP connections on the both the sides. Possible values: ENABLED, DISABLED Default value: DISABLED

timeout

CLI session inactivity timeout, in seconds. Timeout cannot have values in between 1 and 9. Maximum value: 100000000

Top

unset system parameter

Synopsis

unset system parameter [-rbaOnResponse] [-promptString] [-natPcbForceFlushLimit] [-natPcbRstOnTimeout] [-timeout]

Description

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

Top

show system parameter

Synopsis

show system parameter

Description

Get System parameters.

Top

TM Commands

This group of commands can be used to perform operations on the following entities:

- tm sessionPolicy
- tm sessionAction
- tm trafficPolicy
- tm formSSOAction
- tm trafficAction
- tm global
- tm sessionParameter

tm sessionPolicy

[add | rm | set | unset | show]

add tm sessionPolicy

Synopsis

add tm sessionPolicy <name> <rule> <action>

Description

Add a tm session policy, which conditionally sets characteristics of a tm session upon session establishment.

Parameters

name

The name for the new tm session policy.

rule

The rule to be evaluated in the policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

action

The action to be performed when the rule is matched.

Top

rm tm sessionPolicy

Synopsis

rm tm sessionPolicy <name>

Description

Remove a previously created tm session policy.

Parameters

name

The name of the policy to be removed.

Top

set tm sessionPolicy

Synopsis

set tm sessionPolicy <name> [-rule <expression>] [-action <string>]

Description

Modify the rule or action of a tm session policy.

Parameters

name

The name of the tm session policy.

rule

The new rule to be associated with the policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

action

The new tm session action for the policy.

Top

unset tm sessionPolicy

Synopsis

unset tm sessionPolicy <name> [-rule] [-action]

Description

Use this command to remove tm sessionPolicy settings.Refer to the set tm sessionPolicy command for meanings of the arguments.

Top

show tm sessionPolicy

Synopsis

show tm sessionPolicy [<name>]

Description

Display the configured tm session policies.

Parameters

name

The name of the tm session policy.

Top

tm sessionAction

[add | rm | set | unset | show]

add tm sessionAction

Synopsis

add tm sessionAction <name> [-sessTimeout <mins>] [-defaultAuthorizationAction (ALLOW | DENY)] [-SSO (ON | OFF)] [-ssoCredential (PRIMARY | SECONDARY)] [-ssoDomain <string>] [-httpOnlyCookie (YES | NO)] [-persistentCookie (ON | OFF)] [-persistentCookieValidity <mins>]

Description

Create a session action, which defines the properties of a TM session.

Parameters

name

The name for the new tm session action.

sessTimeout

The session timeout, in minutes, to be set by the action. Minimum value: 1

defaultAuthorizationAction

This toggles the default authorization action to either ALLOW or DENY. Possible values: ALLOW, DENY

SSO

Enables or disables the use of Single Sign-on for the session. Possible values: ON, OFF Default value: OFF

ssoCredential

The set of user credentials (primary or secondary) to use for Single Sign-On Possible values: PRIMARY, SECONDARY

ssoDomain

NT domain to use with SSO

httpOnlyCookie

whether the session cookie will be httpOnly or not Possible values: YES, NO

persistentCookie

Whether persistent cookie should be allowed on this TM session Possible values: ON, OFF

persistentCookieValidity

Number of minutes for which the persistent cookie would be valid Minimum value: 1

Top

rm tm sessionAction

Synopsis

rm tm sessionAction <name>

Description

Delete a previously created session action.

Parameters

name

The tm session action to be removed.

Top

set tm sessionAction

Synopsis

set tm sessionAction <name> [-sessTimeout <mins>] [-defaultAuthorizationAction (ALLOW | DENY)] [-SSO (ON | OFF)] [-ssoCredential (PRIMARY | SECONDARY)] [-ssoDomain <string>] [-httpOnlyCookie (YES | NO)] [-persistentCookie (ON | OFF)] [-persistentCookieValidity <positive_integer>]

Description

Modify a session action, which defines the properties of a TM session.

Parameters

name

The name of the tm session action.

sessTimeout

The session timeout, in minutes, to be set by the action. Minimum value: 1

defaultAuthorizationAction

This toggles the default authorization action to either ALLOW or DENY. Possible values: ALLOW, DENY

SSO

Enables or disables the use of Single Sign-on for the session. Possible values: ON, OFF Default value: OFF

ssoCredential

The set of user credentials (primary or secondary) to use for Single Sign-On Possible values: PRIMARY, SECONDARY

ssoDomain

NT domain to use with SSO

httpOnlyCookie

whether the session cookie will be httpOnly or not Possible values: YES, NO

persistentCookie

Whether persistent cookie should be allowed on this TM session Possible values: ON, OFF

persistentCookieValidity

Number of minutes for which the persistent cookie would be valid Minimum value: 1

Top

unset tm sessionAction

Synopsis

unset tm sessionAction <name> [-sessTimeout] [-defaultAuthorizationAction] [-SSO] [-ssoCredential] [-ssoDomain] [-httpOnlyCookie] [-persistentCookie] [-persistentCookieValidity]

Description

Use this command to remove tm sessionAction settings.Refer to the set tm sessionAction command for meanings of the arguments.

Top

show tm sessionAction

Synopsis

show tm sessionAction [<name>]

Description

Display tm session action details.

Parameters

name

The name of the tm session action.

Top

tm trafficPolicy

[add | rm | set | unset | show | stat]

add tm trafficPolicy

Synopsis

add tm trafficPolicy <name> <rule> <action>

Description

Add a traffic policy. A traffic policy conditionally sets VPN traffic characteristics at run time.

Parameters

name

The name for the new vpn traffic policy.

rule

The rule to be used by the vpn traffic policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

action

The action to be applied by the policy if its rule is matched.

Top

rm tm trafficPolicy

Synopsis

rm tm trafficPolicy <name>

Description

Remove a vpn traffic policy.

Parameters

name

The name of the vpn traffic policy to be removed.

Top

set tm trafficPolicy

Synopsis

set tm trafficPolicy <name> [-rule <expression>] [-action <string>]

Description

Change the properties of an existing traffic policy.

Parameters

name

The name of the policy.

rule

The new rule to be used in the policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

action

The new action to be applied by the policy.

Top

unset tm trafficPolicy

Synopsis

unset tm trafficPolicy <name> [-rule] [-action]

Description

Use this command to remove tm trafficPolicy settings.Refer to the set tm trafficPolicy command for meanings of the arguments.

Top

show tm trafficPolicy

Synopsis

show tm trafficPolicy [<name>]

Description

Display vpn traffic policies.

Parameters

name

The name of the vpn trafiic policy.

Top

stat tm trafficPolicy

Synopsis

stat tm trafficPolicy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display Traffic Management traffic policy statistics.

Parameters

name

The name of the TM traffic policy for which statistics will be displayed. If not given statistics are shown for all policies.

Example

stat tm trafficpolicy.

Top

tm formSSOAction

[add | rm | set | unset | show]

add tm formSSOAction

Synopsis

add tm formSSOAction <name> -actionURL <URL> -userField <string> -passwdField <string> -ssoSuccessRule <expression> [-nameValuePair <string>] [-responsesize <positive_integer>] [-nvtype (STATIC | DYNAMIC)] [-submitMethod (GET | POST)]

Description

Create a formsso action. A formsso action defines the characteristics of the form.

Parameters

name

The name for the action.

actionURL

The url to which form will be submitted.

userField

Username field in the form to be filled with sessions username.

passwdField

Password field in the form to be filled with sessions username.

ssoSuccessRule

The rule to be used to check whether sso is successfull or not . Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

nameValuePair

Name Value pairs to be submitted. Name value pairs have to separated by '&'. EX: name1=value1&name2=value2

responsesize

Size of the body to be parsed to get the forms. Default value: 8096

nvtype

Bypass Form extraction. Possible values: STATIC, DYNAMIC Default value: NS_ACT_FSSO_NV_DYNAMIC

submitMethod

submit method Possible values: GET, POST Default value: NS_ACT_FSSO_SUBMIT_GET

Top

rm tm formSSOAction

Synopsis

rm tm formSSOAction <name>

Description

Delete a previously created session action.

Parameters

name

The Form sso action to be removed.

Top

set tm formSSOAction

Synopsis

set tm formSSOAction <name> [-actionURL <URL>] [-userField <string>] [-passwdField <string>] [-ssoSuccessRule <expression>] [-responsesize <positive_integer>] [-nameValuePair <string>] [-nvtype (STATIC | DYNAMIC)] [-submitMethod (GET | POST)]

Description

Create a vpn traffic action. A vpn traffic action defines the characteristics of run time VPN traffic.

Parameters

name

The name for the action.

actionURL

Set the url to which form will be submitted.

userField

Set the username field.

passwdField

Set the password field.

ssoSuccessRule

Set the success rule.

responsesize

Set the body size to be parsed Default value: 8096

nameValuePair

Set the name value pair.

nvtype

Bypass Form extraction. Possible values: STATIC, DYNAMIC Default value: NS_ACT_FSSO_NV_DYNAMIC

submitMethod

Submit method. Possible values: GET, POST Default value: NS_ACT_FSSO_SUBMIT_GET

Top

unset tm formSSOAction

Synopsis

unset tm formSSOAction <name> [-responsesize] [-nameValuePair] [-nvtype] [-submitMethod]

Description

Use this command to remove tm formSSOAction settings.Refer to the set tm formSSOAction command for meanings of the arguments.

Top

show tm formSSOAction

Synopsis

show tm formSSOAction [<name>]

Description

Display Form SSO action details.

Parameters

name

The name for the action.

Top

tm trafficAction

[add | rm | set | unset | show]

add tm trafficAction

Synopsis

add tm trafficAction <name> [-appTimeout <mins>] [-SSO (ON | OFF) [-formSSOAction <string>]] [-persistentCookie (ON | OFF)] [-InitiateLogout (ON | OFF)]

Description

Create a tm traffic action. A tm traffic action defines the characteristics of run time tm traffic.

Parameters

name

The name for the action.

appTimeout

The inactivity timeout after which the system closes a connection. Minimum value: 1 Maximum value: 715827

SSO

Enable or disable Single Sign-On Possible values: ON, OFF

formSSOAction

Name of configured tm formssoaction

persistentCookie

Whether persistent cookie should be allowed on this traffic action Possible values: ON, OFF

InitiateLogout

Initiate Logout on this session Possible values: ON, OFF

Top

rm tm trafficAction

Synopsis

rm tm trafficAction <name>

Description

Remove a previously created traffic action.

Parameters

name

The name of the action to be removed.

Top

set tm trafficAction

Synopsis

set tm trafficAction <name> [-appTimeout <mins>] [-SSO (ON | OFF)] [-formSSOAction <string>] [-persistentCookie (ON | OFF)] [-InitiateLogout (ON | OFF)]

Description

Modifies a vpn traffic action. A vpn traffic action defines the characteristics of run time VPN traffic.

Parameters

name

The name for the action.

appTimeout

The inactivity timeout after which the system closes a connection. Minimum value: 1 Maximum value: 715827

SSO

switch to turn on the SSO engine for HTTP traffic. Possible values: ON, OFF

formSSOAction

Name of configured tm formssoaction

persistentCookie

Whether persistent cookie should be allowed on this TM session Possible values: ON, OFF

InitiateLogout

switch to turn on the Logout of TM session. Possible values: ON, OFF

Top

unset tm trafficAction

Synopsis

unset tm trafficAction <name> -persistentCookie

Description

Use this command to remove tm trafficAction settings.Refer to the set tm trafficAction command for meanings of the arguments.

Top

show tm trafficAction

Synopsis

show tm trafficAction [<name>]

Description

Display the configured vpn traffic action(s).

Parameters

name

The name of the vpn trafiic action.

Top

tm global

[bind | unbind | show]

bind tm global

Synopsis

bind tm global [-policyName <string> [-priority <positive_integer>]]

Description

Bind session/audit policies to tm global.

Parameters

policyName

The name of the policy to be bound to tm global.

Top

unbind tm global

Synopsis

unbind tm global -policyName <string>

Description

Unbind audit/session policies from tm global.

Parameters

policyName

The name of the policy to be unbound.

Top

show tm global

Synopsis

show tm global

Description

Display the tm global bindings.

Top

tm sessionParameter

[set | unset | show]

set tm sessionParameter

Synopsis

set tm sessionParameter [-sessTimeout <mins>] [-defaultAuthorizationAction (ALLOW | DENY)] [-SSO (ON | OFF)] [-ssoCredential (PRIMARY | SECONDARY)] [-ssoDomain <string>] [-httpOnlyCookie (YES | NO)] [-persistentCookie (ON | OFF)] [-persistentCookieValidity <positive_integer>]

Description

Set global parameters for the tm session

Parameters

sessTimeout

The session idle timeout value in minutes. This idle timeout meters the overall network inactivity for a session. Default value: 30 Minimum value: 1

defaultAuthorizationAction

The authorization action state. Toggles the default authorization action to either ALLOW or DENY. Possible values: ALLOW, DENY Default value: NS_ALLOW

SSO

Whether or not Single Sign-On is used Possible values: ON, OFF Default value: OFF

ssoCredential

The set of user credentials (primary or secondary) to use for Single Sign-On Possible values: PRIMARY, SECONDARY Default value: VPN_SESS_ACT_USE_PRIMARY_CREDENTIALS

ssoDomain

NT domain to use with SSO

httpOnlyCookie

whether the session cookie will be httpOnly or not Possible values: YES, NO Default value: VPN_SESS_ACT_HTTPONLYCOOKIE_ALLOW

persistentCookie

Whether persistent cookie should be allowed on this TM session Possible values: ON, OFF Default value: OFF

persistentCookieValidity

Number of minutes for which the persistent cookie would be valid Minimum value: 1

Top

unset tm sessionParameter

Synopsis

unset tm sessionParameter [-sessTimeout] [-SSO] [-ssoDomain] [-persistentCookie] [-defaultAuthorizationAction] [-ssoCredential] [-httpOnlyCookie] [-persistentCookieValidity]

Description

Unset parameters for the tm session.Refer to the set tm sessionParameter command for meanings of the arguments.

Top

show tm sessionParameter

Synopsis

show tm sessionParameter

Description

Display the configured tm session parameters.

Top

Transform Commands

This group of commands can be used to perform operations on the following entities:

- transform profile
- transform action
- transform policy
- transform policylabel
- transform global

transform profile

[add | rm | set | unset | show]

add transform profile

Synopsis

add transform profile <name> [-type URL]

Description

Create a URL Transformation profile.

Parameters

name

URL Transformation profile name.

type

Type of transformation. Possible values: URL

Top

rm transform profile

Synopsis

rm transform profile <name>

Description

Remove a URL Transformation profile.

Parameters

name

URL Transformation profile name.

Top

set transform profile

Synopsis

set transform profile <name> [-type URL] [-onlyTransformAbsURLinBody (ON | OFF)] [-comment <string>]

Description

Modify URL Transformation action settings.

Parameters

name

URL Transformation action name.

type

Type of transformation. Possible values: URL

onlyTransformAbsURLinBody

Flag to only perform transformations of absolute URLs in HTTP body. Possible values: ON, OFF

comment

Comments.

Top

unset transform profile

Synopsis

unset transform profile <name> [-type] [-onlyTransformAbsURLinBody] [-comment]

Description

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

Top

show transform profile

Synopsis

show transform profile [<name>]

Description

Display the configured URL Transformation profiles.

Parameters

name

URL Transformation profile name.

Top

transform action

[add | rm | set | unset | show]

add transform action

Synopsis

add transform action <name> <profileName> <priority> [-state (ENABLED | DISABLED)]

Description

Create a URL Transformation action.

Parameters

name

URL Transformation action name.

profileName

URL Transformation profile name.

priority

Priority of the Action within the Profile. Minimum value: 1 Maximum value: 2147483647

state

Enabled flag. Possible values: ENABLED, DISABLED Default value: GENENABLED

Top

rm transform action

Synopsis

rm transform action <name>

Description

Remove a URL Transformation action.

Parameters

name

URL Transformation action name.

Top

set transform action

Synopsis

set transform action <name> [-priority <positive_integer>] [-reqUrlFrom <expression>] [-reqUrlInto <expression>] [-resUrlFrom <expression>] [-resUrlInto <expression>] [-cookieDomainFrom <expression>] [-cookieDomainInto <expression>] [-state (ENABLED | DISABLED)] [-comment <string>]

Description

Modify URL Transformation action settings.

Parameters

name

URL Transformation action name.

priority

Priority of the Action within the Profile. Minimum value: 1 Maximum value: 2147483647

reqUrlFrom

Pattern of original request URLs. It corresponds to the way external users view the server, and acts as a source for request transformations.

reqUrlInto

Pattern of transformed request URLs. It corresponds to internal addresses and indicates how they are created.

resUrlFrom

Pattern of original response URLs. It corresponds to the way external users view the server, and acts as a source for response transformations.

resUrlInto

Pattern of transformed response URLs. It corresponds to internal addresses and indicates how they are created.

cookieDomainFrom

Pattern of the original domain in Set-Cookie headers.

cookieDomainInto

Pattern of the transformed domain in Set-Cookie headers.

state

Enabled flag. Possible values: ENABLED, DISABLED Default value: GENENABLED

comment

Comments.

Top

unset transform action

Synopsis

unset transform action <name> [-priority] [-reqUrlFrom] [-reqUrlInto] [-resUrlFrom] [-resUrlInto] [-cookieDomainFrom] [-cookieDomainInto] [-state] [-comment]

Description

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

Top

show transform action

Synopsis

show transform action [<name>]

Description

Display the configured URL Transformation action.

Parameters

name

URL Transformation profile name.

Top

transform policy

[add | rm | set | unset | show | stat | rename]

add transform policy

Synopsis

add transform policy <name> <rule> <profileName> [-comment <string>] [-logAction <string>]

Description

Create a URL Transformation policy.

Parameters

name

URL Transformation policy name.

rule

The rule associated with the policy.

profileName

URL Transformation profile name.

comment

Comments associated with this transform policy.

logAction

The log action associated with the transform policy

Top

rm transform policy

Synopsis

rm transform policy <name>

Description

Remove a URL Transformation policy.

Parameters

name

URL Transformation policy name.

Example

rm transform policy trans_pol

Top

set transform policy

Synopsis

set transform policy <name> [-rule <expression>] [-profileName <string>] [-comment <string>] [-logAction <string>]

Description

Set a new rule/profile/comment for existing transform policy.

Parameters

name

URL Transformation policy name.

rule

The rule associated with the policy.

profileName

URL Transformation profile name.

comment

Comments associated with this transform policy.

logAction

The log action associated with the transform policy

Example

set transform policy pol9 -rule "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

Top

unset transform policy

Synopsis

unset transform policy <name> [-comment] [-logAction]

Description

Unset comment/logaction for existing transform policy..Refer to the set transform policy command for meanings of the arguments.

Example

unset transform policy pol9 -undefAction

Top

show transform policy

Synopsis

show transform policy [<name>]

Description

Display the Url Transform policies.

Parameters

name

URL Transformation policy name.

Top

stat transform policy

Synopsis

stat transform policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display transform policy statistics.

Parameters

name

The name of the transform policy for which statistics will be displayed. If not given statistics are shown for all transform policies.

Example

stat transform policy

Top

rename transform policy

Synopsis

rename transform policy <name>@ <newName>@

Description

Rename a transform policy.

Parameters

name

The name of the transform policy.

newName

The new name of the transform policy.

Example

rename transform policy oldname newname

Top

transform policylabel

[add | rm | bind | unbind | show | stat | rename]

add transform policylabel

Synopsis

add transform policylabel <labelName> <policylabeltype>

Description

Add a transform policy label.

Parameters

labelName

Name of the transform policy label.

policylabeltype

The type of transformations allowed by the policies bound to the label. Possible values: http_req

Example

add transform policylabel trans_policylabel http_req

Top

rm transform policylabel

Synopsis

rm transform policylabel <labelName>

Description

Remove a transform policy label.

Parameters

labelName

Name of the transform policy label.

Example

rm transform policylabel trans_policylabel

Top

bind transform policylabel

Synopsis

bind transform policylabel <labelName> <policyName> <priority> [<gotoPriorityExpression>] [-invoke (<labelType> <labelName>)]

Description

Bind the transform policy to one of the labels.

Parameters

labelName

Name of the transform policy label.

policyName

The transform policy name.

Example

i) bind transform policylabel trans_policylabel pol_1 1 2 -invoke reqvserver CURRENT
ii) bind transform policylabel trans_policylabel pol_2 2

Top

unbind transform policylabel

Synopsis

unbind transform policylabel <labelName> <policyName> [-priority <positive_integer>]

Description

Unbind entities from transform label.

Parameters

labelName

Name of the transform policy label.

policyName

The transform policy name.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind transform policylabel trans_policylabel pol_1

Top

show transform policylabel

Synopsis

show transform policylabel [<labelName>]

Description

Display policy label or policies bound to transform policylabel.

Parameters

labelName

Name of the transform policy label.

Example

i) show transform policylabel trans_policylabel
ii) show transform policylabel

Top

stat transform policylabel

Synopsis

stat transform policylabel [<labelName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display statistics of transform policylabel(s).

Parameters

labelName

The name of the transform policy label for which statistics will be displayed. If not given statistics are shown for all transform policylabels.

Top

rename transform policylabel

Synopsis

rename transform policylabel <labelName>@ <newName>@

Description

Rename a transform policy label.

Parameters

labelName

The name of the transform policylabel.

newName

The new name of the transform policylabel.

Example

rename transform policylabel oldname newname

Top

transform global

[bind | unbind | show]

bind transform global

Synopsis

bind transform global <policyName> <priority> [<gotoPriorityExpression>] [-type (REQ_OVERRIDE | REQ_DEFAULT)] [-invoke (<labelType> <labelName>)]

Description

Bind the Url Transform policy globally

Parameters

policyName

Name of the policy to be bound to URL transform global.

Example

bind transform global pol9 9

Top

unbind transform global

Synopsis

unbind transform global <policyName> [-type (REQ_OVERRIDE | REQ_DEFAULT)] [-priority <positive_integer>]

Description

Unbind globally bound Url Transform policy.

Parameters

policyName

The name of the policy to be unbound.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind transform global pol9

Top

show transform global

Synopsis

show transform global [-type (REQ_OVERRIDE | REQ_DEFAULT)]

Description

Display the transform global bindings.

Parameters

type

The bindpoint to which policy is bound. Possible values: REQ_OVERRIDE, REQ_DEFAULT

Example

show transform global

Top

Tunnel Commands

This group of commands can be used to perform operations on the following entities:

- tunnel trafficPolicy
- tunnel global

tunnel trafficPolicy

[add | rm | set | unset | show]

add tunnel trafficPolicy

Synopsis

add tunnel trafficPolicy <name> <rule> <action>

Description

Create a tunnel trafficpolicy.

Parameters

name

The name of the new tunnel trafficpolicy.

rule

The expression specifying the condition under which this policy is applied.

action

The name of the action to be performed. The string value may be one of the following built-in compression actions: COMPRESS: Enables default compression (DEFLATE). NOCOMPRESS: Disables compression. GZIP: Enables GZIP compression. DEFLATE: Enables DEFLATE compression.

Example

Example 1:
add tunnel trafficpolicy cmp_all_destport "REQ.TCP.DESTPORT == 0-65535" GZIP

After creating above tunnel policy, it can be activated by binding it globally:
bind tunnel global cmp_all_destport

The policy is evaluated for all traffic flowing through the ssl-vpn tunnel, and compresses traffic for all TCP a

Example 2:
The following tunnel policy disables compression for all access from a specific subnet:
add tunnel trafficpolicy local_sub_nocmp "SOURCEIP == 10.1.1.0 -netmask 255.255.255.0" NOCOMPRESS
bind tunnel global local_sub_nocmp

Top

rm tunnel trafficPolicy

Synopsis

rm tunnel trafficPolicy <name>

Description

Remove a tunnel traffic policy.

Parameters

name

The name of the tunnel traffic policy.

Example

rm tunnel trafficpolicy tunnel_policy_name
The "show tunnel trafficpolicy" command shows all tunnel policies that are currently defined.

Top

set tunnel trafficPolicy

Synopsis

set tunnel trafficPolicy <name> [-rule <expression>] [-action <string>]

Description

Modify the rule and/or action of an existing tunnel traffic policy, created using the "add tunnel trafficpolicy" command.

Parameters

name

The name of the policy to be modified.

rule

The new rule to be used in the policy.

action

The new action to be applied by the policy.

Example

```
add tunnel trafficpolicy cmp_all_destport "REQ.TCP.DESTPORT == 0-65535" GZIP
   set tunnel trafficpolicy cmp_all_destport -action NOCOMPRESS

   Above 'set' command changes action for policy cmp_all_destport from GZIP to NOCOMPRESS
```

Top

unset tunnel trafficPolicy

Synopsis

unset tunnel trafficPolicy <name> [-rule] [-action]

Description

Use this command to remove tunnel trafficPolicy settings.Refer to the set tunnel trafficPolicy command for meanings of the arguments.

Top

show tunnel trafficPolicy

Synopsis

show tunnel trafficPolicy [<name>]

Description

Display all tunnel policies that are currently defined.

Parameters

name

The name of the tunnel traffic policy.

Example

```
> show tunnel trafficpolicy
      2 Tunnel policies:
```

```
1) Name: local_sub_nocmp   Rule: SOURCEIP == 10.1.1.0 -netmask 255.255.255.0
   Action: NOCOMPRESS
   Hits: 3

2) Name: cmp_all   Rule: REQ.TCP.DESTPORT == 0-65535
   Action: GZIP
   Hits: 57125
   Bytes In:...796160       Bytes Out:... 197730
   Bandwidth saving...75.16%   Ratio 4.03:1
 Done
```

Top

tunnel global

[bind | unbind | show]

bind tunnel global

Synopsis

bind tunnel global (<policyName> [-priority <positive_integer>]) [-state (ENABLED | DISABLED)]

Description

Activate the tunnel traffic policy globally. The tunnel policies are created using the "add tunnel trafficpolicy" command. The command "show tunnel trafficpolicy" shows all the existing tunnel policies and the command "show tunnel global" shows all the globally active tunnel policies. Note that the ssl-vpn license is required for tunnel compression feature to work.

Parameters

policyName

The name of the tunnel traffic policy to be bound.

Example

add tunnel trafficpolicy cmp_all_destport "REQ.TCP.DESTPORT == 0-65535" GZIP

After creating above tunnel policy, it can be activated by binding it globally:
bind tunnel global cmp_all_destport

After binding cmp_all_destport compression policy globally, the policy gets activated and the NetScaler will

Globally active tunnel policies can be seen using command:
> show tunnel global
1 Globally Active Tunnel Policies:
1) Policy Name: cmp_all_destport Priority: 0
Done

Top

unbind tunnel global

Synopsis

unbind tunnel global <policyName>

Description

Deactivate an active tunnel traffic policy. Use command "show tunnel global" to see all the globally active tunnel policies.

Parameters

policyName

The name of the tunnel traffic policy.

Example

Globally active tunnel policies can be seen using command:
> show tunnel global
1 Globally Active Tunnel Policies:
1) Policy Name: cmp_all_destport Priority: 0
Done

The globally active tunnel traffic policy can be deactivated on the NetScaler system by issuing the command
unbind tunnel global cmp_all_destport

Top

show tunnel global

Synopsis

show tunnel global

Description

Display global active tunnel policies.

Example

> sh tunnel global
1) Policy Name: cmp_all_destport Priority: 0
2) Policy Name: local_sub_nocmp Priority: 500
Done

Top

Utility Commands

This group of commands can be used to perform operations on the following entities:

- nstrace
- scp
- shell
- install
- grep
- traceroute6
- traceroute
- ping6
- ping
- techsupport
- callhome

nstrace

nstrace

Synopsis

nstrace [-nf <positive_integer>] [-time <secs>] [-size <positive_integer>] [-mode <mode> ...] [-tcpdump (ENABLED | DISABLED) [-perNIC (ENABLED | DISABLED)]] [-name <string> [-id <string>]] [-filter <expression> [-link (ENABLED | DISABLED)]]

Description

Invoke nstrace program to log traffic flowing through netscaler

Parameters

h

prints this message - exclusive option

nf

number of files to be generated in cycle Default value: 24

time

Log in each trace file for 'time' seconds. (could be an expression) Default value: 3600

size

size of the packet to be logged(should be in the range of 60 to 1514 bytes). Setting size as zero, logs full packet. Default value: 164 Maximum value: 1514

m

Capturing mode: sum of the values: 1 - Transmitted packets (TX) 2 - Packets buffered for transmission (TXB) 4 - Received packets (RX) Default value: 6

tcpDump

nstrace-format, tcpdump-format Possible values: NSTRACE, TCPDUMP

mode

Capturing mode for trace. Mode can be any of the following values or combination of these values: RX Received packets before NIC pipelining NEW_RX Received packets after NIC pipelining TX Transmitted packets TXB Packets buffered for transmission IPV6 Translated IPv6 packets Default mode: NEW_RX TXB Default value: DEFAULT_MODE

tcpdump

Log files format supported:nstrace-format, tcpdump-format. default:nstrace-format Possible values: ENABLED, DISABLED Default value: DISABLED

name

Custom file name for nstrace files

filter

Filter expression for nstrace. Maximum length of filter is 255 and it can be of following format: <expression> [<relop> <expression>] <relop> = (&& | ||) <expression> = the expression string in the format: <qualifier> <operator> <qualifier-value> <qualifier> = SOURCEIP. <qualifier-value> = A valid IP address <qualifier> = SOURCEPORT. <qualifier-value> = A valid port number. <qualifier> = DESTIP. <qualifier-value> = A valid IP address. <qualifier> = DESTPORT. <qualifier-value> = A valid port number. <qualifier> = IP. <qualifier-value> = A valid IP address. <qualifier> = PORT. <qualifier-value> = A valid port number. <qualifier> = SVCNAME. <qualifier-value> = The name of a service. <qualifier> = VSVRNAME. <qualifier-value> = The name of a vserver. <qualifier> = CONNID <qualifier-value> = A valid PCB dev number. <qualifier> = VLAN <qualifier-value> = A valid VLAN ID. <qualifier> = INTF <qualifier-value> = A valid interface id in the form of x/y. <operator> = (== | eq | != | neq | > | gt | < | lt | >= | ge | <= | le | BETWEEN) eg: nstrace.sh -filter SOURCEIP == 10.102.34.201 || (SVCNAME != s1 && SOURCEPORT > 80) Filter expression should be given in doble quotes.

Example

nstrace -nf 10 -time 100 -mode RX IPV6 TXB -name abc -tcpdump ENABLED -perNIC ENABLED

scp

scp

Synopsis

scp [-r] [-C] [-q] <sourceString> <destString>

Description

Securely copy data from one computer to another via the ssh protocol.

Parameters

r

Recursively copy subdirectories

C

Enable compression

q

Quiet output - disable progress meter

sourceString

The source user, host and file path, specified as user@host:path/to/copy/from. User and host parts are optional.

destString

The destination user, host and file path, specified as user@host:path/to/copy/to. User and host parts are optional.

Example

scp /nsconfig/ns.conf nsroot@10.102.4.107:/nsconfig/

shell

shell

Synopsis

shell [(command)]

Description

Exit to the FreeBSD command prompt, where FreeBSD commands may be entered. Press the <Control> + <D> keys or type exit to return to the NetScaler system CLI prompt.

Parameters

command

The shell command(s) to be invoked.

Example

```
> shell
# ps | grep nscli
485  p0  S      0:01.12 -nscli (nscli)
590  p0  S+     0:00.00 grep nscli
# ^D  Done
> shell ps -aux |grep nscli
485  p0  S      0:01.12 -nscli (nscli)
590  p0  S+     0:00.00 grep nscli
```

install

install

Synopsis

install <url> [-c] [-y]

Description

Install a version of NetScaler software on the system. The command takes a single argument consisting of a valid URL for the HTTP, HTTPS, FTP, and SFTP protocols. Local files may be specified using the file:// URL variation. http://[user]:[password]@host/path/to/file https://[user]:[password]@host/path/to/file sftp://[user]:[password]@host/path/to/file scp://[user]:[password]@host/path/to/file ftp://[user]:[password]@host/path/to/file file://path/to/file

Parameters

url

http://[user]:[password]@host/path/to/file https://[user]:[password]@host/path/to/file sftp://[user]:[password]@host/path/to/file scp://[user]:[password]@host/path/to/file ftp://[user]:[password]@host/path/to/file file://path/to/file

c

Specifiy this option to backup existing kernel.

y

Specify this option to avoid prompt for yes/no i.e. reboot.

Example

install http://host.netscaler.com/ns-6.0-41.2.tgz

grep

grep

Synopsis

grep [-c] [-E] [-i] [-v] [-w] [-x] <pattern>

Description

grep to search files or output for lines containing a match to the given <pattern>. By default, grep prints the matching lines.

Parameters

c

Suppress normal output; instead print a count of matching lines. With the -v option, count non-matching lines.

E

Interpret <pattern> as an extended regular expression.

i

Ignore case distinctions.

v

Invert the sense of matching, to select non-matching lines.

w

Select only those lines containing matches that form whole words.

x

Select only those matches that exactly match the whole line.

pattern

The pattern (regular expression or text string) being sought.

Example

```
show ns info | grep off -i
```

traceroute6

traceroute6

Synopsis

traceroute6 [-n] [I] [-r] [-v] [-m <hoplimit>] [-p <port>] [-q <probes>] [-s <src_addr>] [-w <waittime>] <target> [<packetlen>]

Description

Invoke the UNIX traceroute6 command. Traceroute6 attempts to track the route that the packets follow to reach the destination host.

Parameters

n

Print hop addresses numerically rather than symbolically and numerically.

I

Use ICMP ECHO for probes

r

Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned.

v

Verbose output. Received ICMP packets other than TIME_EXCEEDED and UNREACHABLEs are listed.

m

The maximum hop value used in outgoing probe packets. Default value: 64 Minimum value: 1 Maximum value: 255

p

The base port number used in probes. Default value: 33434 Minimum value: 1 Maximum value: 65535

q

The number of probe per hop. Default value: 3 Minimum value: 1 Maximum value: 65535

s

The source IP address to be used in the outgoing query packets. If the IP address is not one of this machine's addresses, an error is returned and nothing is sent.

w

The time (in seconds) to wait for a response to a query. Default value: 5 Minimum value: 2 Maximum value: 86399

host

The destination host ip address or name.

packetlen

The packet length (in bytes) of the query packets. Default value: 44 Minimum value: 44 Maximum value: 32768

Example

traceroute6 2002::7

traceroute

traceroute

Synopsis

traceroute [-S] [-n] [-r] [-v] [-M <min_ttl] [-m <max_ttl>] [-P <protocol>][-p <portno>] [-q <nqueries>] [-s <src_addr>] [-t <tos>] [-w <wait>] <host> [<packetlen>]

Description

Invoke the UNIX traceroute command. Traceroute attempts to track the route that the packets follow to reach the destination host.

Parameters

S

Print a summary of how many probes were not answered for each hop.

n

Print hop addresses numerically rather than symbolically and numerically.

r

Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned.

v

Verbose output. Received ICMP packets other than TIME_EXCEEDED and UNREACHABLEs are listed.

M

The minimum ttl value used in outgoing probe packets. Default value: 1 Minimum value: 1 Maximum value: 255

m

The maximum TTL value used in outgoing probe packets. Default value: 64 Minimum value: 1 Maximum value: 255

P

Send packets of specified IP protocol. The currently supported protocols are UDP and ICMP.

p

The base port number used in probes. Default value: 33434 Minimum value: 1 Maximum value: 65535

q

The number of queries per hop. Default value: 3 Minimum value: 1 Maximum value: 65535

s

The source IP address to be used in the outgoing query packets. If the IP address is not one of this machine's addresses, an error is returned and nothing is sent.

t

The type-of-service in query packets. Maximum value: 255

w

The time (in seconds) to wait for a response to a query. Default value: 5 Minimum value: 2 Maximum value: 86399

host

The destination host ip address or name.

packetlen

The packet length (in bytes) of the query packets. Default value: 44 Minimum value: 44 Maximum value: 32768

Example

traceroute 10.102.4.107

ping6

ping6

Synopsis

ping6 [-c <count>] [-i <interval>] [-I <interface>] [-n] [-p <pattern>] [-q] [-S sourceaddr] [-V <vlanid>] [-s <size>] Hostname

Description

Invoke the UNIX ping6 command. The <hostName> option is used if the name is in /etc/hosts file directory or is otherwise known in DNS.

Parameters

c

Number of packets to send (default is infinite) Minimum value: 1 Maximum value: 65535

i

Waiting time in seconds (default is 1 sec) Maximum value: 65535

I

Network interface on which to ping6, if you have multiple interfaces

n

Numeric output only - no name resolution

p

Pattern to fill in packets. Can be up to 16 bytes, useful for diagnosing data-dependent problems.

q

Quiet output - only summary is printed

s

Data size in bytes (default is 56) Maximum value: 65507

V

VLAN ID for link local address Minimum value: 1 Maximum value: 4094

S

The source IP address to be used in the outgoing query packets.

t

Timeout in seconds before ping6 exits

hostName

Address of host to ping6

Example

```
ping6 -p ff -I 1/1 -c 4 2002::1
```

ping

ping

Synopsis

ping [-c <count>] [-i <interval>] [-I <interface>] [-n] [-p <pattern>] [-q] [-s <size>] [-S <src_addr>] [-t <timeout>] <hostname>

Description

Invoke the UNIX ping command. The <hostName> option is used if the name is in /etc/hosts file directory or is otherwise known in DNS.

Parameters

c

Number of packets to send (default is infinite) Minimum value: 1 Maximum value: 65535

i

Waiting time in seconds (default is 1 sec) Maximum value: 65535

I

Network interface on which to ping, if you have multiple interfaces

n

Numeric output only - no name resolution

p

Pattern to fill in packets. Can be up to 16 bytes, useful for diagnosing data-dependent problems.

q

Quiet output - only summary is printed

s

Data size in bytes (default is 56) Maximum value: 65507

S

The source IP address to be used in the outgoing query packets. If the IP addrESS Is not one of this machine's addresses, an error is returned and nothing is sent.

t

Timeout in seconds before ping exits Minimum value: 1 Maximum value: 3600

hostName

Address of host to ping

Example

ping -p ff -c 4 10.102.4.107

techsupport

show techsupport

Synopsis

show techsupport [-scope (NODE | CLUSTER)]

Description

This command generates a tar archive of system configuration data and statistics for submission to Citrix ANG technical support with file name collector_<NS IP>_<P/S>_<DateTime>.tgz. The archive is always pointed by the symbolic link /var/tmp/support/support.tgz for each invocation of the command.

Parameters

scope

Use this option to run showtechsupport on present node or all cluster nodes. Possible values: NODE, CLUSTER Default value: NS_TECH_NODE

Example

show techsupport

callhome

[show | set | unset]

show callhome

Synopsis

show callhome

Description

Displays the trigger events configured and the time when these events were triggered.

Example

```
show callhome
   E-mail address configured:xxx@yahoo.com

Trigger event              State    First occurrence            Latest occurrence
-------------              -----    ----------------            -----------------
1) Compact flash errors     Enabled  ..                          ..
2) Hard disk drive errors   Enabled  ..                          ..
3) Power supply unit failure Enabled  27 Aug 2010 18:22:47        28 Aug 2010 18:22:47
4) SSL card failure         Enabled  25 Aug 2010 18:22:47        26 Aug 2010 18:22:47
5) Warm restart             Enabled  N/A                         ..
```

Top

set callhome

Synopsis

set callhome -emailAddress e-mailaddress

Description

Sets the contact person's E-mail address

Parameters

emailAddress

The contact person's E-mail address

Example

set callhome -emailAddress xxxx@yahoo.com

Top

unset callhome

Synopsis

unset callhome -emailAddress

Description

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

Top

VPN Commands

This group of commands can be used to perform operations on the following entities:

- vpn
- vpn vserver
- vpn intranetApplication
- vpn nextHopServer
- vpn trafficPolicy
- vpn trafficAction
- vpn formSSOAction
- vpn url
- vpn sessionPolicy
- vpn sessionAction
- vpn clientlessAccessPolicy
- vpn clientlessAccessProfile
- vpn stats
- vpn icaConnection
- vpn global
- vpn parameter

vpn

stat vpn

Synopsis

stat vpn [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display VPN statistics.

vpn vserver

[add | rm | set | unset | bind | unbind | enable | disable | show | stat | rename]

add vpn vserver

Synopsis

add vpn vserver <name> <serviceType> (<IPAddress> [-range <positive_integer>]) <port> [-state (ENABLED | DISABLED)] [-authentication (ON | OFF)] [-doubleHop (ENABLED | DISABLED)] [-maxAAAUsers <positive_integer>] [-icaOnly (ON | OFF)] [-downStateFlush (ENABLED | DISABLED)] [-Listenpolicy <expression> [-Listenpriority <positive_integer>]] [-tcpProfileName <string>] [-httpProfileName <string>] [-comment <string>] [-appflowLog (ENABLED | DISABLED)] [-icmpVsrResponse (PASSIVE | ACTIVE)]

Description

Add a VPN virtual server.

Parameters

name

The name for the new vpn vserver.

serviceType

The vpn vserver's protocol type, e.g. SSL Possible values: SSL Default value: NSSVC_SSL

IPAddress

The IP address for the vpn vserver.

port

The TCP port on which the vserver listens. Minimum value: 1

state

The intital vserver server state, e.g. ENABLED or DISABLED Possible values: ENABLED, DISABLED Default value: ENABLED

authentication

This option toggles on or off the application of authentication of incoming users to the VPN. Possible values: ON, OFF Default value: ON

doubleHop

This option toggles on or off the application of authentication of incoming users to the VPN. Possible values: ENABLED, DISABLED Default value: DISABLED

maxAAAUsers

The maximum number of concurrent users allowed to login into this vserver at a time. The administrator can configure any number between 0 and 65535 for this virtual server, but the actual number of users allowed to login into this virtual server will also depend on the total number of user licenses and the total number of currently logged in users. Maximum value: 65535

icaOnly

This option tells whether ica only license feature is on or off. Possible values: ON, OFF Default value: OFF

downStateFlush

Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

Listenpolicy

Use this parameter to specify the listen policy for VPN Vserver. The string can be either an existing expression name (configured using add policy expression command) or else it can be an in-line expression with a maximum of 1500 characters. Default value: "none"

Listenpriority

Use this parameter to specify the priority for listen policy of VPN Vserver. Default value: 101 Maximum value: 100

tcpProfileName

The name of the TCP profile.

httpProfileName

Name of the HTTP profile.

comment

Comments associated with this virtual server.

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

icmpVsrResponse

Can be active or passive Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

Example

The following example creates a VPN vserver named myvpnvip which supports SSL portocol and with AAA fun
vserver myvpnvip SSL 65.219.17.34 443 -aaa ON

Top

rm vpn vserver

Synopsis

rm vpn vserver <name>@ ...

Description

Remove a virtual server.

Parameters

name

The name of the virtual server to be removed.

Example

rm vserver vpn_vip

Top

set vpn vserver

Synopsis

set vpn vserver <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-authentication (ON | OFF)] [-doubleHop (ENABLED | DISABLED)] [-icaOnly (ON | OFF)] [-maxAAAUsers <positive_integer>] [-downStateFlush (ENABLED | DISABLED)] [-Listenpolicy <expression>] [-Listenpriority <positive_integer>] [-tcpProfileName <string>] [-httpProfileName <string>] [-comment <string>] [-appflowLog (ENABLED | DISABLED)] [-icmpVsrResponse (PASSIVE | ACTIVE)]

Description

Change the parameters of a VPN virtual server.

Parameters

name

The name of the vserver to be modified.

IPAddress

The new IP address of the virtual server.

authentication

Indicates whether or not authentication is being applied to incoming users to the VPN. Possible values: ON, OFF Default value: ON

doubleHop

Indicates whether double hop functionality is enabled or not. Possible values: ENABLED, DISABLED Default value: DISABLED

icaOnly

Indicates whether ica only feature is enabled or not Possible values: ON, OFF Default value: OFF

maxAAAUsers

The maximum number of concurrent users allowed to login into this vserver at a time. The administrator can configure any number between 0 and 65535 for this virtual server, but the actual number of users allowed to login into this virtual server will also depend on the total number of user licenses and the total number of currently logged in users. Maximum value: 65535

downStateFlush

Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

Listenpolicy

Use this parameter to specify the listen policy for VPN Vserver. The string can be either an existing expression name (configured using add policy expression command) or else it can be an in-line expression with a maximum of 1500 characters. Default value: "none"

Listenpriority

Use this parameter to specify the priority for listen policy of VPN Vserver. Default value: 101 Maximum value: 100

tcpProfileName

The name of the TCP profile.

httpProfileName

Name of the HTTP profile.

comment

Comments associated with this virtual server.

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

icmpVsrResponse

Can be active or passive Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

Top

unset vpn vserver

Synopsis

unset vpn vserver <name> [-authentication] [-doubleHop] [-icaOnly] [-maxAAAUsers] [-downStateFlush] [-Listenpolicy] [-Listenpriority] [-tcpProfileName] [-httpProfileName] [-comment] [-appflowLog] [-icmpVsrResponse]

Description

Use this command to remove vpn vserver settings.Refer to the set vpn vserver command for meanings of the arguments.

Top

bind vpn vserver

Synopsis

bind vpn vserver <name> [-policy <string> [-priority <positive_integer>] [-secondary] [-gotoPriorityExpression <expression>] [-type (REQUEST | RESPONSE)]] [-intranetApplication <string>] [-nextHopServer <string>] [-urlName <string>] [-intranetIP <ip_addr> <netmask>] [-staServer <URL>]

Description

Bind attributes to a vserver.

Parameters

name

The vserver to which this command shall bind parameters.

policy

The name of the policy to be bound to the vserver.

intranetApplication

The name of the intranet application to be bound to the vserver.

nextHopServer

The name of the next hop server to be bound to the vserver.

urlName

The name of the vpn url to be bound.

intranetIP

The network id for the range of intranet IP addresses or individual intranet ip to be bound to the vserver.

staServer

Secure Ticketing Authority (STA) server, in the format 'http(s)://IP/FQDN/URLPATH'

Top

unbind vpn vserver

Synopsis

unbind vpn vserver <name> [-policy <string> [-secondary] [-type (REQUEST | RESPONSE)]] [-intranetApplication <string>] [-nextHopServer <string>] [-urlName <string>] [-intranetIP <ip_addr> <netmask>] [-staServer <URL>]

Description

Unbind attributes from a vserver.

Parameters

name

The name of the vserver from which an attribute is to be unbound.

policy

The name of the policy to be unbound.

intranetApplication

The intranet application to be unbound.

nextHopServer

The name of the next hop server to be unbound.

urlName

The vpn url to be unbound.

intranetIP

The network id for the range of intranet IP addresses or the individually bound intranet IP address to be unbound.

staServer

Secure Ticketing Authority (STA) server to be removed, in the format 'http(s)://IP/FQDN/URLPATH'

Top

enable vpn vserver

Synopsis

enable vpn vserver <name>@

Description

Enable a virtual vpn server. Note: Virtual servers, when added, are enabled by default.

Parameters

name

The name of the virtual server to be enabled.

Example

enable vserver vpn1

Top

disable vpn vserver

Synopsis

disable vpn vserver <name>@

Description

Disable (take out of service) a virtual server.

Parameters

name

The name of the virtual server to be disabled. Notes: 1. The system still responds to ARP and/or ping requests for the IP address of this virtual server. 2. As the virtual server is still configured in the system, you can enable the virtual server using ###enable vserver### command.

Example

disable vserver lb_vip

Top

show vpn vserver

Synopsis

show vpn vserver [<name>] show vpn vserver stats - alias for 'stat vpn vserver'

Description

Display all of the configured VPN virtual servers.

Parameters

name

The name of the VPN vserver.

Example

show vpn vserver

Top

stat vpn vserver

Synopsis

stat vpn vserver [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]

Description

Display vpn vserver statistics.

Parameters

name

The name of the vserver for which statistics will be displayed. If not given statistics are shown for all vpn vservers.

Top

rename vpn vserver

Synopsis

rename vpn vserver <name>@ <newName>@

Description

Rename a content virtual server.

Parameters

name

The name of the content switching virtual server.

newName

The new name of the virtual server.

Example

rename vpn vserver vpn1 vpn1new

Top

vpn intranetApplication

[add | rm | show]

add vpn intranetApplication

Synopsis

add vpn intranetApplication <intranetApplication> [<protocol>] ((<destIP> [-netmask <netmask>]) | <IPRange> | <hostName> | (-clientApplication <string> ... [-spoofIIP (ON | OFF)])) [-destPort <port[-port]>] [-interception (PROXY | TRANSPARENT) [-srcIP <ip_addr>] [-srcPort <port>]]

Description

Add an intranet application.

Parameters

intranetApplication

The name for the new vpn intranet application.

protocol

The protocol of the intranet application, e.g. TCP, UDP or ANY. Possible values: TCP, UDP, ANY

destIP

The destination IP address for the application. This address is the real application server IP address.

clientApplication

The names of the client applications

destPort

The destination TCP or UDP port range. Minimum value: 1

interception

The interception type, e.g. proxy or transparent Possible values: PROXY, TRANSPARENT

srcIP

This is the source IP address of the client application. If not optionally specified, the default is 127.0.0.1.

srcPort

The source application TCP or UDP port. Minimum value: 1

Top

rm vpn intranetApplication

Synopsis

rm vpn intranetApplication <intranetApplication>

Description

Remove a configured intranet application.

Parameters

intranetApplication

The name of the vpn intranet application to remove.

Top

show vpn intranetApplication

Synopsis

show vpn intranetApplication [<intranetApplication>]

Description

Display the configured vpn intranet applications.

Parameters

intranetApplication

The name for the new vpn intranet application.

Top

vpn nextHopServer

[add | rm | show]

add vpn nextHopServer

Synopsis

add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (ON | OFF)]

Description

Add an next hop server.

Parameters

name

Configures new vpn next hop server. Maximum value: 32

nextHopIP

Configures next hop IP address.

nextHopPort

Configures next hop port number.

secure

Configures next hop over secure connection. Possible values: ON, OFF Default value: OFF

Example

add vpn nexthopserver dh1 10.1.1.1 80 -secure OFF

Top

rm vpn nextHopServer

Synopsis

rm vpn nextHopServer <name>

Description

Remove vpn next hop server.

Parameters

name

The name of the vpn next hop server to be removed. Maximum value: 32

Example

rm vpn nexthopserver dh1

Top

show vpn nextHopServer

Synopsis

show vpn nextHopServer [<name>]

Description

Display the configured vpn next hop servers.

Parameters

name

Configures new vpn next hop server. Maximum value: 32

Example

show vpn nexthopserver dh1

Top

vpn trafficPolicy

[add | rm | set | unset | show]

add vpn trafficPolicy

Synopsis

add vpn trafficPolicy <name> <rule> <action>

Description

Add a traffic policy. A traffic policy conditionally sets VPN traffic characteristics at run time.

Parameters

name

The name for the new vpn traffic policy.

rule

The rule to be used by the vpn traffic policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

action

The action to be applied by the policy if its rule is matched.

Top

rm vpn trafficPolicy

Synopsis

rm vpn trafficPolicy <name>

Description

Remove a vpn traffic policy.

Parameters

name

The name of the vpn traffic policy to be removed.

Top

set vpn trafficPolicy

Synopsis

set vpn trafficPolicy <name> [-rule <expression>] [-action <string>]

Description

Change the properties of an existing traffic policy.

Parameters

name

The name of the policy.

rule

The new rule to be used in the policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

action

The new action to be applied by the policy.

Top

unset vpn trafficPolicy

Synopsis

unset vpn trafficPolicy <name> [-rule] [-action]

Description

Use this command to remove vpn trafficPolicy settings.Refer to the set vpn trafficPolicy command for meanings of the arguments.

Top

show vpn trafficPolicy

Synopsis

show vpn trafficPolicy [<name>]

Description

Display vpn traffic policies.

Parameters

name

The name of the vpn trafiic policy.

Top

vpn trafficAction

[add | rm | set | unset | show]

add vpn trafficAction

Synopsis

add vpn trafficAction <name> <qual> [-appTimeout <mins>] [(-SSO (ON | OFF) [-formSSOAction <string>]) | -wanscaler (ON | OFF)] [-fta (ON | OFF)]

Description

Create a vpn traffic action. A vpn traffic action defines the characteristics of run time VPN traffic.

Parameters

name

The name for the action.

qual

The protocol to be set with the action, e.g. http or tcp. Possible values: http, tcp

appTimeout

The inactivity timeout after which the system closes a connection. Minimum value: 1 Maximum value: 715827

SSO

Enable or disable Single Sign-On Possible values: ON, OFF

formSSOAction

Name of configured vpn formssoaction

fta

Enable or disable file-type association Possible values: ON, OFF

wanscaler

Enable or disable Repeater Possible values: ON, OFF

Top

rm vpn trafficAction

Synopsis

rm vpn trafficAction <name>

Description

Remove a previously created traffic action.

Parameters

name

The name of the action to be removed.

Top

set vpn trafficAction

Synopsis

set vpn trafficAction <name> [-appTimeout <mins>] [-SSO (ON | OFF) | -wanscaler (ON | OFF)] [-formSSOAction <string>] [-fta (ON | OFF)]

Description

Modifies a vpn traffic action. A vpn traffic action defines the characteristics of run time VPN traffic.

Parameters

name

The name for the action.

appTimeout

The inactivity timeout after which the system closes a connection. Minimum value: 1 Maximum value: 715827

SSO

switch to turn on the SSO engine for HTTP traffic. Possible values: ON, OFF

formSSOAction

Name of configured vpn formssoaction

fta

Enable or disable file-type association Possible values: ON, OFF

wanscaler

Enable or disable Repeater Possible values: ON, OFF

Top

unset vpn trafficAction

Synopsis

unset vpn trafficAction <name> -wanscaler

Description

Use this command to remove vpn trafficAction settings.Refer to the set vpn trafficAction command for meanings of the arguments.

Top

show vpn trafficAction

Synopsis

show vpn trafficAction [<name>]

Description

Display the configured vpn traffic action(s).

Parameters

name

The name of the vpn trafiic action.

Top

vpn formSSOAction

[add | rm | set | unset | show]

add vpn formSSOAction

Synopsis

add vpn formSSOAction <name> -actionURL <URL> -userField <string> -passwdField <string> -ssoSuccessRule <expression> [-nameValuePair <string>] [-responsesize <positive_integer>] [-nvtype (STATIC | DYNAMIC)] [-submitMethod (GET | POST)]

Description

Create a formsso action. A formsso action defines the characteristics of the form.

Parameters

name

The name for the action.

actionURL

The url to which form will be submitted.

userField

Username field in the form to be filled with sessions username.

passwdField

Password field in the form to be filled with sessions username.

ssoSuccessRule

The rule to be used to check whether sso is successfull or not . Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

nameValuePair

Name Value pairs to be submitted. Name value pairs have to separated by '&'. EX: name1=value1&name2=value2

responsesize

Size of the body to be parsed to get the forms. Default value: 8096

nvtype

Bypass Form extraction. Possible values: STATIC, DYNAMIC Default value: NS_ACT_FSSO_NV_DYNAMIC

submitMethod

submit method Possible values: GET, POST Default value: NS_ACT_FSSO_SUBMIT_GET

Top

rm vpn formSSOAction

Synopsis

rm vpn formSSOAction <name>

Description

Delete a previously created session action.

Parameters

name

The Form sso action to be removed.

Top

set vpn formSSOAction

Synopsis

set vpn formSSOAction <name> [-actionURL <URL>] [-userField <string>] [-passwdField <string>] [-ssoSuccessRule <expression>] [-responsesize <positive_integer>] [-nameValuePair <string>] [-nvtype (STATIC | DYNAMIC)] [-submitMethod (GET | POST)]

Description

Create a vpn traffic action. A vpn traffic action defines the characteristics of run time VPN traffic.

Parameters

name

The name for the action.

actionURL

Set the url to which form will be submitted.

userField

Set the username field.

passwdField

Set the password field.

ssoSuccessRule

Set the success rule.

responsesize

Set the body size to be parsed Default value: 8096

nameValuePair

Set the name value pair.

nvtype

Bypass Form extraction. Possible values: STATIC, DYNAMIC Default value: NS_ACT_FSSO_NV_DYNAMIC

submitMethod

Submit method. Possible values: GET, POST Default value: NS_ACT_FSSO_SUBMIT_GET

Top

unset vpn formSSOAction

Synopsis

unset vpn formSSOAction <name> [-responsesize] [-nameValuePair] [-nvtype] [-submitMethod]

Description

Use this command to remove vpn formSSOAction settings.Refer to the set vpn formSSOAction command for meanings of the arguments.

Top

show vpn formSSOAction

Synopsis

show vpn formSSOAction [<name>]

Description

Display Form SSO action details.

Parameters

name

The name for the action.

Top

vpn url

[add | rm | set | unset | show]

add vpn url

Synopsis

add vpn url <urlName> <linkName> <actualURL> [-clientlessAccess (ON | OFF)] [-comment <string>]

Description

Add vpn urls. A vpn url provides a link to intranet resources on the vpn portal page.

Parameters

urlName

The name for the new vpn url.

linkName

The display name for the vpn url. This is the name that will display in the bookmark links in the vpn portal page.

actualURL

The actual URL that the vpn url points to.

clientlessAccess

Enable clientless access for the URL in other VPN modes if permitted. In clientless mode of VPN, it is enabled by default. Possible values: ON, OFF Default value: OFF

comment

Comments associated with this vpn url entity.

Example

add vpn url ggl search www.google.com.

Top

rm vpn url

Synopsis

rm vpn url <urlName>

Description

Remove vpn urls.

Parameters

urlName

The name of the vpn url to be removed.

Example

rm vpn url ggl

Top

set vpn url

Synopsis

set vpn url <urlName> [-linkName <string>] [-actualURL <string>] [-clientlessAccess (ON | OFF)] [-comment <string>]

Description

Modifies a vpn url. A vpn url provides a link to intranet resources on the vpn portal page.

Parameters

urlName

The name of the vpn url to be modified.

linkName

The display name for the vpn url. This is the name that will display in the bookmark links in the vpn portal page.

actualURL

The actual URL that the vpn url points to.

clientlessAccess

Enable or disable clientless access mode for the url in other modes. Possible values: ON, OFF Default value: OFF

comment

Comments associated with this vpn url entity.

Example

set vpn url wiurl -clientlessAccess on

Top

unset vpn url

Synopsis

unset vpn url <urlName> [-clientlessAccess] [-comment]

Description

Use this command to remove vpn url settings.Refer to the set vpn url command for meanings of the arguments.

Top

show vpn url

Synopsis

show vpn url [<urlName>]

Description

Display the configured vpn urls.

Parameters

urlName

The name for the new vpn url.

Top

vpn sessionPolicy

[add | rm | set | unset | show]

add vpn sessionPolicy

Synopsis

add vpn sessionPolicy <name> <rule> <action>

Description

Add a vpn session policy, which conditionally sets characteristics of a vpn session upon session establishment.

Parameters

name

The name for the new vpn session policy.

rule

The rule to be evaluated in the policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

action

The action to be performed when the rule is matched.

Top

rm vpn sessionPolicy

Synopsis

rm vpn sessionPolicy <name>

Description

Remove a previously created vpn session policy.

Parameters

name

The name of the policy to be removed.

Top

set vpn sessionPolicy

Synopsis

set vpn sessionPolicy <name> [-rule <expression>] [-action <string>]

Description

Modify the rule or action of a vpn session policy.

Parameters

name

The name of the vpn session policy.

rule

The new rule to be associated with the policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

action

The new vpn session action for the policy.

Top

unset vpn sessionPolicy

Synopsis

unset vpn sessionPolicy <name> [-rule] [-action]

Description

Use this command to remove vpn sessionPolicy settings.Refer to the set vpn sessionPolicy command for meanings of the arguments.

Top

show vpn sessionPolicy

Synopsis

show vpn sessionPolicy [<name>]

Description

Display the configured vpn session policies.

Parameters

name

The name of the vpn session policy.

Top

vpn sessionAction

[add | rm | set | unset | show]

add vpn sessionAction

Synopsis

add vpn sessionAction <name> [-httpPort <port> ...] [-winsIP <ip_addr>] [-dnsVserverName <string>] [-splitDns <splitDns>] [-sessTimeout <mins>] [-clientSecurity <expression> [-clientSecurityGroup <string>] [-clientSecurityMessage <string>]] [-clientSecurityLog (ON | OFF)] [-splitTunnel <splitTunnel>] [-localLanAccess (ON | OFF)] [-rfc1918 (ON | OFF)] [-spoofIIP (ON | OFF)] [-killConnections (ON | OFF)] [-transparentInterception (ON | OFF)] [-defaultAuthorizationAction (ALLOW | DENY)] [-authorizationGroup <string>] [-clientIdleTimeout <mins>] [-proxy <proxy>] [-allProtocolProxy <string> | -httpProxy <string> | -ftpProxy <string> | -socksProxy <string> | -gopherProxy <string> | -sslProxy <string>] [-proxyException <string>] [-proxyLocalBypass (ENABLED | DISABLED)] [-clientCleanupPrompt (ON | OFF)] [-forceCleanup <forceCleanup> ...] [-clientOptions <clientOptions> ...] [-clientConfiguration <clientConfiguration> ...] [-SSO (ON | OFF)] [-ssoCredential (PRIMARY | SECONDARY)] [-windowsAutoLogon (ON | OFF)] [-useMIP (NS | OFF)] [-useIIP <useIIP>] [-clientDebug <clientDebug>] [-loginScript <input_filename>] [-logoutScript <input_filename>] [-homePage <URL>] [-icaProxy (ON | OFF)] [-wihome <URL>] [-citrixReceiverHome <URL>] [-wiPortalMode (NORMAL | COMPACT)] [-ClientChoices (ON | OFF)] [-iipDnsSuffix <string>] [-forcedTimeout <mins>] [-forcedTimeoutWarning <mins>] [-ntDomain <string>] [-clientlessVpnMode <clientlessVpnMode>] [-emailHome <URL>] [-clientlessModeUrlEncoding <clientlessModeUrlEncoding>] [-clientlessPersistentCookie <clientlessPersistentCookie>] [-allowedLoginGroups <string>] [-SecureBrowse (ENABLED | DISABLED)] [-storefronturl <string>]

Description

Create a session action, which defines the properties of a VPN session.

Parameters

name

The name for the new vpn session action.

httpPort

The http port number for this session. Minimum value: 1

winsIP

The WINS server ip address for this session.

dnsVserverName

The name of the DNS vserver to be configured by the session action.

splitDns

Set the VPN client to route the DNS requests to remote network or local network or both. Possible values: LOCAL, REMOTE, BOTH

sessTimeout

The session timeout, in minutes, to be set by the action. Minimum value: 1

clientSecurity

The client security check string to be applied. This is in the form of an Expression. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

clientSecurityLog

Controls client side logging of security checks. Possible values: ON, OFF

splitTunnel

The split tunnel state, e.g. ON, OFF or REVERSE. Split Tunnelling ON enables the VPN client to route non-VPN traffic through its local network interface. When Split Tunnelling is OFF, no traffic may go to the local interface while the client session is active. Split tunneling can also be set to REVERSE. In this case all traffic directed to domains configured on the system will bypass the VPN tunnel. All other traffic is forced through the VPN tunnel. Possible values: ON, OFF, REVERSE

localLanAccess

Finer grained local lan access. ON or OFF. splitTunnel, when OFF, permits no traffic to be routed to the client's local interface. But if, in addition, localLanAccess is turned ON, the client MAY route traffic to its local interface. This combination of switches is useful primarily when the rfc1918 switch is also specified. In this fashion, the client may restrict local lan access to devices which commonly have non-routable addresses, such as local printers or local file servers. Possible values: ON, OFF

rfc1918

Only allow RFC1918 local addresses when local LAN access feature is enabled. Possible values: ON, OFF

spoofIIP

Controls the Spoofing of Intranet IP to the Windows Applications by Windows VPN client when the end-user is connected to SSL VPN in '-splittunnel OFF' mode. Possible values: ON, OFF

killConnections

Determines whether Windows VPN client should kill all pre-existing connections (ie, the connections existing before the end user logged in to SSL VPN) and prevent new incoming connections on the Windows Client system when the end-user is connected to SSL VPN in '-splittunnel OFF' mode. Possible values: ON, OFF

transparentInterception

The transparent interception state, e.g. ON or OFF. Possible values: ON, OFF

windowsClientType

Choose between two types of Windows Client\ a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed\ b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

defaultAuthorizationAction

This toggles the default authorization action to either ALLOW or DENY. Possible values: ALLOW, DENY

authorizationGroup

The authorization group to be applied to the session.

clientIdleTimeout

Defines the client idle timeout value. Measured in minutes, the client idle timeout default is 20 minutes and meters a client session's keyboard and mouse inactivity. Minimum value: 1 Maximum value: 9999

proxy

Enables or disables use of a proxy configuration in the session. Possible values: BROWSER, NS, OFF

allProtocolProxy

Sets the address to use for all proxies.

httpProxy

Sets the HTTP proxy IP address.

ftpProxy

Defines the FTP proxy IP address.

socksProxy

The SOCKS proxy IP address.

gopherProxy

Sets the Gopher proxy IP address.

sslProxy

Sets the HTTPS proxy IP address.

proxyException

Proxy Exception string that will be configured in the Browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass

Bypass proxy server for local addresses option in IE proxy server settings will be enabled Possible values: ENABLED, DISABLED

clientCleanupPrompt

Toggles the prompt for client clean up on a client intitiated session close. Possible values: ON, OFF

forceCleanup

The client side items for force cleanup on session close. Options are: none, all, cookie, addressbar, plugin, filesystemapplication, addressbar, application, clientcertificate, applicationdata, and autocomplete. You may specify all or none alone or any combination of the client side items.

clientOptions

Display only configured buttons(and/or menu options in the docked client) in the Windows VPN client.\ Options:\ none\ none of the Windows Client's buttons/menu options (except logout) are displayed.\ all\ all of the Windows Client's buttons/menu options are displayed.\ \ One or more of the following\ services\ only the "Services" button/menu option is displayed.\ filetransfer\ only the "File Transfer" button/menu option is displayed.\ configuration\ only the "Configuration" button/menu option is displayed.

clientConfiguration

Display only configured tabs in the Windows VPN client.\ Options:\ none\ none of the Windows Client's tabs(except About) are displayed.\ all\ all of the Windows Client's tabs (except "Resptime") are displayed.\ \ One or more of the following\ general\ only the "General" tab is displayed.\ tunnel\ only the "Tunnel" tab is displayed.\ trace\ only the "Trace" tab is displayed.\ compression\ only the "Compression" tab is displayed.\ resptime\ only the "Resptime" tab is displayed.

SSO

Enables or disables the use of Single Sign-on for the session. Possible values: ON, OFF

ssoCredential

The set of user credentials (primary or secondary) to use for Single Sign-On Possible values: PRIMARY, SECONDARY

windowsAutoLogon

Enables or disables the Windows Auto Logon for the session. Possible values: ON, OFF

useMIP

Enables or disables the use of a Mapped IP address for the session Possible values: NS, OFF

useIIP

Controls how the intranet IP module is configured for usage. \ Options:\ SPILLOVER\ specifies that iip is ON and when we can't assign an intranet IP to an entity, which has other instances active, we spill over to using Mapped IP.\ NOSPILLOVER\ specifies that iip is ON and when we can't assign intranet IP to an entity, which has other instances active, then we initiate transfer login.\ OFFn specifies that intranet IP module won't be activated for this entity. Possible values: NOSPILLOVER, SPILLOVER, OFF

clientDebug

Sets the trace level on the Windows VPN Client.\ Options:\ debugn\ Detailed debug messages are collected are written into the specified file.\ stats\ Application audit level error messages and debug statistic counters are written into the specified file.\ events\ Application audit level error messages are written into the specified file.\ off\ Only critical events are logged into the Windows Application Log. Possible values: debug, stats, events, OFF

loginScript

Login script path.

logoutScript

Logout script path.

homePage

Sets the client home page. Setting this parameter overrides serving the default portal page to SSL VPN users with the URL specified here.

icaProxy

Enable ICA proxy mode. This can be used to enable Secure Gateway functionality for the Web Interface. If enabled, a VPN homepage that points to a Web Interface in SG mode, has to be configured. Possible values: ON, OFF

wihome

Sets the home page of wi interface. Used only in conjunction with icaProxy ON. If clientChoices is ON, wiHome has to be configured. Since the end user is given a choice between FullClient and ICAProxy the homepage/landing page for each of these options could be different i.e. for FullClient it could be a Intranet web site and for the ICAProxy choice it will be a Web Interface web site. Hence we don't presume wihome == homepage.

citrixReceiverHome

Sets the home page of apprecvr interface.

wiPortalMode

WI layout on the VPN portal. Possible values: NORMAL, COMPACT

ClientChoices

Enables user to select different clients by displaying a set of options in a html page. The different client can be a) agent b) plugin c) wimode. Possible values: ON, OFF

epaClientType

Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

iipDnsSuffix

Configure the IntranetIP DNS suffix. When a user logs into SSL-VPN, an A record is added to the DNS cache, after appending the configured IntranetIP DNS suffix to the username.

forcedTimeout

Maximum number of minutes a session is allowed to persist. Minimum value: 1 Maximum value: 3000

forcedTimeoutWarning

Number of minutes to warn a user before their session is removed by a forced time out. Minimum value: 1 Maximum value: 255

ntDomain

NT domain to use with Smart Access when User Principle Name is not extracted from Active Directory

clientlessVpnMode

Whether clientlessVPN is available to the session. ON will make the session clientless and no client will be downloaded OFF will download the client but the clientlessVPN will also be available DISABLED will disable clientlessVPN altogether. Possible values: ON, OFF, DISABLED

emailHome

Sets the EMail home for the portal

clientlessModeUrlEncoding

URL encoding to be used in clientless mode. No encoding will be done for TRANSPARENT. Protocol and domain will be encoded or encrypted with OPAQUE or ENCRYPT respectively. Possible values: TRANSPARENT, OPAQUE, ENCRYPT

clientlessPersistentCookie

Controls the use of persistent cookie in clientless mode. ALLOW lets cookie to be stored on disk. DENY prevents usage of persistent cookie. PROMPT lets VPN user choose whether persistent cookie should be used or not. Possible values: ALLOW, DENY, PROMPT

allowedLoginGroups

The groups allowed login to VPN

SecureBrowse

Enable and Disable the Secure Browse functionality. Possible values: ENABLED, DISABLED

storefronturl

The Account Service or Auto Discovery url for this session.

Top

rm vpn sessionAction

Synopsis

rm vpn sessionAction <name>

Description

Delete a previously created session action.

Parameters

name

The vpn session action to be removed.

Top

set vpn sessionAction

Synopsis

set vpn sessionAction <name> [-httpPort <port> ...] [-winsIP <ip_addr>] [-dnsVserverName <string>] [-splitDns <splitDns>] [-sessTimeout <mins>] [-clientSecurity <expression> [-clientSecurityGroup <string>] [-clientSecurityMessage <string>]] [-clientSecurityLog (ON | OFF)] [-splitTunnel <splitTunnel>] [-localLanAccess (ON | OFF)] [-rfc1918 (ON | OFF)] [-spoofIIP (ON | OFF)] [-killConnections (ON | OFF)] [-transparentInterception (ON | OFF)] [-defaultAuthorizationAction (ALLOW | DENY)] [-authorizationGroup <string>] [-clientIdleTimeout <mins>] [-proxy <proxy>] [-allProtocolProxy <string> | -httpProxy <string> | -ftpProxy <string> | -socksProxy <string> | -gopherProxy <string> | -sslProxy <string>] [-proxyException <string>] [-proxyLocalBypass (ENABLED | DISABLED)] [-clientCleanupPrompt (ON | OFF)] [-forceCleanup <forceCleanup> ...] [-clientOptions <clientOptions> ...] [-clientConfiguration <clientConfiguration> ...] [-SSO (ON | OFF)] [-ssoCredential (PRIMARY | SECONDARY)] [-windowsAutoLogon (ON | OFF)] [-useMIP (NS | OFF)] [-useIIP <useIIP>] [-clientDebug <clientDebug>] [-loginScript <input_filename>] [-logoutScript <input_filename>] [-homePage <URL>] [-icaProxy (ON | OFF)] [-wihome <URL>] [-citrixReceiverHome <URL>] [-wiPortalMode (NORMAL | COMPACT)] [-ClientChoices (ON | OFF)] [-iipDnsSuffix <string>] [-forcedTimeout <mins>] [-forcedTimeoutWarning <mins>] [-ntDomain <string>] [-clientlessVpnMode <clientlessVpnMode>] [-emailHome <URL>] [-clientlessModeUrlEncoding <clientlessModeUrlEncoding>] [-clientlessPersistentCookie <clientlessPersistentCookie>] [-allowedLoginGroups <string>] [-SecureBrowse (ENABLED | DISABLED)] [-storefronturl <string>]

Description

Modify a session action, which defines the properties of a VPN session.

Parameters

name

The name of the vpn session action.

httpPort

The http port number for this session. Minimum value: 1

winsIP

The WINS server ip address.

dnsVserverName

The name of the DNS vserver to be configured by the session action.

splitDns

Set the VPN client to route the DNS requests to remote network or local network or both. Possible values: LOCAL, REMOTE, BOTH

sessTimeout

The session timeout, in minutes, to be set by the action. Minimum value: 1

clientSecurity

The client security check string to be applied. This is in the form of an Expression. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

clientSecurityLog

Controls client side logging of security checks. Possible values: ON, OFF

splitTunnel

The split tunnel state, e.g. ON, OFF or REVERSE. Split Tunnelling ON enables the VPN client to route non-VPN traffic through its local network interface. When Split Tunnelling is OFF, no traffic may go to the local interface while the client session is active. Split tunneling can also be set to REVERSE. In this case all traffic directed to domains configured on the system will bypass the VPN tunnel. All other traffic is forced through the VPN tunnel. Possible values: ON, OFF, REVERSE

localLanAccess

Finer grained local lan access. ON or OFF. splitTunnel, when OFF, permits no traffic to be routed to the client's local interface. But if, in addition, localLanAccess is turned ON, the client MAY route traffic to its local interface. This combination of switches is useful primarily when the rfc1918 switch is also specified. In this fashion, the client may restrict local lan access to devices which commonly have non-routable addresses, such as local printers or local file servers. Possible values: ON, OFF

rfc1918

Only allow RFC1918 local addresses when local LAN access feature is enabled Possible values: ON, OFF

spoofIIP

Controls the Spoofing of Intranet IP to the Windows Applications by Windows VPN client when the end-user is connected to SSL VPN in '-splittunnel OFF' mode. Possible values: ON, OFF

killConnections

Determines whether Windows VPN client should kill all pre-existing connections (ie, the connections existing before the end user logged in to SSL VPN) and prevent new incoming connections on the Windows Client system when the end-user is connected to SSL VPN in '-splittunnel OFF' mode. Possible values: ON, OFF

transparentInterception

The transparent interception state, e.g. ON or OFF. Possible values: ON, OFF

windowsClientType

Choose between two types of Windows Client\ a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed\ b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

defaultAuthorizationAction

This toggles the default authorization action to either ALLOW or DENY. Possible values: ALLOW, DENY

authorizationGroup

The authorization group to be applied to the session.

clientIdleTimeout

Defines the client idle timeout value. Measured in minutes, the client idle timeout default is 20 minutes and meters a client session's keyboard and mouse inactivity. Minimum value: 1 Maximum value: 9999

proxy

Enables or disables use of a proxy configuration in the session. Possible values: BROWSER, NS, OFF

allProtocolProxy

Sets the address to use for all proxies.

httpProxy

Sets the HTTP proxy IP address.

ftpProxy

Defines the FTP proxy IP address.

socksProxy

The SOCKS proxy IP address.

gopherProxy

Sets the Gopher proxy IP address.

sslProxy

Sets the HTTPS proxy IP address.

proxyException

Proxy Exception string that will be configured in the Browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass

Bypass proxy server for local addresses option in IE proxy server settings will be enabled Possible values: ENABLED, DISABLED

clientCleanupPrompt

Toggles the prompt for client clean up on a client intitiated session close. Possible values: ON, OFF

forceCleanup

The client side items for force cleanup on session close. Options are: none, all, cookie, addressbar, plugin, filesystemapplication, addressbar, application, clientcertificate, applicationdata, and autocomplete. You may specify all or none alone or any combination of the client side items.

clientOptions

Display only configured buttons(and/or menu options in the docked client) in the Windows VPN client.\ Options:\ none\ none of the Windows Client's buttons/menu options (except logout) are displayed.\ all\ all of the Windows Client's buttons/menu options are displayed.\ \ One or more of the following\ services\ only the "Services" button/menu option is displayed.\ filetransfer\ only the "File Transfer" button/menu option is displayed.\ configuration\ only the "Configuration" button/menu option is displayed.

clientConfiguration

Display only configured tabs in the Windows VPN client.\ Options:\ none\ none of the Windows Client's tabs(except About) are displayed.\ all\ all of the Windows Client's tabs (except "Resptime") are displayed.\ \ One or more of the following\ general\ only the "General" tab is displayed.\ tunnel\ only the "Tunnel" tab is displayed.\ trace\ only the "Trace" tab is displayed.\ compression\ only the "Compression" tab is displayed.\ resptime\ only the "Resptime" tab is displayed.

SSO

Enables or disables the use of Single Sign-on for the session. Possible values: ON, OFF

ssoCredential

The set of user credentials (primary or secondary) to use for Single Sign-On Possible values: PRIMARY, SECONDARY

windowsAutoLogon

Enables or disables the Windows Auto Logon for the session. Possible values: ON, OFF

useMIP

Enables or disables the use of a Mapped IP address for the session Possible values: NS, OFF

useIIP

Controls how the intranet IP module is configured for usage. \ Options:\ SPILLOVER\ specifies that iip is ON and when we can't assign an intranet IP to an entity, which has other instances active, we spill over to using Mapped IP.\ NOSPILLOVER\ specifies that iip

is ON and when we can't assign intranet IP to an entity, which has other instances active, then we initiate transfer login.\ OFFn specifies that intranet IP module won't be activated for this entity. Possible values: NOSPILLOVER, SPILLOVER, OFF

clientDebug

Sets the trace level on the Windows VPN Client.\ Options:\ debugn\ Detailed debug messages are collected are written into the specified file.\ stats\ Application audit level error messages and debug statistic counters are written into the specified file.\ events\ Application audit level error messages are written into the specified file.\ off\ Only critical events are logged into the Windows Application Log. Possible values: debug, stats, events, OFF

loginScript

Login script path.

logoutScript

Logout script path.

homePage

Sets the client home page. Setting this parameter overrides serving the default portal page to SSL VPN users with the URL specified here.

icaProxy

Enable ICA proxy mode. This can be used to enable Secure Gateway functionality for the Web Interface. If enabled, a VPN homepage that points to a Web Interface in SG mode, has to be configured. Possible values: ON, OFF Default value: OFF

wihome

Sets the home page of wi interface. Used only in conjunction with icaProxy ON. If clientChoices is ON, wiHome has to be configured. Since the end user is given a choice between FullClient and ICAProxy the homepage/landing page for each of these options could be different i.e. for FullClient it could be a Intranet web site and for the ICAProxy choice it will be a Web Interface web site. Hence we don't presume wihome == homepage.

citrixReceiverHome

Sets the home page of apprecvr interface.

wiPortalMode

WI layout on the VPN portal. Possible values: NORMAL, COMPACT

ClientChoices

Enables user to select different clients by displaying a set of options in a html page. The different client can be a) agent b) plugin c) wimode. Possible values: ON, OFF

epaClientType

Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

iipDnsSuffix

Configure the IntranetIP DNS suffix. When a user logs into SSL-VPN, an A record is added to the DNS cache, after appending the configured IntranetIP DNS suffix to the username.

forcedTimeout

Maximum number of minutes a session is allowed to persist. Minimum value: 1 Maximum value: 3000

forcedTimeoutWarning

Number of minutes to warn a user before their session is removed by a forced time out. Minimum value: 1 Maximum value: 255

ntDomain

NT domain to use with Smart Access when User Principle Name is not extracted from Active Directory

clientlessVpnMode

Whether clientlessVPN is available to the session. ON will make the session clientless and no client will be downloaded OFF will download the client but the clientlessVPN will also be available DISABLED will disable clientlessVPN altogether. Possible values: ON, OFF, DISABLED Default value: VPN_SESS_ACT_CVPNMODE_OFF

emailHome

Sets the EMail home for the portal

clientlessModeUrlEncoding

URL encoding to be used in clientless mode. No encoding will be done for TRANSPARENT. Protocol and domain will be encoded or encrypted with OPAQUE or ENCRYPT respectively. Possible values: TRANSPARENT, OPAQUE, ENCRYPT

clientlessPersistentCookie

Controls the use of persistent cookie in clientless mode. ALLOW lets cookie to be stored on disk. DENY prevents usage of persistent cookie. PROMPT lets VPN user choose whether persistent cookie should be used or not. Possible values: ALLOW, DENY, PROMPT Default value: VPN_SESS_ACT_CVPN_PERSCOOKIE_DENY

allowedLoginGroups

The groups allowed login to VPN

SecureBrowse

Enable and Disable the Secure Browse functionality. Possible values: ENABLED, DISABLED

storefronturl

The Account Service or Auto Discovery url for this session.

Top

unset vpn sessionAction

Synopsis

unset vpn sessionAction <name> [-httpPort] [-winsIP] [-dnsVserverName] [-splitDns] [-sessTimeout] [-clientSecurity] [-clientSecurityGroup] [-clientSecurityMessage] [-clientSecurityLog] [-splitTunnel] [-localLanAccess] [-rfc1918] [-spoofIIP] [-killConnections] [-transparentInterception] [-defaultAuthorizationAction] [-authorizationGroup] [-clientIdleTimeout] [-proxy] [-allProtocolProxy] [-httpProxy] [-ftpProxy] [-socksProxy] [-gopherProxy] [-sslProxy] [-proxyException] [-proxyLocalBypass] [-clientCleanupPrompt] [-forceCleanup] [-clientOptions] [-clientConfiguration] [-SSO] [-ssoCredential] [-windowsAutoLogon] [-useMIP] [-useIIP] [-clientDebug] [-loginScript] [-logoutScript] [-homePage] [-icaProxy] [-wihome] [-citrixReceiverHome] [-wiPortalMode] [-ClientChoices] [-iipDnsSuffix] [-forcedTimeout] [-forcedTimeoutWarning] [-ntDomain] [-clientlessVpnMode] [-emailHome] [-clientlessModeUrlEncoding] [-clientlessPersistentCookie] [-allowedLoginGroups] [-SecureBrowse] [-storefronturl]

Description

Use this command to remove vpn sessionAction settings.Refer to the set vpn sessionAction command for meanings of the arguments.

Top

show vpn sessionAction

Synopsis

show vpn sessionAction [<name>]

Description

Display vpn session action details.

Parameters

name

The name of the vpn session action.

Top

vpn clientlessAccessPolicy

[add | rm | set | show]

add vpn clientlessAccessPolicy

Synopsis

add vpn clientlessAccessPolicy <name> <rule> <profileName>

Description

Add a clientless access policy.

Parameters

name

The name for the new clientless access policy.

rule

The rule to be used by the clientless access policy.

profileName

The profile to be invoked for clientless access.

Top

rm vpn clientlessAccessPolicy

Synopsis

rm vpn clientlessAccessPolicy <name>

Description

Remove a clientless access policy.

Parameters

name

The name of the clientless access policy to be removed.

Top

set vpn clientlessAccessPolicy

Synopsis

set vpn clientlessAccessPolicy <name> [-rule <expression>] [-profileName <string>]

Description

Set a new rule/profile for existing clientless access policy.

Parameters

name

The name of the existing clientless access policy.

rule

The rule to be used by the clientless access policy.

profileName

The profile to be invoked for clientless access.

Top

show vpn clientlessAccessPolicy

Synopsis

show vpn clientlessAccessPolicy [<name>]

Description

Display clientless access policies.

Parameters

name

The name of the clientless access policy.

Top

vpn clientlessAccessProfile

[add | rm | set | unset | show]

add vpn clientlessAccessProfile

Synopsis

add vpn clientlessAccessProfile <profileName>

Description

Add a clientless access profile.

Parameters

profileName

The name of the clientless access profile.

Top

rm vpn clientlessAccessProfile

Synopsis

rm vpn clientlessAccessProfile <profileName>

Description

Remove a clientless access profile.

Parameters

profileName

The name of the clientless access profile.

Top

set vpn clientlessAccessProfile

Synopsis

set vpn clientlessAccessProfile <profileName> [-URLRewritePolicyLabel <string>] [-JavaScriptRewritePolicyLabel <string>] [-ReqHdrRewritePolicyLabel <string>] [-ResHdrRewritePolicyLabel <string>] [-RegexForFindingURLinJavaScript <string>] [-RegexForFindingURLinCSS <string>] [-RegexForFindingURLinXComponent <string>] [-RegexForFindingURLinXML <string>] [-RegexForFindingCustomURLs <string>] [-ClientConsumedCookies <string>] [-requirePersistentCookie (ON | OFF)]

Description

Set a policylabel on the clientless access profile.

Parameters

profileName

The name of the clientless vpn profile.

URLRewritePolicyLabel

The configured URL rewrite policylabel.

JavaScriptRewritePolicyLabel

The configured JavaScript rewrite policylabel.

ReqHdrRewritePolicyLabel

The configured Request Header rewrite policylabel.

ResHdrRewritePolicyLabel

The configured Response rewrite policylabel.

RegexForFindingURLinJavaScript

Patclass having regexes to find the URLs in JavaScript.

RegexForFindingURLinCSS

Patclass having regexes to find the URLs in CSS.

RegexForFindingURLinXComponent

Patclass having regexes to find the URLs in X-Component.

RegexForFindingURLinXML

Patclass having regexes to find the URLs in XML.

RegexForFindingCustomURLs

Patclass having regexes to find the custom URLs.

ClientConsumedCookies

Patclass having the client consumed Cookie names.

requirePersistentCookie

The flag to select Persistent cookie for the profile Possible values: ON, OFF Default value: OFF

Top

unset vpn clientlessAccessProfile

Synopsis

unset vpn clientlessAccessProfile <profileName> [-URLRewritePolicyLabel] [-JavaScriptRewritePolicyLabel] [-ReqHdrRewritePolicyLabel] [-ResHdrRewritePolicyLabel] [-RegexForFindingURLinJavaScript] [-RegexForFindingURLinCSS] [-RegexForFindingURLinXComponent] [-RegexForFindingURLinXML] [-RegexForFindingCustomURLs] [-ClientConsumedCookies] [-requirePersistentCookie]

Description

Unset a policylabel on a clientless access profile..Refer to the set vpn clientlessAccessProfile command for meanings of the arguments.

Top

show vpn clientlessAccessProfile

Synopsis

show vpn clientlessAccessProfile [<profileName>]

Description

Show clientless access profile.

Parameters

profileName

The name of the clientless vpn profile.

Top

vpn stats

show vpn stats

Synopsis

show vpn stats - alias for 'stat vpn'

Description

show vpn stats is an alias for stat vpn

vpn icaConnection

show vpn icaConnection

Synopsis

show vpn icaConnection [-userName <string>]

Description

Display the active ICA connections.

Parameters

userName

The user name.

vpn global

[bind | unbind | show]

bind vpn global

Synopsis

bind vpn global [-policyName <string> [-priority <positive_integer>] [-secondary]] [-intranetDomain <string>] [-intranetApplication <string>] [-nextHopServer <string>] [-urlName <string>] [-intranetIP <ip_addr> <netmask>] [-staServer <URL>]

Description

Bind vpn entities to vpn global.

Parameters

policyName

The name of the policy to be bound to vpn global.

intranetDomain

A conflicting intranet domain name.

intranetApplication

The vpn intranet application to be bound.

nextHopServer

The name of the next hop server to be bound globally.

urlName

The vpn url to be bound.

intranetIP

The intranet ip or range to be bound to VPN global.

staServer

Secure Ticketing Authority (STA) server, in the format 'http(s)://IP/FQDN/URLPATH'

Top

unbind vpn global

Synopsis

unbind vpn global [-policyName <string> [-secondary]] [-intranetDomain <string>] [-intranetApplication <string>] [-nextHopServer <string>] [-urlName <string>] [-intranetIP <ip_addr> <netmask>] [-staServer <URL>]

Description

Unbind entities from vpn global.

Parameters

policyName

The name of the policy to be unbound.

intranetDomain

A conflicting intranet domain name to be unbound.

intranetApplication

The name of a vpn intranet application to be unbound.

nextHopServer

The name of the next hop server to be unbound globally.

urlName

The name of a vpn url to be unbound from vpn global.

intranetIP

The intranet ip address or range to be unbound.

staServer

Secure Ticketing Authority (STA) server to be removed, in the format 'http(s)://IP/FQDN/URLPATH'

Top

show vpn global

Synopsis

show vpn global

Description

Display the vpn global bindings.

Top

vpn parameter

[set | unset | show]

set vpn parameter

Synopsis

set vpn parameter [-httpPort <port> ...] [-winsIP <ip_addr>] [-dnsVserverName <string>] [-splitDns <splitDns>] [-sessTimeout <mins>] [-clientSecurity <expression> [-clientSecurityGroup <string>] [-clientSecurityMessage <string>]] [-clientSecurityLog (ON | OFF)] [-splitTunnel <splitTunnel>] [-localLanAccess (ON | OFF)] [-rfc1918 (ON | OFF)] [-spoofIIP (ON | OFF)] [-killConnections (ON | OFF)] [-transparentInterception (ON | OFF)] [-defaultAuthorizationAction (ALLOW | DENY)] [-authorizationGroup <string>] [-clientIdleTimeout <mins>] [-proxy <proxy>] [-allProtocolProxy <string> | -httpProxy <string> | -ftpProxy <string> | -socksProxy <string> | -gopherProxy <string> | -sslProxy <string>] [-proxyException <string>] [-proxyLocalBypass (ENABLED | DISABLED)] [-clientCleanupPrompt (ON | OFF)] [-forceCleanup <forceCleanup> ...] [-clientOptions <clientOptions> ...] [-clientConfiguration <clientConfiguration> ...] [-SSO (ON | OFF)] [-ssoCredential (PRIMARY | SECONDARY)] [-windowsAutoLogon (ON | OFF)] [-useMIP (NS | OFF)] [-useIIP <useIIP>] [-clientDebug <clientDebug>] [-loginScript <input_filename>] [-logoutScript <input_filename>] [-homePage <URL>] [-icaProxy (ON | OFF)] [-wihome <URL>] [-citrixReceiverHome <URL>] [-wiPortalMode (NORMAL | COMPACT)] [-ClientChoices (ON | OFF)] [-iipDnsSuffix <string>] [-forcedTimeout <mins>] [-forcedTimeoutWarning <mins>] [-ntDomain <string>] [-clientlessVpnMode <clientlessVpnMode>] [-clientlessModeUrlEncoding <clientlessModeUrlEncoding>] [-clientlessPersistentCookie <clientlessPersistentCookie>] [-emailHome <URL>] [-allowedLoginGroups <string>] [-encryptCsecExp (ENABLED | DISABLED)] [-appTokenTimeout <positive_integer>] [-SecureBrowse (ENABLED | DISABLED)] [-storefronturl <string>]

Description

Set global parameters for the SSL VPN feature.

Parameters

httpPort

The SSL VPN HTTP port. Minimum value: 1

winsIP

The WINS server IP address to be used for WINS host resolution by the VPN.

dnsVserverName

The configured DNS vserver to be used for DNS host resolution by the VPN.

splitDns

Set the VPN client to route the DNS requests to remote network or local network or both. Possible values: LOCAL, REMOTE, BOTH

sessTimeout

The session idle timeout value in minutes. This idle timeout meters the overall network inactivity for a session. Default value: 30 Minimum value: 1

clientSecurity

The client security check string to be applied to client sessions. This is in the form of an Expression. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

clientSecurityLog

Controls client side logging of security checks. Possible values: ON, OFF Default value: VPN_SESS_ACT_ON

splitTunnel

The split tunnel state, e.g. ON, OFF or REVERSE. Split Tunnelling ON enables the VPN client to route non-VPN traffic through its local network interface. When Split Tunnelling is OFF, no traffic may go to the local interface while the client session is active. Split tunneling can also be set to REVERSE. In this case all traffic directed to domains configured on the system will bypass the VPN tunnel. All other traffic is forced through the VPN tunnel. Possible values: ON, OFF, REVERSE Default value: VPN_SESS_ACT_OFF

localLanAccess

Finer grained local lan access. ON or OFF. splitTunnel, when OFF, permits no traffic to be routed to the client's local interface. But if, in addition, localLanAccess is turned ON, the client MAY route traffic to its local interface. This combination of switches is useful primarily when the rfc1918 switch is also specified. In this fashion, the client may restrict local lan access to devices which commonly have non-routable addresses, such as local printers or local file servers. Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

rfc1918

Only allow RFC1918 local addresses when local LAN access feature is enabled Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

spoofIIP

The Spoof IP Address. Controls the Spoofing of Intranet IP to the Windows Applications by Windows VPN client when the end-user is connected to SSL VPN in '-splittunnel OFF' mode. Possible values: ON, OFF Default value: ON

killConnections

The state of kill connections. Determines whether Windows VPN client should kill all pre-existing connections (ie, the connections existing before the end user logged in to SSL VPN) and prevent new incoming connections on the Windows Client system when the end-user is connected to SSL VPN in '-splittunnel OFF' mode. Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

transparentInterception

The transparent interception state, e.g. ON or OFF. Possible values: ON, OFF Default value: VPN_SESS_ACT_ON

windowsClientType

The Windows client type. Choose between two types of Windows Client\ a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed\ b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN Default value: VPN_SESS_ACT_CLT_AGENT

defaultAuthorizationAction

The authorization action state. Toggles the default authorization action to either ALLOW or DENY. Possible values: ALLOW, DENY

authorizationGroup

The authorization group to be applied to client sessions.

clientIdleTimeout

The client idle time out interval, which meters the client session's mouse and keyboard inactivity. The value is specified in minutes. Minimum value: 1 Maximum value: 9999

proxy

The usage of proxy configuration. Possible values: BROWSER, NS, OFF

allProtocolProxy

The address to be used for all proxies.

httpProxy

The HTTP proxy IP address.

ftpProxy

The FTP proxy IP address.

socksProxy

The SOCKS proxy IP address.

gopherProxy

The Gopher proxy IP address.

sslProxy

The HTTPS proxy IP address.

proxyException

The Proxy Exception string that will be configured in the Browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass

Bypass proxy server for local addresses option in IE proxy server settings will be enabled Possible values: ENABLED, DISABLED Default value: VPN_SESS_ACT_DISABLED

clientCleanupPrompt

The state for prompting for client clean up on session close. Possible values: ON, OFF Default value: VPN_SESS_ACT_ON

forceCleanup

The client side items for force cleanup on session close. You may specify all or none alone or any combination of the client side items.

clientOptions

Configured buttons(and/or menu options in the docked client) in the Windows VPN client.\ Possible options \ none \ none of the Windows Client's buttons/menu options (except logout) are displayed. \ all \ all of the Windows Client's buttons/menu options are displayed. \ \ One or more of the following \ services \ only the "Services" button/menu option is displayed. \ filetransfer \ only the "File Transfer" button/menu option is displayed. \ configuration \ only the "Configuration" button/menu option is displayed.

clientConfiguration

Configured tabs in the Windows VPN client. \ Options: \ none \ none of the Windows Client's tabs(except About) are displayed. \ all \ all of the Windows Client's tabs (except "Resptime") are displayed. \ \ One or more of the following \ general \ only the "General" tab is displayed. \ tunnel \ only the "Tunnel" tab is displayed. \ trace \ only the "Trace" tab is displayed. \ compression \ only the "Compression" tab is displayed. \ resptime \ only the "Resptime" tab is displayed.

SSO

Whether or not Single Sign-On is used Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

ssoCredential

The set of user credentials (primary or secondary) to use for Single Sign-On Possible values: PRIMARY, SECONDARY Default value: VPN_SESS_ACT_USE_PRIMARY_CREDENTIALS

windowsAutoLogon

Whether or not Windows Auto Logon is enabled Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

useMIP

Whether or not a Mapped IP address is used Possible values: NS, OFF Default value: VPN_SESS_ACT_NS

useIIP

Controls how the intranet IP module is configured for usage. \ Options:\ SPILLOVER\ specifies that iip is ON and when we can't assign an intranet IP to an entity, which has other instances active, we spill over to using Mapped IP.\ NOSPILLOVER\ specifies that iip is ON and when we can't assign intranet IP to an entity, which has other instances active, then we initiate transfer login.\ OFFn specifies that intranet IP module won't be activated for this entity. Possible values: NOSPILLOVER, SPILLOVER, OFF Default value: VPN_SESS_ACT_NOSPILLOVER

clientDebug

The trace level on the Windows VPN Client.\ Options:\ debugn\ Detailed debug messages are collected are written into the specified file.\ stats\ Application audit level error messages and debug statistic counters are written into the specified file.\ events\ Application audit level error messages are written into the specified file.\ off\ Only critical events are logged into the Windows Application Log. Possible values: debug, stats, events, OFF Default value: VPN_FLAG_TRACE_OFF

loginScript

Login script path.

logoutScript

Logout script path.

homePage

The client home page. Setting this parameter overrides the serving of the default portal page with the URL specified here.

icaProxy

Enable ICA proxy mode. This can be used to enable Secure Gateway functionality for the Web Interface. If enabled, a VPN homepage that points to a Web Interface in SG mode, has to be configured. Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

wihome

Sets the home page of wi interface. Used only in conjunction with icaProxy ON. If clientChoices is ON, wiHome has to be configured. Since the end user is given a choice between FullClient and ICAProxy the homepage/landing page for each of these options could be different i.e. for FullClient it could be a Intranet web site and for the ICAProxy choice it will be a Web Interface web site. Hence we don't presume wihome == homepage.

citrixReceiverHome

Sets the home page of apprecvr interface.

wiPortalMode

WI layout on the VPN portal. Possible values: NORMAL, COMPACT

ClientChoices

Enables user to select different clients by displaying a set of options in a html page. The different client can be a) agent b) plugin c) wimode. Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

epaClientType

Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

iipDnsSuffix

The IntranetIP DNS suffix. When a user logs into SSL-VPN, an A record is added to the DNS cache, after appending the configured IntranetIP DNS suffix to the username.

forcedTimeout

Maximum number of minutes a session is allowed to persist. Minimum value: 1 Maximum value: 3000

forcedTimeoutWarning

Number of minutes to warn a user before their session is removed by a forced time out. Minimum value: 1 Maximum value: 255

ntDomain

NT domain to use with Smart Access when User Principle Name is not extracted from Active Directory

clientlessVpnMode

Whether clientlessVPN is available to the session. ON will make the session clientless and no client will be downloaded OFF will download the client but the clientlessVPN will also be available DISABLED will disable clientlessVPN altogether. Possible values: ON, OFF, DISABLED Default value: VPN_SESS_ACT_CVPNMODE_OFF

clientlessModeUrlEncoding

URL encoding to be used in clientless mode. No encoding will be done for TRANSPARENT. Protocol and domain will be encoded or encrypted with OPAQUE or ENCRYPT respectively. Possible values: TRANSPARENT, OPAQUE, ENCRYPT Default value: VPN_SESS_ACT_CVPN_ENC_OPAQUE

clientlessPersistentCookie

Controls the use of persistent cookie in clientless mode. ALLOW lets cookie to be stored on disk. DENY prevents usage of persistent cookie. PROMPT lets VPN user choose whether persistent cookie should be used or not. Possible values: ALLOW, DENY, PROMPT Default value: VPN_SESS_ACT_CVPN_PERSCOOKIE_DENY

emailHome

Sets the EMail home for the portal

allowedLoginGroups

The groups allowed login to VPN

encryptCsecExp

Enable encryption of client security expressions. Possible values: ENABLED, DISABLED Default value: VPN_SESS_ACT_DISABLED

appTokenTimeout

The timeout value in seconds for tokens to access cloud gateway applications Default value: 100 Minimum value: 1 Maximum value: 255

SecureBrowse

Enable and Disable the Secure Browse functionality. Possible values: ENABLED, DISABLED Default value: VPN_SESS_ACT_ENABLED

storefronturl

The Account Service or Auto Discovery url for this session.

Example

```
set vpn parameter -httpport 80 90 -winsIP
192.168.0.220 -dnsVserverName mydns -sessTimeout
240
```

Top

unset vpn parameter

Synopsis

unset vpn parameter [-httpPort] [-winsIP] [-dnsVserverName] [-splitDns] [-sessTimeout] [-clientSecurity] [-clientSecurityGroup] [-clientSecurityMessage] [-clientSecurityLog] [-authorizationGroup] [-clientIdleTimeout] [-allProtocolProxy | -httpProxy | -ftpProxy | -socksProxy | -gopherProxy | -sslProxy] [-proxyException] [-forceCleanup] [-clientOptions] [-clientConfiguration] [-loginScript] [-logoutScript] [-homePage] [-proxy] [-wihome] [-citrixReceiverHome] [-wiPortalMode] [-iipDnsSuffix] [-forcedTimeout] [-forcedTimeoutWarning] [-defaultAuthorizationAction] [-ntDomain] [-clientlessVpnMode] [-emailHome] [-clientlessModeUrlEncoding] [-clientlessPersistentCookie] [-allowedLoginGroups] [-appTokenTimeout] [-storefronturl] [-splitTunnel] [-localLanAccess] [-rfc1918] [-spoofIIP] [-killConnections] [-transparentInterception] [-proxyLocalBypass] [-clientCleanupPrompt] [-SSO] [-ssoCredential] [-windowsAutoLogon] [-useMIP] [-useIIP] [-clientDebug] [-icaProxy] [-ClientChoices] [-encryptCsecExp] [-SecureBrowse]

Description

Unset parameters for the SSL VPN feature..Refer to the set vpn parameter command for meanings of the arguments.

Top

show vpn parameter

Synopsis

show vpn parameter

Description

Display the configured vpn parameters.

Top

WI Commands

This group of commands can be used to perform operations on the following entities:

- wi site
- wi package

wi site

[add | rm | set | unset | bind | unbind | show]

add wi site

Synopsis

add wi site <sitePath> [<agURL> [<staURL> [-secondSTAURL <string> [-useTwoTickets (ON | OFF)]] [-sessionReliability (ON | OFF)]] [-authenticationPoint (WebInterface | AccessGateway) [-agAuthenticationMethod (Explicit | SmartCard)]]] [-wiAuthenticationMethods (Explicit | Anonymous) ...] [-defaultCustomTextLocale <defaultCustomTextLocale>] [-webSessionTimeout <positive_integer>] [-defaultAccessMethod <defaultAccessMethod>] [-loginTitle <string>] [-siteType (XenAppWeb | XenAppServices)] [-userInterfaceBranding (Desktops | Applications)] [-publishedResourceType <publishedResourceType>] [-kioskMode (ON | OFF)]

Description

Add a new Web Interface site for XenApp

Parameters

sitePath

The path of Web Interface site

agURL

The URL of Access Gateway

wiAuthenticationMethods

The method of authentication to be used at Web Interface Default value: WI_EXPLICIT

defaultCustomTextLocale

Choice of language Possible values: German, English, Spanish, French, Japanese, Korean, Russian, Chinese_simplified, Chinese_traditional Default value: LANG_EN

webSessionTimeout

Specifies the time-out value in minutes for idle Web browser sessions Default value: 20 Minimum value: 1 Maximum value: 1440

defaultAccessMethod

The default value of secure access method, which will be Direct in absence of agURL or GatewayDirect otherwise Possible values: Direct, Alternate, Translated, GatewayDirect, GatewayAlternate, GatewayTranslated

loginTitle

Title to be displayed on Login page Default value: "Welcome to Web Interface on NetScaler"

siteType

The type of site, whether site provides access through Web browser or XenApp Plugin Possible values: XenAppWeb, XenAppServices Default value: WI_XENAPPWEB

userInterfaceBranding

The user interface branding for the site, whether it is used for Applications or Desktops Possible values: Desktops, Applications Default value: WI_UIBRAND_APP

publishedResourceType

The method to access the published XenApp resources Possible values: Online, Offline, DualMode Default value: WI_ONLINE

kioskMode

Enables Kiosk Mode (discard user customizations) Possible values: ON, OFF Default value: OFF

Example

add wi site /Citrix/PNAgent -siteType XenAppServices

Top

rm wi site

Synopsis

rm wi site <sitePath>

Description

Remove existing Web Interface site for XenApp

Parameters

sitePath

The path of Web Interface site

Example

rm wi site /Citrix/PNAgent

Top

set wi site

Synopsis

set wi site <sitePath> [-agURL <string>] [-staURL <string>] [-sessionReliability (ON | OFF)] [-useTwoTickets (ON | OFF)] [-secondSTAURL <string>] [-wiAuthenticationMethods (Explicit | Anonymous) ...] [-defaultAccessMethod <defaultAccessMethod>] [-defaultCustomTextLocale <defaultCustomTextLocale>] [-webSessionTimeout <positive_integer>] [-loginTitle <string>] [-userInterfaceBranding (Desktops | Applications)] [-authenticationPoint (WebInterface | AccessGateway)] [-agAuthenticationMethod (Explicit | SmartCard)] [-publishedResourceType <publishedResourceType>] [-kioskMode (ON | OFF)]

Description

Modify a Web Interface site for XenApp

Parameters

sitePath

The path of Web Interface site

agURL

The URL of Access Gateway

staURL

The URL of Secure Ticket Authortity server

sessionReliability

Enables session reliability Possible values: ON, OFF Default value: OFF

useTwoTickets

Request tickets from two STA Servers, if available Possible values: ON, OFF Default value: OFF

secondSTAURL

The URL of the second Secure Ticket Authortity server

wiAuthenticationMethods

The method of authentication to be used at Web Interface Default value: WI_EXPLICIT

defaultAccessMethod

The default value of secure access method, which will be Direct in absence of agURL or GatewayDirect otherwise Possible values: Direct, Alternate, Translated, GatewayDirect, GatewayAlternate, GatewayTranslated

defaultCustomTextLocale

Choice of language Possible values: German, English, Spanish, French, Japanese, Korean, Russian, Chinese_simplified, Chinese_traditional Default value: LANG_EN

webSessionTimeout

Specifies the time-out value in minutes for idle Web browser sessions Default value: 20 Minimum value: 1 Maximum value: 1440

loginTitle

Title to be displayed on Login page Default value: "Welcome to Web Interface on NetScaler"

userInterfaceBranding

The user interface branding for the site, whether it is used for Applications or Desktops Possible values: Desktops, Applications Default value: WI_UIBRAND_APP

authenticationPoint

The authentication point to be used for the site Possible values: WebInterface, AccessGateway

agAuthenticationMethod

AGEE Authentication method. Default value is Explicit when Authpoint is AcessGateway Possible values: Explicit, SmartCard

publishedResourceType

The method to access the published XenApp resources Possible values: Online, Offline, DualMode Default value: WI_ONLINE

kioskMode

Enables Kiosk Mode (discard user customizations) Possible values: ON, OFF Default value: OFF

Example

```
set wi site /Citrix/PNAgent -staURL http://myStaServer
```

Top

unset wi site

Synopsis

unset wi site [-userInterfaceBranding]

Description

Use this command to remove wi site settings.Refer to the set wi site command for meanings of the arguments.

Top

bind wi site

Synopsis

bind wi site <sitePath> ((<farmName> <xmlServerAddresses> [-xmlPort <positive_integer>] [-transport <transport> [-sslRelayPort <positive_integer>]] [-loadBalance (ON | OFF)]) | ((-accessMethod <accessMethod> (-clientIpAddress <ip_addr> -clientNetMask <netmask>)) | (-translationInternalIp <ip_addr> -translationInternalPort <port|*> -translationExternalIp <ip_addr> -translationExternalPort <port|*> [-accessType <accessType>])))

Description

Add a new XenApp Farm to the Web Interface site for XenApp

Parameters

sitePath

The path of Web Interface site

farmName

The name of XenApp Farm

accessMethod

secure access method to be applied for client ip range Possible values: Direct, Alternate, Translated, GatewayDirect, GatewayAlternate, GatewayTranslated

translationInternalIp

Internal Ip Address to be tranlated from

Example

bind wi site /Citrix/XenApp Farm2 10.10.10.11

Top

unbind wi site

Synopsis

unbind wi site <sitePath> (<farmName> | ((-clientIpAddress <ip_addr> -clientNetMask <netmask>) | (-translationInternalIp <ip_addr> -translationInternalPort <port|*> -translationExternalIp <ip_addr> -translationExternalPort <port|*>)))

Description

Remove existing XenApp Farm from Web Interface site

Parameters

sitePath

The path of Web Interface site

farmName

The name of XenApp Farm

clientIpAddress

Client's Ip Address

translationInternalIp

Internal Ip Address to be tranlated from

Example

unbind wi site /Citrix/XenApp Farm2

Top

show wi site

Synopsis

show wi site [<sitePath>]

Description

Display existing Web Interface sites for XenApp

Parameters

sitePath

The path of Web Interface site

Example

show wi site

Top

wi package

[install | uninstall]

install wi package

Synopsis

install wi package [-jre <URL>] [-wi <URL>] [-maxSites <maxSites>]

Description

Install Web Interface for XenApp.

Parameters

jre

The location from where to get the java runtime package. Java package can be downloaded from http://ftp.riken.jp/pub/FreeBSD/ports/amd64/packages-6-stable/java/openjdk6-b17_2.tbz or http://www.freebsdfoundation.org/cgi-bin/download?download=diablo-jdk-freebsd6.amd64.1.6.0.07.02.tbz Default value: "file://tmp/diablo-jdk-freebsd6.amd64.1.6.0.07.02.tbz"

wi

The location from where to get the web interface package. Default value: "http://citrix.com/downloads/nswi-1.6.tgz"

maxSites

Maximum number of WI sites that can be created; changes the amount of RAM reserved for WI usage; changing its value results in restart of Tomcat & invalidates any existing WI session Possible values: 3, 25, 50, 100, 200, 500

Example

install wi package -jre http://10.102.1.10/diablo-latte-freebsd6-amd64-1.6.0_07-b02.tar.bz2 -wi http://citr

Top

uninstall wi package

Synopsis

uninstall wi package

Description

Remove the Web Interface for XenApp and all its configuration

Example

uninstall wi package

Top

Documentation Library

This appendix contains links to various NetScaler guides. You can either click the respective document ID to open the PDF version of the guide, or use the ID to search the guide in the Citrix Knowledge Center website available at http://support.citrix.com.

To search the guide on Citrix Knowledge Center website

1. Open the http://support.citrix.com link in a web browser.
2. Type the document ID in the Knowledge Center search text box and click **Search**.
3. Select the appropriate link from the search results.

Release Notes

Title	Document ID
Citrix NetScaler Release Notes	CTX132356

Quick Start Guides

Title	Document ID
Citrix NetScaler Quick Start Guide for NetScaler MPX	CTX132374
Citrix NetScaler Quick Start Guide for NetScaler MPX 5500	CTX132371
Citrix NetScaler Quick Start Guide for NetScaler MPX 7500, 9500	CTX132370
Citrix NetScaler Quick Start Guide for NetScaler MPX 9700, 10500, 12500, 15500	CTX132373
Citrix NetScaler Quick Start Guide for MPX 11500, 13500, 14500, 16500, 18500	CTX132379
Citrix NetScaler Quick Start Guide MPX 17550/19550/20550/21550	CTX132380
Citrix NetScaler Quick Start Guide for NetScaler MPX 17500, 19500, 21500	CTX132377
Citrix NetScaler Quick Start Guide for SDX 11500, 13500, 14500, 16500, 18500, 20500	CTX132785
Citrix NetScaler Quick Start Guide for SDX 17500/19500/21500	CTX132784
Citrix NetScaler Quick Start Guide for SDX 17550/19550/20550/21550	CTX132783

Configuration Guides

Title	Document ID
Citrix NetScaler Administration Guide	CTX132357
Citrix NetScaler AppExpert Guide	CTX132358
Citrix NetScaler Application Optimization Guide	CTX132361
Citrix NetScaler Application Security Guide	CTX132366
Citrix NetScaler Clustering Guide	CTX132840
Citrix Application Firewall Guide	CTX132360
Citrix NetScaler Getting Started Guide	CTX132368
Citrix Hardware Installation and Setup Guide	CTX132365
Citrix NetScaler Migration Guide	CTX132364
Citrix NetScaler Networking Guide	CTX132369
Citrix NetScaler Policy Configuration and Reference Guide	CTX132362
Citrix NetScaler SDX Administration	CTX132782
Citrix NetScaler Traffic Management Guide	CTX132359
Citrix NetScaler VPX Getting Started Guide	CTX132363

Reference Guides

Title	Document ID
Citrix NetScaler Command Reference Guide	CTX132384
Citrix NetScaler Developers Guide	CTX132367
Citrix NetScaler Glossary	CTX132383
Citrix NetScaler Log Message Reference	CTX132382
Citrix NetScaler SNMP OID Reference	CTX132381

Glossary

A

AAA

A NetScaler feature providing authentication, authorization, and auditing for all application traffic.

AAA-TM

See AAA. The configuration utility displays AAA as AAA-TM, meaning AAA traffic management.

access control

A general term denoting something that controls access to a resource. A more specific term is usually preferable.

Access Gateway

Former name of NetScaler Gateway.

action

A policy element that specifies what to do with a request or response that matches the expression in the policy. For example, if an expression in a policy matches a particular source IP address in a request, the action associated with the policy determines whether the connection is permitted.

action analytics

A NetScaler data-collection feature that can automatically optimize traffic in real time.

active-active mode

A deployment mode that, in addition to preventing downtime, makes efficient use of all the NetScaler ADCs in the deployment. In active-active deployment mode, the same virtual IP (VIP) addresses are assigned to all NetScaler ADCs in the configuration, but with different priorities, so that a given VIP can be active on only one ADC at a time. The ADCs can be configured so that no NetScaler ADC is idle.

ADC

See application delivery controller.

Amazon Elastic Block Store (EBS)

AWS feature that provides storage volumes that can be attached to EC2 instances.

Amazon Machine Image (AMI)

A special type of virtual appliance used to instantiate (create) a virtual machine within the Amazon Elastic Compute Cloud (EC2). It serves as the basic unit of deployment for services delivered through EC2.

AMI

See Amazon Machine Image.

AppFlow

A NetScaler feature that provides transaction-level visibility into HTTP, SSL, TCP, and SSL_TCP traffic flows.

application delivery controller (ADC)

A product, such as Citrix NetScaler, that optimizes delivery of applications. An ADC provides advanced features in addition to basic load balancing.

application visualizer

A graphical representation of an AppExpert application. Displays the public endpoints, application units, backend services, and policies that are configured for the application. You can use the Visualizer to obtain a visual overview of an AppExpert application's configuration and configure some of the displayed entities. By default, the Visualizer displays application units, services, and monitors for the selected application.

APV

See Attribute-Value Pair.

Attribute-Value Pair (APV)

AVPs are the basic units inside a Diameter and Radius message that carry authentication, security, and any other data pertaining to the application. There must be at least one AVP inside a Diameter or RADIUS message.

auditing

Feature that keeps a record of each user's activity on a protected server.

authentication

Feature for verifying client credentials, either locally or with a third-party authentication server, and allowing only approved users to access protected servers.

authorization

Feature for verifying which content on a protected server each user is allowed to access.

AWS region

Amazon EC2 is hosted in multiple locations world-wide. These locations are composed of regions and Availability Zones. Each region is a separate geographic area. Each region has multiple, isolated locations known as Availability Zones. Amazon EC2 gives you the ability to place resources, such as instances, and data in multiple locations. Resources are not replicated across regions unless you do so specifically.

B

back end

The server-facing side of a network.

bind point

An entity, or a stage of traffic processing, at which traffic is examined to see if it matches a policy. For example, a bind point can be a load balancing virtual server, or it can apply to all traffic at given stage of processing, such as when a request is received or when a response is sent.

bridge group

A NetScaler feature for merging multiple VLANs into a single broadcast domain.

C

cache redirection

A policy and virtual-server based NetScaler feature that evaluates the type of content requested and directs requests to a cache instead of a server.

call home

A NetScaler feature that monitors the appliance and automatically uploads data to the Support server if an error condition is detected.

CEA

Capabilities Exchange Answer. A message used by the Diameter protocol to establish a connection.

CER

Capabilities Exchange Request. A message used by the Diameter protocol to establish a connection.

certificate-key pair

An SSL certificate and its corresponding private key. Stored on a NetScaler ADC that offloads SSL processing from servers.

classic policy

The older, less robust type of NetScaler policy.

CLI

Command-line interface.

client

A computer that receives data from a server. Can also refer to a person.

client data plane

The logical grouping of the physical connections between the cluster nodes and the client-side connecting device.

client drive mapping

A method that enables users to access some or all of their clients' drives from an application running on an application server.

client keep-alive

A setting that enables receiving multiple client requests on a single client connection. Applies only to HTTP and HTTPS services.

CloudBridge Connector

A NetScaler feature for connecting a datacenter to a cloud or another datacenter. The feature establishes a "CloudBridge Connector tunnel" between the connected entities.

CloudFormation

An Amazon Web Services (AWS) feature for managing cloud resources. Uses templates to manage groups of resources, which are called "stacks."

CloudPlatform

A Citrix software platform (powered by Apache CloudStack) that pools computing resources to build public, private, and hybrid Infrastructure as a Service (IaaS) clouds.

cluster

A group of nCore appliances working together as a single system image. The cluster can include as few as 2 or as many as 32 NetScaler nCore hardware or virtual appliances as nodes. The client traffic is distributed between the nodes to provide high availability, high throughput, and scalability.

cluster backplane

The logical grouping of the physical connections between the cluster nodes and the cluster backplane switch. The nodes of a cluster communicate with each other over the cluster backplane.

cluster backplane switch

A switch through which cluster nodes communicate with each other.

cluster instance

A logical entity created on the first node added to a NetScaler cluster. The cluster instance is assigned a cluster ID, which uniquely identifies the cluster.

cluster IP address

The management IP address of a cluster, through which configuration tasks must be performed. This IP address is owned by the cluster's configuration coordinator.

cluster link aggregation

A feature combining groups of cluster interfaces into channels. Similar to NetScaler link aggregation, but without the requirement that all interfaces be on the same appliance. The interfaces can be on different nodes of the same cluster.

cluster node

A NetScaler ADC that is part of a cluster.

cluster propagation

The process through which configurations that are performed on the cluster IP address are propagated to all the nodes of the cluster.

cluster synchronization

The process through which cluster configurations are synchronized to appliances that are added as cluster nodes or to nodes that rejoin the cluster.

clustering

The process of creating a cluster of NetScaler ADCs.

collector

An AppFlow entity that receives flow records generated by a NetScaler appliance.

community string

A password for authenticating SNMP queries from SNMP managers.

configuration coordinator

The cluster node on which cluster configurations are performed and then propagated to the other cluster nodes. The configuration coordinator owns the cluster IP address.

configuration utility

The NetScaler graphical user interface (GUI).

console

The command line interface accessed through the console port of a NetScaler appliance.

content filtering

A NetScaler feature that takes a user-specified action when the something in the header of a request or response matches a policy.

content group

A group of all virtual servers and policies involved in a particular content switching configuration.

content switching

Load balancing that bases server selection on the type of content requested.

critical interface

A NetScaler interface that, if it fails or is disabled, triggers a high-availability (HA) failover.

crossover cable

An Ethernet cable in which the sending and receiving wires are crossed.

D

dashboard

An interface element that displays performance data in graphical form.

data set

A specialized form of pattern set, consisting of an array of patterns of type number (integer), IPv4 address, or IPv6 address.

datacenter

A facility housing computer systems and associated components, such as telecommunications and storage systems. Usually includes redundant or backup power supplies, redundant data communications connections, environmental controls such as air conditioning and fire suppression, and security devices.

DataStream

NetScaler feature for load balancing database servers.

default syntax policies

The newer type of NetScaler policies, which provide more capabilities than do classic policies. Most NetScaler features are migrating from classic to default syntax policies.

Desktop Director

A Citrix product that provides a detailed and intuitive overview of XenDesktop environments.

Diameter

An Authentication, Authorization, and Accounting (AAA) protocol derived from RADIUS.

direct server return (DSR)

A NetScaler load balancing mode in which servers send responses directly to the clients, instead of through the NetScaler ADC.

Disconnect Peer Acknowledgment (DPA)

A response acknowledging a DPR.

Disconnect Peer Request (DPR)

A Diameter request sent to a peer to initiate session termination.

down state flush

A NetScaler feature for delayed cleanup of a virtual-server's connections. Connections remain open until the virtual server enters the DOWN state.

DPA

See Disconnect Peer Acknowledgment.

DPR

See Disconnect Peer Request.

DSR

See direct server return.

E

EBS

See Amazon Elastic Block Store.

EC2

See Elastic Cloud Compute.

effective state

Cumulative state of the primary and backup virtual servers. If any of virtual servers in the chain is UP, the effective state is UP. For a GSLB service, the effective state reflects the effective state of the corresponding load balancing virtual server. (A load balancing *service* has no effective state.)

Elastic Cloud Compute (EC2)

Amazon Web Services (AWS) feature with which users create virtual computers (instances).

Elastic Network Interface (ENI)

An Amazon Web Services (AWS) virtual network interface that you can attach to an instance in a virtual private cloud (VPC).

ENI

See Elastic Network Interface.

ETag

An identifier assigned by a web server to a specific resource at a URL. Useful for cache validation and for preventing one simultaneous update of a resource from overwriting another.

expression

A logic statement, such as a Perl Compatible Regular Expression (PCRE), specifying the characteristics of requests or responses that match the policy of which the expression is a part. Also called a *rule*.

F

failover interface set

A pair of interfaces, with each interface on a different appliance. If one appliance fails, process is transferred to the other appliance without triggering a failover event.

Federal Information Processing Standards (FIPS)

Standards developed by the National Institute for Standards and Technology (NIST) to ensure compliance with federal security and data-privacy requirements.

field replaceable unit (FRU)

A NetScaler component that can be replaced by the user.

FIPS

See Federal Information Processing Standards.

FRU

See field replaceable unit.

flow processor

The cluster node that is selected as the node to process the traffic. The flow processor receives the traffic from the flow receiver through the cluster backplane.

flow receiver

The cluster node that receives traffic from the external network. The flow receiver node steers or forwards the traffic to the flow processor through the cluster backplane.

front end

The client-facing side of a network.

G

global server load balancing (GSLB)

A NetScaler feature that performs load balancing across data centers in a WAN.

GSLB

See global server load balancing.

GUI

See configuration utility.

H

HDX Insight

NetScaler Insight Center component that monitors ICA traffic.

high availability (HA)

A deployment mode in which one appliance (the primary) is backed up by another appliance (the secondary). If the primary appliance fails, a failover event transfers control to the secondary appliance.

HA

See high availability.

I

IAM

See Identity and Access Management.

INC

See Independent Network Configuration (INC) mode.

Identity and Access Management (IAM)

An Amazon Web Services (AWS) feature with which you can control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups and use permissions to allow or deny their access to AWS resources.

ICA

See Independent Computing Architecture (ICA)

Independent Computing Architecture (ICA)

Citrix proprietary protocol for XenApp and XenDesktop traffic.

Independent Network Configuration (INC) mode

A type of High availability deployment in which the two HA nodes reside in different networks. The following independent network entities and configurations are neither propagated nor synced to the other node: MIPs, SNIPs, VLANs, routes (except LLB routes), route monitors, RNAT rules (except any RNAT rule with a VIP as the NAT IP), and dynamic routing configurations.

information element

A description of an attribute that can appear in an IPFIX Record. RFC5102 defines the base set of IPFIX information elements.

inline mode

A two-arm deployment mode in which the traffic between clients and servers passes through the deployed appliance.

IP set

A set of subnet IP (SNIP) addresses and virtual IP (VIP) addresses, identified with a meaningful name indicating the usage of the IP addresses contained in the set.

L

link load balancing (LLB)

A NetScaler feature that balances outbound traffic across multiple Internet connections provided by different service providers.

Linkset

An entity specifying interfaces through which a node can connect to the external switch through the cluster backplane. Linksets must be used for traffic distribution in an asymmetric (some nodes not connected to the external switch) cluster topology. Linksets can be used exclusively or combined with ECMP or cluster link aggregation.

load balancing

A core NetScaler feature that distributes user requests for web pages and other protected applications across multiple servers that all host (or mirror) the same content.

load balancing virtual server

The IP address, port, and protocol combination to which a client sends connection requests for a particular load-balanced website or application. If the application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area

network (WAN), the VIP is usually a private (ICANN non-routable) IP address.

M

management service

The graphical user interface (GUI) of a NetScaler SDX appliance. Also used on some CloudBridge appliances.

mapped IP (MIP)

Mapped IP address. A NetScaler IP address used for server-side connections. Citrix recommends using a subnet IP (SNIP) address instead.

MEP

Metric Exchange Protocol, a Citrix protocol used for GSLB.

MIP

See mapped IP.

MIR

See multiple IP response.

monitor

A NetScaler entity that periodically probes each service to which you assign it. If a service does not respond within a specified interval, and the specified number of probes fail, the service is marked DOWN. In that case, the monitor continues to send probes, and can change the status to UP.

multiple IP response (MIR)

A GSLB option for the NetScaler ADC to send multiple IP addresses in response to a DNS request.

multitenant

A configuration in which multiple clients are served from the same platform.

N

named expression

An expression that has been assigned a name, which is used instead of the expression itself in a policy.

nCore

The multiple-core, 64-bit version of the NetScaler operating system.

negative caching

The caching of negative responses from servers in a domain, to speed up responses to queries.

net profile

An information set that contains NetScaler owned IP addresses (IP set) or an IP address. During communication with physical servers or peers, the NetScaler ADC uses the addresses specified in the profile as source IP addresses.

netbridge

A logical container that holds or represents a CloudBridge Connector tunnel configuration on a NetScaler appliance. A GRE tunnel entity is associated with the netbridge. A particular CloudBridge Connector tunnel configuration on a NetScaler appliance is identified by the name of the netbridge entity.

netmask

A network mask. Also called a *subnet mask*.

NetScaler Gateway

A NetScaler feature (also available as a standalone appliance) that provides secure access to a LAN or WAN from any location on the Internet.

NetScaler Insight Center

A Citrix virtual appliance that can monitor NetScaler appliances.

NetScaler IP (NSIP)

NetScaler IP address. The IP address for management and general system access to the NetScaler appliance.

NetScaler owned IP address

An IP address that exists only on a NetScaler ADC. NetScaler owned IP addresses can be of the following types: NetScaler IP address (NSIP), Virtual IP addresses (VIPs), Subnet IP addresses (SNIPs), and global server load balancing site IP addresses (GSLBIPs). The NetScaler IP address (NSIP) uniquely identifies the NetScaler ADC on your network, and it provides access to the ADC. A Virtual IP address (VIP) is a public IP address to which a client sends requests. The NetScaler ADC terminates the client connection at the VIP and initiates a connection with a server. This new connection uses a subnet IP address (SNIP) as the source IP address for packets forwarded to the server. If you have multiple data centers that are geographically distributed, each data center can be identified by a unique global server load balancing site IP address (GSLBIP).

NetScaler software

The NetScaler operating system.

NetScaler VPX

A NetScaler virtual machine image that can be installed on a virtualization platform.

NetScaler Web Logging (NSWL) client

Software installed on the client system to collect logs of HTTP and HTTPS requests.

network visualizer

A Network feature that displays the network configuration of a NetScaler ADC, including the network configuration of the nodes in a high availability (HA) deployment. You can also modify the configuration of VLANs, interfaces, channels, and bridge groups, and perform HA configuration tasks.

Next Secure (NSEC)

A DNS record showing that no records exist between two points.

NITRO

The NetScaler API suite.

node group

A group of cluster nodes that have a specific set of cluster configurations. Node groups are used to define partially striped configurations.

node instance

A logical entity on a cluster node. The node instance is assigned a node ID, which uniquely identifies the node.

non-INC mode

A high availability-deployment mode in which both HA nodes are in the same network.

NSIP

See NetScaler IP.

NSVLAN

The virtual LAN (VLAN) to which the subnet that includes the NetScaler management IP (NSIP) address is bound. This subnet is available only on interfaces that are associated with NSVLAN.

O

one-arm mode

Configuration in which only one NetScaler interface is connected to an Ethernet segment.

P

partially striped configuration

A configuration available on a subset of cluster nodes. The subset is defined by the node group.

pattern set

An array of indexed patterns used for string matching during default syntax policy evaluation. Example of a pattern set: image types {svg, bmp, png, gif, tiff, jpg}. Also called a patset.

policy

An entity that identifies requests or responses on which to perform specified actions. A policy is essentially of the form: if <expression>, do <action>

policy binding

The act of binding a policy to a bind point, which determines the instant at which the policy is invoked. A policy can be bound to a virtual server or globally to the NetScaler appliance.

pre-shared key

A text string manually configured on CloudBridge peers. The strings are matched against each other for authentication before security associations are established.

profile

A collection of settings that enable a feature to perform a complex function. For example, in the application firewall, a profile for XML data can perform multiple screening operations, such as examining the data for illegal XML syntax or evidence of SQL injection.

R

rate limit identifier

A named entity that specifies numeric rate-limiting thresholds, such as the maximum number of requests or connections (of a particular type) that are permitted in a specified period called a *time slice*.

rate limiting

A NetScaler feature with which you can configure the appliance to monitor the rate of traffic associated with an entity and take preventive action, in real time, when the rate reaches a specified value.

reboot

To restart an appliance.

redirection

Sending a client request to a different web page or server.

Request Switching

Citrix technology that enables an appliance to multiplex and offload TCP connections, maintain persistent connections, and manage traffic at the request (application layer) level.

responder

NetScaler feature that sends an automatic response based on who sent the request, where it is from, and other criteria with security and system-management implications.

REST interface

REpresentational State Transfer interface. A software architecture for using simple HTML calls to create or modify information on a server.

rewrite

NetScaler feature that modifies information in the headers or bodies of requests or responses.

rule

A policy element consisting of a logical expression used to evaluate requests or responses. If the evaluation returns TRUE, the action that is bound to the policy is performed.

S

SDX

An advanced NetScaler or CloudBridge platform hosting virtual machines (VMs). NetScaler SDX hosts multiple NetScaler VMs. CloudBridge SDX hosts a NetScaler VM and multiple CloudBridge VMs.

Secure Ticket Authority (STA)

The XenApp/XenDesktop entity responsible for issuing session tickets in response to connection requests for published applications on XenApp and published desktops on XenDesktop. These session tickets form the basis of authentication and authorization for access to published resources.

selectlets

A group of non-compound, default syntax expressions, each of which is called a selectlet. A traffic stream selector can contain up to five selectlets. Each selectlet is considered to be in an AND relationship with the other expressions.

selector

A filter for identifying requests, or for identifying objects in a content group.

server data plane

The logical grouping of the physical connections between cluster nodes and the server-side connecting device.

server object

A virtual entity representing a physical server. Enables naming a server, rather than identifying it by its IP address.

service

The IP address, port, and protocol combination used to route requests to a specific load-balanced application server. A service can be a logical representation of the application server itself, or of an application running on a server that hosts multiple applications. After creating a service, you bind it to a virtual server.

sessionless load balancing

Load balancing on a per packet basis, without storing session information. Reduces NetScaler resource requirements. Used in DSR mode.

shell

Refers to the BSD command shell unless otherwise stated.

single sign-on (SSO)

A Citrix password manager that provides access to multiple password-protected information systems in a Citrix environment without requiring multiple authentications.

single-hop mode

The mode in which NetScaler Insight Center collects data from NetScaler appliances handling connections in which users connect to XenApp and XenDesktop applications through a NetScaler Gateway appliance.

slow start

A NetScaler feature that avoids assigning all new connections to a server when it is added to the network.

spotted configuration

A configuration that is available on only a single cluster node.

SSO profile

In forms-based single signon (SSO), the profile that defines how to handle an authentication request that matches the associated policy.

start

To start an appliance (formerly "boot").

stream selector

A filter for identifying an entity for which you want to throttle access.

string map

A NetScaler entity, consisting of key-value pairs, that can be used for pattern matching in all NetScaler features that use the default policy syntax.

striped configuration

A configuration available on all nodes of a cluster.

subnet IP (SNIP)

Subnet IP address. A NetScaler-owned IP address used for server-side connections.

SureConnect

A NetScaler feature that directs requests to an alternative web page if the primary page is DOWN.

Sysid

See system ID

SYSLOG

A standard logging protocol, implemented on a SYSLOG auditing module, (which runs on the monitored appliance), and a SYSLOG server, which can run on a remote system. SYSLOG uses User Data Protocol (UDP) for data transfer.

system ID (sysid)

A number, or possibly characters, identifying an appliance or virtual appliance.

T

thick provisioned format

VMDK format in which all physical disk space required for a virtual disk is allocated and zeroed out (wiped) when the disk is first created. In other words, space for a thick provisioned VMDK is reserved in advance for that VMDK only. You cannot overallocate physical disk space if you use thick provisioned VMDKs, which limits the number and size of VMDKs and can waste physical disk space, but ensures that you will have enough physical disk space in all circumstances.

thin provisioned format

VMDK format in which physical disk space needed for a virtual disk is allocated and zeroed out (wiped) only when the VMDK is written to the physical disk. In other words, space for a thin provisioned VMDK is allocated dynamically as needed; physical disk space is not allocated and reserved in advance. You can overallocate physical disk space if you use thin provisioned VMDKs, which allows you to put more and larger VMDKs on a given

physical disk and avoid wasting unused space, but risks running out of physical disk space if your VMDKs are too full.

time stamp

Data indicating when an event occurred.

timeout

A setting indicating when an entity is to become unavailable (for example, how long a connection can remain idle without being closed). Also, the act of becoming unavailable after the specified period of time.

tracing

The use of trace files to debug problems in the flow of packets to the cluster nodes. The NetScaler operating system includes a utility called nstrace, which provides a dump of the packets received and sent by the appliance, and stores the packets in trace files. You use the Wireshark application to view the trace files.

traffic domains

A NetScaler feature with which you can create multiple isolated environments within a the appliance. An application belonging to a specific traffic domain communicates with entities and processes traffic within that domain. You can, for example, use the same IP address in different domains.

transparent mode

An operational mode in which an appliance between the end points of a connection does not have its own IP address. The appliance intercepts packets that one end point sends to the other.

two-arm mode

A deployment mode in which two network interfaces on the deployed appliance are connected to different Ethernet segments.

U

Use Source IP (USIP)

A NetScaler mode in which the ADC uses the client's IP address, instead of a SNIP address, in packets sent to the server.

USNIP

NetScaler mode that uses a subnet IP (SNIP) address as the source IP address of packets sent to the server, and as the address at which packets are received from the server. This mode is enabled by default.

V

view based access control model (VACM)

An SNMPv3 feature that enables you to configure access rights to a specific subtree of the MIB on the basis of various parameters, such as security level, security model, user name, and view type. You can configure agents to provide different levels of MIB access to different managers.

virtual IP (VIP)

A virtual IP (VIP) address is the IP address associated with a virtual server. It is the IP address to which clients connect for access to one of the servers represented by the virtual server. An appliance managing a wide range of traffic might have many virtual servers, each configured with its own VIP address. Some of the attributes of a VIP address are customized to meet the requirements of the virtual server.

virtual machine disk (VMDK)

File format for virtual disk drives. Originally developed by VMWare, but now an open format that is widely used in many types of clouds and virtual machines (VMs).

VMDK

See virtual machine disk

virtual server

A NetScaler entity with an IP address to which clients send requests. Distributes the requests to physical servers.

VPX

See NetScaler VPX.

W

waterfall chart

A NetScaler Insight Center chart that shows the cumulative effect of sequentially introduced positive or negative values.

Web 2.0 push

A NetScaler feature in which the NetScaler ADC functions as a proxy server to offload long-lived client TCP connections and maintain relatively fewer, reusable connections to the server.

Web Insight

A component of NetScaler Insight Center. Monitors HTTP traffic.

Web Interface

A NetScaler feature that provides access to Citrix XenApp and Citrix XenDesktop applications. Users access resources through a standard web browser or by using the Citrix XenApp plug-in.

web server logging

A NetScaler feature that sends logs of HTTP and HTTPS requests to a client system for storage and retrieval.

wildcard virtual server

A virtual server that accepts all traffic.

X

XenApp

A Citrix on-demand application delivery solution that enables any Windows application to be virtualized, centralized, and managed in the datacenter, and instantly delivered as a service to users anywhere on any device.

XenCenter

Management application for XenServer. You can use XenCenter to create, deploy, manage, and monitor virtual machines (VMs) from a Windows computer.

XenDesktop

A Citrix desktop virtualization and VDI solution that delivers a complete Windows desktop experience as an on-demand service to any user, anywhere.

XenServer

The Citrix open-source virtualization platform.

Syslog Message Reference

Feature	Message	Category	Description	Format
AAA	LOGIN_FAILED	WARNING	When the aaa module failed to login the user.The reason for failure is indicated in the message	"User%s-Client_ip%s-Failure_reason\"%s\""
AAA	EXTRACTED_GROUPS	INFO	After a user logs in the group for the user has been extracted	"Extracted_groups\"%s\""
UI	CMD_EXECUTED	INFO	Logs the NSCLI/GUI command executed in NetScaler	"User%s-Remote_ip%s-Command\"%s\"-""Status\"%s\""
SSLVPN	LOGIN	INFO	SSLVPN login succeeds	"User%s-Client_ip%s-""Nat_ip%s-Vserver%s:%d-Browser_type\"%s\"-SSLVPN_client_type%s-Group(s)\"%s\""
SSLVPN	LOGOUT	INFO	SSLVPN session logs out.Logout method is captured in the message	"User%s-""Client_ip%s-Nat_ip%s-""Vserver%s:%d-""Start_time\"%s\"-End_time\"%s\"-Duration%s-""Http_resources_accessed%s-NonHttp_services_accessed%s-""Total_TCP_connections%d-Total_UDP_flows%d-""Total_policies_allowed%d-Total_policies_denied%d-""Total_bytes_send%s-Total_bytes_recv%s-""Total_compressedbytes_send%s-Total_compressedbytes_recv%s-""Compression_ratio_send%d.%02u%%-""Compression_ratio_recv%d.%02u%%-""LogoutMethod\"%s\"-Group(s)\"%s\""
SSLVPN	ICASTART	INFO	ICA application launch has started	"Source%s:%d-Destination%s:%d-""username:domainname%s-""applicationName%s-startTime\"%s\"-""connectionId%x"
SSLVPN	ICAEND_CONNSTAT	INFO	ICA application has terminated	"Source%s:%d-Destination%s:%d-username:domainname%s-

				""startTime\"%s\"-endTime\"%s\"-""Duration%s-Total_bytes_send%d-Total_bytes_recv%d-""Total_compressedbytes_send%d-Total_compressedbytes_recv%d-""Compression_ratio_send%d.%02u%%-Compression_ratio_recv%d.%02u%%-""connectionId%x"
SSLVPN	TCPCONNSTAT	INFO	Logs the TCP connection related information for a connection belonging to a SSLVPN session	"User%s-Client_ip%s-Nat_ip%s-Vserver%s:%d-""Source%s:%d-Destination%s:%d-Start_time\"%s\"-End_time\"%s\"-""Duration%s-Total_bytes_send%d-Total_bytes_recv%d-""Total_compressedbytes_send%d-Total_compressedbytes_recv%d-""Compression_ratio_send%d.%02u%%-Compression_ratio_recv%d.%02u%%-Access%s-Group(s)\"%s\""
SSLVPN	TCPCONN_TIMEDOUT	INFO	An SSLVPN connection timed out.The information about the connection start and end time the amount of data transferred and received are present in the message date	"User%s-Client_ip%s-""Nat_ip%s-Vserver%s:%d-Last_contact\"%s\"-Group(s)\"%s\""
SSLVPN	UDPFLOWSTAT	INFO	When a UDP flow , within a SSLVPN session, terminates	"User%s-Client_ip%s-""Nat_ip%s-Vserver%s:%d-Source%s:%d-""Destination%s:%d-Start_time\"%s\"-End_time\"%s\"-""Duration%s-Total_bytes_send%d-""Total_bytes_recv%d-Access%s-Group(s)\"%s\""
SSLVPN	HTTPREQUEST	INFO	A SSLVPN session receives a HTTP request	"%sUser%s:Group(s)%s:Vserver%s:%d-%s%s%s%s"
SSLVPN	NONHTTP_RESOURCEACCESS_DENIED	NOTICE	A non-http resource access is denied by policy engine. The denied policy name is captured in the log message.	"User%s-Client_ip%s-Nat_ip%s-""Vserver%s:%d-Source%s:%d-Destination%s:%d-""Total_bytes_send%d-Total_bytes_recv%d-Denied_by_policy\"%s\"-

				Group(s)\"%s\""
SSLVPN	HTTP_RESOURCEACCESS_DENIED	NOTICE	A http resource access is denied by policy engine. The denied policy name is captured in the log message.	"User%s-Vserver%s:%d-Total_bytes_send%d-Remote_host%s-""Denied_url%s-Denied_by_policy\"%s\"-Group(s)\"%s\""
SSLVPN	LICLMT_REACHED	INFO	SSLVPN license limit reached	"Vserver%s:%d-License_limit%d"
SSLVPN	CLISEC_CHECK	ERROR	Logs with severity ERROR when client security check for a SSLVPN session fails, otherwise logs with severity DEBUG	"User%s-ClientIP%s-Vserver%s:%d-Client_security_expression\"%s\"-"
SSLVPN	CLISEC_EXP_EVAL	ERROR	Logs with severity ERROR when client security expression evaluates to False, otherwise logs with severity DEBUG	"User%s:-ClientIP%s-Vserver%s:%d-""Clientsecurityexpression%sevaluatedto%s(%d)"
SSLVPN	STA_VALIDATE_RESP	INFO	After a user logs into SSLVPN and the group for the user has been extracted	"Xdatalen%d-Xdata%s"
EVENT	ALERTSTARTED	ALERT	When SNMP module starts an alarm (usually when the value of a monitored attribute crosses the threshold value	"%s"
EVENT	ALERTENDED	ALERT	When SNMP module stops an alarm (usually when the value of a monitored attribute returns to normal state)	"%s"
EVENT	STARTSYS	INFO	When NetScaler starts	"%s"
EVENT	STARTCPU	INFO	When a particular CPU starts	"%s"
EVENT	DEVICEDOWN	NOTICE	Whenever a device is down	"%s"
EVENT	DEVICEOFS	NOTICE	Whenever a device is out of service	"%s"
EVENT	DEVICEUP	NOTICE	Whenever a device is up	"%s"
EVENT	NICSTART	NOTICE	When the network interface is started	"%s"
EVENT	NICSTOP	NOTICE	When the network	"%s"

			interface is stopped	
EVENT	NICHANG	NOTICE	When the network interface is in hung state	"%s"
EVENT	NICRESET	NOTICE	When the network interface is reset	"%s"
EVENT	NICMIGRATE	NOTICE	When an interface is bound or unbound from a channel	"%s"
EVENT	STOPSYS	INFO	When the NetScaler system is stopped	"%s"
EVENT	FREEBADMEM	EMERGENCY	When bad memory is freed (internal error)	"%s"
EVENT	FREEDUPMEM	EMERGENCY	When duplicate memory free occurs (internal error)	"%s"
EVENT	FREEEXTMEM	EMERGENCY	When memory is freed from a wrong pool (internal error)	"%s"
EVENT	PROPSUCCESS	INFO	When HA propagation is successful	"%s"
EVENT	PROPFAIL	ALERT	When HA propagation fails	"%s"
EVENT	STATECHANGE	0	HA State has changed.The string along with the message gives more information	"%s"
EVENT	CLSTATECHANGE	0	Cluster State has changed.The string along with the message gives more information	"%s"
EVENT	CACHESTARTFLUSH	INFO	When cache flush starts	"%s"
EVENT	CACHESTOPFLUSH	INFO	When cache flush is complete	"%s"
EVENT	MONITORTH	INFO	The monitor bound to the service has hit threshold limit	"%s"
EVENT	MONITORDOWN	INFO	The monitor bound to the service is down.	"%s"
EVENT	MONITORUP	INFO	The monitor bound to the service is up.	"%s"
EVENT	ROUTEDOWN	INFO	When the route is down	"%s"
EVENT	ROUTEUP	INFO	When the route is up	"%s"
EVENT	VRID6DOWN	INFO	When the vrid changes state to	"%s"

			backup	
EVENT	VRIDDOWN	INFO	When the vrid changes state to backup	"%s"
EVENT	VRIDUP	INFO	When the vrid changes state to master	"%s"
EVENT	VRIDINIT	INFO	When the vrid changes state to init	"%s"
EVENT	VIPRHIUP	INFO	When the rhi state of vip changes to up	"%s"
EVENT	VIPRHIDOWN	INFO	When the rhi state of vip changes to down	"%s"
EVENT	STARTSAVECONFIG	INFO	When save configuration started	"%s"
EVENT	STOPSAVECONFIG	INFO	When save configuration has stopped	"%s"
EVENT	CONFIGSTART	INFO	When NetScaler starts to read the configuration from ns.conf file (during boot-up)	"%s"
EVENT	CONFIGEND	INFO	When NetScaler has completed reading the configuration from ns.conf file (during boot-up)	"%s"
EVENT	NICLACPSC	NOTICE		"%s"
EVENT	NICLOW_THROUGHPUT	NOTICE	When an interface's throughput is less than the min required	"%s"
EVENT	NICNORMAL_THROUGHPUT	NOTICE	When an interface's throughput is equal or greater than the min required	"%s"
EVENT	NICPOWERON	NOTICE	When an interface is powered on	"%s"
EVENT	NICPOWEROFF	NOTICE	When an interface is powered off	"%s"
EVENT	DHCPSVRERR	INFO	When the DHCP server sends an invalid setting	"%s"
EVENT	DHCPCAQUIRE	INFO	When the DHCP client aquires a lease	"%s"
EVENT	DHCPCRELEASE	INFO	When the DHCP client releases a lease	"%s"
EVENT	DHCPCDEPENDPBR	INFO	When the DHCP lease is released	"%s"

			and a PBR is dependent on the lease ip	
EVENT	ROUTE6DOWN	INFO	When the route6 is down	"%s"
EVENT	ROUTE6UP	INFO	When the route6 is up	"%s"
EVENT	UNKNOWN	DEBUG		"%s"
SSLLOG	SSL_HANDSHAKE_FAILURE	DEBUG	SSL HandShake Failure	"SPCBId%d-ClientIP%s-ClientPort%d-"\"VserverServiceIP%s-VserverServicePort%d-"\"ClientVersion%s-CipherSuite\"%s\""
SSLLOG	SSL_HANDSHAKE_SUCCESS	DEBUG	SSL HandShake Success	"SPCBId%d-ClientIP%s-ClientPort%d-"\"VserverServiceIP%s-VserverServicePort%d-"\"ClientVersion%s-CipherSuite\"%s\"-"\"Session%s"
SSLLOG	SSL_CERT_EXPIRY_IMMINENT	NOTICE	SSL Certificate Expiry Imminent	"CertificateKeyPair%s-DaysToExpire%u"
SSLLOG	SSL_HANDSHAKE_ISSUERNAME	DEBUG	SSL Client Certificate IssueName	"SPCBId%d-IssuerName\"%s\""
SSLLOG	SSL_HANDSHAKE_SUBJECTNAME	DEBUG	SSL Client Certificate SubjectName	"SPCBId%d-SubjectName\"%s\""
SSLLOG	SSL_CRL_UPDATE_SUCCESS	NOTICE	SSL CRL Update Success	"crl_name%s-server_ip%s-server_port%d-"\"methodLDAP-ldapscope%s-"
SSLLOG	SSL_CRL_UPDATE_FAILURE	NOTICE	SSL CRL Update Failure	"crl_name%s-server_ip%s-server_port%d-"\"methodLDAP-ldapscope%s-"
APPFW	APPFW_STARTURL	INFO	AppFw StartURL violation	"DisallowIllegalURL.");}else{
APPFW	APPFW_DENYURL	INFO	AppFw DenyURL violation	"DisallowDenyURLforrulepattern=\"%s\"."
APPFW	APPFW_REFERER_HEADER	INFO	AppFw Referer header violation	"parsingrefererheader'%s'failed"
APPFW	APPFW_CSRF_TAG	INFO	AppFw CSRF tag violation	"CSRFTagvalidationfailed");}
APPFW	APPFW_XSS	INFO	AppFw XSS violation	"%sCross-sitescriptcheckfailedfor%s%s=\"%s\""
APPFW	APPFW_XML_XSS	WARNING	AppFw XSS violation in XML	"%sCross-sitescriptcheckfailedfor%s%s=\"%s\""
APPFW	APPFW_SQL	INFO	AppFw SQL Injection violation	"%s%sKeywordcheckfailedfor%s%s=\"%s\""
APPFW	APPFW_XML_SQL	WARNING	AppFw SQL Injection violation in	"%s%sKeywordcheckfailedfor%s%s=\"%s\""

			XML	
APPFW	APPFW_COOKIE	INFO	AppFw Cookie Consistency violation	"%sCookievalidationfailedfor%s%s%s%s"
APPFW	APPFW_FIELDCONSISTENCY	INFO	AppFw Field Consistency violation	"%sFieldconsistencycheckfailedforfield%s"
APPFW	APPFW_BUFFEROVERFLOW_URL	INFO	AppFw Buffer Overflow violation in URL	"URLlength(%d)isgreaterthanmaximumallowed(%d)."
APPFW	APPFW_BUFFEROVERFLOW_COOKIE	INFO	AppFw Buffer Overflow violation in Cookie	"Cookieheaderlength(%d)isgreaterthanmaximumallowed(%d)."
APPFW	APPFW_BUFFEROVERFLOW_HDR	INFO	AppFw Buffer Overflow violation in HTTP Headers	"Header(%s)length(%d)isgreaterthanmaximumallowed(%d)."
APPFW	APPFW_FIELDFORMAT	INFO	AppFw Field Format violation	"%sFieldformatcheckfailedforfield%s=\"%s\""
APPFW	APPFW_SAFECOMMERCE	INFO	AppFw Safe Commerce violation	"%sCreditCardinternalerror(%d)whilematching...takingprecautionaryaction"
APPFW	APPFW_SAFECOMMERCE_XFORM	INFO	AppFw Safe Commerce violation detected and transformed	"%sTransformed(xout)potentialcreditcardnumbersseeninserverresponse"
APPFW	APPFW_SAFEOBJECT	INFO	AppFw Safe Object violation	"%sSafeObjectinternalerror(%d)whilematching...takingprecautionaryaction:%s"
APPFW	APPFW_POLICY_HIT	INFO	AppFw profile invoked	"%s%u-PPE%u%s%s%s <%s>"
APPFW	APPFW_POLICY_HIT_BUILTIN	INFO	AppFw built-in profile invoked	"%sApplicationFirewallprofileinvoked"
APPFW	APPFW_MAX_UPLOADS	INFO	File uploads exceed the allowed number	"%sNumberoffileuploadsisovertheemaximumallowedlimitof%d"
APPFW	APPFW_SIGNATURE_MATCH	INFO	AppFw signature violation	"%sSignatureviolationruleID%u:%s"
APPFW	AF_BIND_TO_PROFILE	INFO	AppFw rule bound to HTML profile	"Profile:%s
APPFW	AF_BIND_XML_TO_PROFILE	INFO	AppFw rule bound to XML profile	"Profile:%s
APPFW	AF_ADD_FIELDTYPE	INFO	Add an AppFw Field Type	"FieldType:%s
APPFW	AF_ADD_PROFILE	INFO	Add an AppFw profile	"Profile:%s\n"
APPFW	AF_RM_FIELDTYPE	INFO	Remove an Appfw Field Type	"FieldType:%s
APPFW	AF_RM_PROFILE	INFO	Remove an AppFw profile	"Profile:%s\n"
APPFW	AF_ADD_CFFIELD	INFO	Add a confidential field	"FieldName:%s
APPF	AF_RM_CFFIELD	INFO	Remove a	"FieldName:%s

W			confidential field	
APPFW	AF_400_RESP	INFO	AppFw Request error. Generated 400 Response	"%sUnabletoparseheaders"
APPFW	AF_MEMORY_ERR	WARNING	Memory allocation request for %lu bytes failed	"Contentlengthistoolarge(%ldBytes).MemoryAllocationfailed.<Resettheconnection.>"
APPFW	AF_MALFORMED_REQ_ERR	INFO	Malformed request	"Malformedrequestreceived-connectionreset");
APPFW	AF_UTHREAD_STACK_ERR	ERROR	Appsecure uthread at 0x%x had a stack error	"Uthreadstackpointeroverflowed:");
APPFW	AF_SIGNATURE_ERR	INFO	Signature error	"Signatureid%ucontainsnofastmatchpattern"
APPFW	APPFW_XML_ATTACHMENT_FOUND	WARNING	Attachment Found in the XML Message.	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW	APPFW_XML_ATTACHMENT_ERR_CALLBACK_NULL	WARNING	XML Attachment CallBack is NULL but HTTP message is MIME Attachment message.	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW	APPFW_XML_ATTACHMENT_ERR_INVALIDHEADER	WARNING	String %s is supposed to be MIME Header. But it is not according to the format of Mime Header HeaderName:HeaderValue	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW	APPFW_XML_ATTACHMENT_ERR_INVALID_HEADER	WARNING	HTTP Content type should be 'application/xop+xml' or '^(text|application)/([a-zA-Z]*\+xml|xml)' but we got %s.	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW	APPFW_XML_ATTACHMENT_ERR_BOUNDARY_MISMATCH	WARNING	Boundary mismatch in mime message.	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW	APPFW_XML_ERR_NO_ATTACHMENT_BOUNDARY	WARNING	The message having content-type as 'Multipart/Related' and not having a boundary is invalid.	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW	APPFW_XML_ATTACHMENT_ERR_MAX_SIZE	WARNING	XML Message has an Attachment with size greater than the Configured Max Attachment Size.	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW	APPFW_XML_ATTACHMENT_ERR_CONTENT_TYPE	WARNING	XML Message has an Attachment with Illegal Content-Type	XML_ATTACHMENT_MSG_INVALIDHEADER

APPFW	APPFW_XML_DDOS_ERR_MSG_SEND_FAIL	WARNING	AppFw XML DDoS Send Fail Error.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_CHAR_DATA_LENGTH	WARNING	Exceeds max character data length.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_DTD	WARNING	DTD present in the XML message.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_EXT_ENTITY	WARNING	External entities present in the XML message.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX	WARNING	AppFw XML DoS Maximum Error	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX_ATTRIBUTES	WARNING	Element '%s' exceeds maximum attributes per element.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX_ATTRIBUTE_NAME_LENGTH	WARNING	In element '%s' an attribute exceeds maximum name length.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX_ATTRIBUTE_VALUE_LENGTH	WARNING	In element '%s' attribute '%s' exceeds maximum attribute value length.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX_ELEMENTS	WARNING	Element '%s' exceeds maximum elements per message.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX_ELEMENT_CHILDREN	WARNING	Parent of element '%s' exceeds maximum children at element '%s'.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX_ELEMENT_DEPTH	WARNING	Element '%s' exceeds maximum element depth.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX_ELEMENT_NAME_LENGTH	WARNING	Element '%s' exceeds maximum element name length.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX_FILE_SIZE	WARNING	Message size exceeds max size.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX_NODES	WARNING	Node '%s' exceeds maximum nodes per message.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MIN_FILE_SIZE	WARNING	Message size less than min size.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_ERR_NOT_WELLFORMED	WARNING	Message is not a well-formed XML.	XML_MSG_NOT_WELLFORMED
APPFW	APPFW_XML_DOS_ERR_PI	WARNING	Processing instructions present in the XML	XML_DOS_MSG_MAX_ELEMENT_DEPTH

			message.	
APPFW	APPFW_XML_DOS_ERR_MAX_NAMESPACES	WARNING	Element '%s' exceeds maximum active namespaces.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX_NAMESPACEURI_LENGTH	WARNING	In element '%s' a namespace exceeds maximum uri length.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX_ENTITY_EXPANSION_DEPTH	WARNING	Exceeds max entity expansion depth	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX_ENTITY_EXPANSIONS	WARNING	Exceeds max number of entity expansions	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX_SOAPARRAY_SIZE	WARNING	Exceeds max total SOAP array size	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_DOS_ERR_MAX_SOAPARRAY_RANK	WARNING	Exceeds max SOAP array rank	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_ERR_CUSTOM	WARNING	AppFw XML internal error	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_DDOS_CONNECT_TO_SERVER_FAILED	WARNING	AppFw XML DDoS Connect to Server Failed.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_ERR_DDOS_INTERATION_SOCKET_OPEN_FAIL	WARNING	AppFw XML DDoS Interaction socket open Failed.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_ERR_DDOS_INVALID_CONFIG_FILE	WARNING	AppFw XML DDoS Invalid Config File.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_ERR_DDOS_NO_FOLDER_INSTALLATION_PATH	WARNING	AppFw XML DDoS No Folder Installation Path.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_ERR_DDOS_OPEN_CONFIG_FILE_FAIL	WARNING	AppFw XML DDoS Failure to Open Config File.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_ERR_DOS_TRIGGERED	WARNING	Denial of Service Error.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW	APPFW_XML_ERR_ENV_NOT_SET	WARNING	Environment variable QTHOME not set.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_HASH_INSERT	WARNING	Problems inserting a namespace into the hash table.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_HASH_LOOKUP	WARNING	Problems getting the key of a namespace from the hash table.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_INITIALIZING_TOKENIZER	WARNING	Unable to initialize XML tokenizer.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_INVALID_FILE	WARNING	Unable to open the file.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_INVALID_STATE	WARNING	AppFw XML Internal State Invalid.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_INVALID_XPATH	WARNING	Invalid XPath.	"%sXMLSecurity:%s%s%s"

APPFW	APPFW_XML_ERR_LOW_MEMORY	WARNING	AppFw XML Low memory.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_CHARDATA_LIMIT_EXCEEDED	WARNING	AppFw XML character data size exceeds the limit of 30MB	XML_GENERIC_ERR_MSG_EMPTYBODY_REQ_CODE);total=snprintf(logmsg
APPFW	APPFW_XML_ERR_MALFORMED_ADDRESS	WARNING	Malformed address	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_NO_DIME	WARNING	NS-XML APPFW supports SwA and MTOM SOAP attachments, but attachment with this message is DIME.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_OPERATION_CALLBACK	WARNING	Problems registering callbacks for operations.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_PREFIX_LENGTH_EXCEEDED	WARNING	Prefix length %d exceeded, encountered length is %d.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_READ_FAILED	WARNING	AppFw XML Read Failure	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_STREAM_POP	WARNING	Problems during pop of the node out of the XML stream.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_STREAM_PUSH	WARNING	Problems during push of the node into the XML stream.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_UNSUPPORTED_PORT	WARNING	Port in address %s is greater than 65535.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_UNSUPPORTED_PROTOCOL	WARNING	Unsupported protocol	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_VALIDATION_FAILED	WARNING	AppFw XML Validation Failed	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_PACKET_PROCESSING_ERR_CONTEXT_NULL	WARNING	AppFw XML Context is NULL.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_PACKET_PROCESSING_ERR_CONTEXT_STATE_NULL	WARNING	Context user state is NULL; internal error.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_PACKET_PROCESSING_ERR_MESSAGE_CONFIG_NULL	WARNING	Message config struct is NULL.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATION_ERR_ABSTRACT_ELEMENT	WARNING	Cannot instantiate abstract element	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_ERR_ABSTRACT_TYPE	WARNING	Cannot instantiate abstract type '%s', for element '%s'.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_ERR_ADDHEADERS	WARNING	Additional soap header %s present	XML_VALIDATOR_MSG_LOAD_FAILED

			in soap message.	
APPFW	APPFW_XML_VALIDATION_ERR_ATTRIBUTE_MAX_OCCURS	WARNING	Attribute '%s' appears more than once in element '%s'.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_ERR_ATTRIBUTE_MIN_OCCURS	WARNING	Required attribute missing in element	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_ERR_COMPILED_WSDL	WARNING	Compiled WSDL file is corrupt.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_ERR_CONTENT_MODEL_VIOLATED	WARNING	Content model of element '%s' not satisfied.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_ERR_CORRUPT_COMPILED_WSDL	WARNING	Compiled WSDL file is corrupt.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATION_ERR_CORRUPT_SCHEMA	WARNING	Error compiling the schema	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATION_ERR_DATATYPE_ENGINE_INIT	WARNING	Initialization of the datatype engine failed.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATION_ERR_INTERNAL	WARNING	Internal corruption of WSDL in-memory structure.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATION_ERR_INVALID_ATTRIBUTE	WARNING	Attribute '%s' is invalid.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_ERR_INVALID_COMBINATION	WARNING	Invalid configuration for soap validation.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATION_ERR_INVALID_COMPILED_WSDL	WARNING	Not able to open compiled WSDL.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATION_ERR_INVALID_CONTENT_MODEL	WARNING	Element '%s' has invalid content model.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_ERR_INVALID_DATATYPE	WARNING	Data type is invalid.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_ERR_INVALID_ELEMENT	WARNING	Invalid element.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_ERR_INVALID_FILE	WARNING	Not able to open the file.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATION_ERR_INVALID_TYPE_SUBSTITUTION	WARNING	Did not get expected type for element '%s', got '%s'.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_ERR_LOADING	WARNING	Unable to load validation engine.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATION_ERR_MAX	WARNING	AppFw XML Validation Max Error.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATION_ERR_NOSERVICEURL	WARNING	Service Url is not present or NULL.	XML_VALIDATOR_MSG_LOAD_FAILED
APPF	APPFW_XML_VALIDATION_	WARNING	Feature not	XML_VALIDATOR_MSG_LOAD

W	ERR_NOT_SUPPORTED		supported.	_FAILED
APPFW	APPFW_XML_VALIDATION_ERR_SOAP_BODY	WARNING	Soap Body structure check failed.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATION_ERR_SOAP_ENVELOPE	WARNING	Soap Envelope structure check failed.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATION_ERR_SOAP_HEADER	WARNING	Soap Header structure check failed.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATION_ERR_UNBOUNDED_PREFIX	WARNING	Prefix '%s' is unbounded.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_LOAD_ERR_CONTENTS_CANNOT_BE_NIL	WARNING	Element '%s' cannot be nil.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_LOAD_ERR_NIL_WITH_CONTENTS	WARNING	Element '%s' is nil, cannot have contents.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_ERR_REX_STACK_OVERFLOW	WARNING	Level of recursion more than maximum allowed depth.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATION_ERR_REX_STACK_EMPTY	WARNING	Trying to pop from an empty stack.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATION_ERR_SOAPBODY_EMPTY	WARNING	Both SOAP Body and SOAP Header are empty in the SOAP request.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_GENERIC_ERR_EMPTYBODY_REQ	WARNING	Request body is empty in the XML request.	XML_GENERIC_ERR_MSG_EMPTYBODY_REQ_CODE);total=snprintf(logmsg
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_ELEMENT_INVALID_DATATYPE_VALUE	WARNING	Value should be of type '%s'.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_ELEMENT_INVALID_LOCATION	WARNING	Element '%s' cannot appears at this location.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_FACET_MISMATCH	WARNING	Facet mismatch.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_FAILED	WARNING	AppFw XML Validator Load Failed.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_INVALID_ATTRIBUTE_VALUE	WARNING	Attribute '%s' has invalid value '%s'.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_INVALID_DATATYPE	WARNING	Invalid schema datatype.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_INVALID_SCHEMA_NODE_TYPE	WARNING	Invalid schema node type.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_INVALID_VALU	WARNING	Value '%s' does not match FIXED	"%sXMLSecurity:%s%s%s"

	E_FOR_FIXED		constraint '%s'.	
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_LIST_LENGTH_GT_MAX	WARNING	List length is greater than max allowed.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_LIST_LENGTH_INVALID	WARNING	List length is invalid.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_LIST_LENGTH_LT_MIN	WARNING	List length is lesser than min allowed.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_MAX	WARNING	AppFw XML Validation Maximum Load Error.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_REQUIRED_ATTRIBUTE	WARNING	Missing require attribute '%s' in element '%s'.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_SCHEMA_COMPILATION	WARNING	Error code in the compiled Schema is being ignored.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_VALIDATOR_LOAD_ERR_WSDL_COMPILATION	WARNING	Error code in the compiled WSDL is being ignored.	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_WSI_ERR_ACCELEMENTNAMESPACED	WARNING	R2735: A MESSAGE described with an rpc-literal binding MUST place the part accessor elements for parameters and return value in no namespace. Element '%s' must be unqualified.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_ARRAYTYPE	WARNING	R2113: A MESSAGE containing serialized arrays MUST NOT include the soapenc:arrayType attribute. Element '%s' must not include the soapenc:arrayType attribute.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_BAD_ENV_NAMESPACE	WARNING	R1015: A RECEIVER MUST generate a fault if they encounter a message whose document element has a local name of "Envelope" but a namespace name that is not	XML_WSI_MSG_BODY_ENV_NAMESPACE

			"http://schemas.xmlsoap.org/soap/envelope/" or "http://www.w3.org/2003/05/soap-envelope". We got namespace '%s' in SOAP Request.	
APPFW	APPFW_XML_WSI_ERR_BINDINGFAULTRESP	WARNING	R2740: The response envelope contained soap:Fault element(s), but they were not defined in the WSDL description. Element '%s' should be defined as soap:fault in WSDL description.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_BODY_CHILD_NAMESPACE	WARNING	R1014: The children of the soap:Body element in a MESSAGE MUST be namespace qualified. Unqualified children of soap:Body is '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_BODY_ENV_NAMESPACE	WARNING	BP1201: The envelope does not use SOAP 1.1 or SOAP 1.2, i.e. does not have a document element named "Envelope" or a namespace value of http://schemas.xmlsoap.org/soap/envelope/ or http://www.w3.org/2003/05/soap-envelope. We got namespace '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_CHILDAFTERBODY	WARNING	R1011: A MESSAGE MUST NOT have any element children of soap:Envelope following the soap:Body element. Element '%s' should not appear after 'soap:Body' element.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPF	APPFW_XML_WSI_ERR_CL	WARNING	R0007: A SENDER	XML_WSI_MSG_BODY_ENV_N

W	AIM_MUSTUNDERSTAND		MUST NOT use the soap:mustUnderstand attribute when sending a SOAP header block containing a conformance claim. soap:mustUnderstand attribute is present on element '%s'.	AMESPACE
APPFW	APPFW_XML_WSI_ERR_CTXT_NULL	WARNING	AppFw XML WSI Internal Context NULL	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_DOCTYPEALLOWED	WARNING	R1008: A MESSAGE MUST NOT contain a Document Type Declaration. DOCTYPE name is '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_DOT_NOTATION	WARNING	R1031: When a MESSAGE contains a faultcode element the content of that element SHOULD NOT use of the SOAP 1.1 "dot" notation to refine the meaning of the Fault. Data '%s' should not contain 'DOT'(.) in it.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_ENCODINGSTYLE	WARNING	R1005: A MESSAGE MUST NOT contain soap:encodingStyle attribute on any of the elements whose namespace is the same as the namespace of the qualified document element 'Envelope'. 'soap:encodingStyle' attribute should not be present on element '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_ENCODINGSTYLECHILD	WARNING	R1006: A MESSAGE MUST NOT contain soap:encodingStyle attributes on any element that is a child of soap:Body. 'soap:encodingStyle'	XML_WSI_MSG_BODY_ENV_NAMESPACE

			attribute should not be present on immidiate child '%s' of soap:Body.	
APPFW	APPFW_XML_WSI_ERR_ENCODINGSTYLEGRANDCHILD	WARNING	R1007: A MESSAGE described in an rpc-literal binding MUST NOT contain soap:encodingStyle attribute on any elements are grandchildren of soap:Body. 'soap:encodingStyle' attribute should not be present on grandchild '%s' of soap:Body.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_ENVELEMENTSNOATTRIBUTES	WARNING	R1032: The soap:Envelope, soap:Header, and soap:Body elements in an ENVELOPE MUST NOT have attributes in the same namespace as that of the qualified document element 'Envelope'. Attribute '%s' should not be in the same namespace as that of the qualified document element 'Envelope'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_ENVNONAMESPACE	WARNING	R1033: An ENVELOPE SHOULD NOT contain the namespace declaration xmlns:xml="http://www.w3.org/XML/1998/namespace".	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_GOODRESPONSE200	WARNING	R1111: An INSTANCE SHOULD use a "200 OK" HTTP status code for responses that contain a SOAP message that is not a SOAP fault. We should not get 'soap:Fault' element	XML_WSI_MSG_BODY_ENV_NAMESPACE

			when HTTP response code is '200 OK'.	
APPFW	APPFW_XML_WSI_ERR_HEADER_HAS_WSICLAIM	WARNING	R0005: A MESSAGE's conformance claims MUST be carried as SOAP header blocks. Element '%s' should be immidiate children of soap:Header.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_HTTP	WARNING	AppFw XML WSI HTTP Error	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_ISHTTPPOST	WARNING	R1132: A HTTP request MESSAGE MUST use the HTTP POST method. We got '%s' HTTP method.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_ISUTF8OR16	WARNING	R1012: A MESSAGE MUST be serialized as either UTF-8 or UTF-16. We got encoding '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_MSGHASALLHEADERS	WARNING	R2738: A MESSAGE MUST include all soapbind:headers specified on a wsdl:input or wsdl:output of a wsdl:operation of a wsdl:binding that describes it.Wsdl header %s is not present in soap message.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_MUSTUNDERSTAND	WARNING	R1013: A MESSAGE containing a soap:mustUnderstand attribute MUST only use the lexical forms "0" and "1". Value of 'soap:mustUnderstand' attribute is '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_NODEPLOYED	WARNING	Resource id of deployment is NULL.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_NOENVELOPEWSDLMATCH	WARNING	BP1701: The envelope does not	XML_WSI_MSG_BODY_ENV_NAMESPACE

			conform to the SOAP schema located at 'http://schemas.xmlsoap.org/soap/envelope/' or 'http://www.w3.org/2003/05/soap-envelope'.	
APPFW	APPFW_XML_WSI_ERR_NONPOSTREQUEST	WARNING	R1114: An INSTANCE SHOULD use a "405 Method not Allowed" HTTP status code if the request method was not "POST". We got '%d' HTTP status code.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_NONXMLREQUEST	WARNING	R1115: An INSTANCE SHOULD use a "415 Unsupported Media Type" HTTP status code if a HTTP request message's Content-Type header field-value is not permitted by its WSDL description. we got '%d' HTTP status code.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_NOPORTURL	WARNING	Port URL is NULL.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_NOREQWSDLMATCH	WARNING	BP1011: The content of the request envelope does not match the wsdl:message definition.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_NORESPWSDLMATCH	WARNING	BP1013 The content of the response envelope does not match the wsdl:message definition.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_NOWSDLDEPLOYED	WARNING	Deployed resource is not WSDL.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_ONEWAYRESPONSE	WARNING	R2714: For one-way operations, an INSTANCE MUST NOT return a HTTP response that contains a SOAP envelope.	XML_WSI_MSG_BODY_ENV_NAMESPACE

			Specifically, the HTTP response entity-body must be empty. we got the element soap:Envelope.	
APPFW	APPFW_XML_WSI_ERR_RESPONSESTATUS200OR202	WARNING	R1112: An INSTANCE SHOULD use either a "200 OK" or "202 Accepted" HTTP status code for a response that does do not contain a SOAP message but indicates successful HTTP outcome of a request. We got '%d' HTTP response code.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_RESPONSEWRAPPED	WARNING	R2729: A MESSAGE described with an rpc-literal binding that is a response message MUST have a wrapper element whose name is the corresponding wsdl:operation name suffixed with the string "Response". Element name should be '%sResponse' but got '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_SOAPACTIONHEADERMATCH	WARNING	R2744: A HTTP request MESSAGE MUST contain a SOAPAction HTTP header field with a quoted value equal to the value of the soapAction attribute of soapbind:operation, if present in the corresponding WSDL description. Expected '%s' soapAction but got '%s' soapAction in HTTP header.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPF	APPFW_XML_WSI_ERR_SO	WARNING	R1109: The value of	XML_WSI_MSG_BODY_ENV_N

W	APACTIONQUOTED		the SOAPAction HTTP header field in a HTTP request MESSAGE MUST be a quoted string. We got '%s' SOAPAction HTTP header.	AMESPACE
APPFW	APPFW_XML_WSI_ERR_SOAPFAULTALLOWEDCHILD	WARNING	R1000: When a MESSAGE contains a soap:Fault element, that element MUST NOT have element children other than faultcode, faultstring, faultactor and detail. Element '%s' is not a allowed child of 'soap:Fault'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_SOAPFAULTCHILDQ	WARNING	R1001: When a MESSAGE contains a soap:Fault element its element children MUST be unqualified. 'soap:Fault' child '%s' should be unqualified.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_SOAPFAULTINHTTP	WARNING	R1126: An INSTANCE MUST use a "500 Internal Server Error" HTTP status code if the response message is a SOAP Fault. We got '%s' HTTP response code.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_SOAPFAULTNONENV	WARNING	R1003: A RECEIVER MUST accept fault messages that have any number of qualified or unqualified attributes, including zero, appearing on the detail element. The namespace of qualified attributes can be anything other than the namespace of the qualified document element 'Envelope'.	XML_WSI_MSG_BODY_ENV_NAMESPACE

			Namespace of attribute '%s' should not be the same as that of the qualified document element 'Envelope'.	
APPFW	APPFW_XML_WSI_ERR_SOAPGOODXML10	WARNING	BP1601: The soap:Envelope or soap:Body does not conform to XML 1.0. Error is '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_STDFAULTCODE	WARNING	R1004: When a MESSAGE contains a faultcode element the content of that element SHOULD be one of the fault codes defined in SOAP 1.1 or a namespace qualified fault code. 'faultcode' '%s' is not defined in SOAP 1.1 or it is not namespace qualified.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_USEHTTP10OR11	WARNING	R1141: A MESSAGE MUST be sent using either HTTP/1.1 or HTTP/1.0. We got HTTP version '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_USEHTTP11	WARNING	R1140: A MESSAGE SHOULD be sent using HTTP/1.1. We got HTTP version '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_WSICLAIMSWELLFORMED	WARNING	R0004: A MESSAGE MAY contain conformance claims, as specified in the conformance claim schema. Either 'conformsTo' attribute is absent or 'soap:mustUnderstand' attribute is present on element '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_WSI_ERR_WSI_LIST_NULL	WARNING	AppFw XML WSI List Null.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPF	APPFW_XML_WSI_ERR_XM	WARNING	R1009: A	XML_WSI_MSG_BODY_ENV_N

W	LPI		MESSAGE MUST NOT contain Processing Instructions. Name of Processing Instruction is '%s'.	AMESPACE
APPFW	APPFW_XML_WSI_ERR_XSINIL	WARNING	R2211: A MESSAGE described with an rpc-literal binding MUST NOT have the xsi:nil attribute with a value of "1" or "true" on the part accessors. Element '%s' must not have the xsi:nil attribute.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW	APPFW_XML_XSD_COMPILE_INIT_ERR	WARNING	Error during initialization	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_XSD_COMPILE_LOADXSD_ERR	WARNING	AppFw XML XSDLOAD Failed during Compile	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_XSD_COMPILE_NOMODEL_ERR	WARNING	No XSModel to print	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_XSD_COMPILE_PARSE_ERR	INFO	Error during parsing	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_XSD_COMPILE_UNEXPECTED_ERR	WARNING	Unexpected exception during parsing	"%sXMLSecurity:%s%s%s"
APPFW	APPFW_XML_ERR_SOAP_FAULT	WARNING	Message contains SOAP Fault.	XML_MSG_SOAP_FAULT);total =snprintf(logmsg
APPFW	APPFW_XML_SOAP_FAULT_CONTENTS	WARNING	Dumps the SOAP Fault contents to Audit log.	XML_MSG_SOAP_FAULT);total =snprintf(logmsg
TCP	CONN_DELINK	INFO	When a server side and a client side TCP connection is delinked.These are the connections which are being tracked by netscaler like HTTP	"Source%s:%d-Vserver%s:%d-NatIP%s:%d-""Destination%s:%d-DelinkTime%s-Total_bytes_send%llu-""Total_bytes_recv%llu"
TCP	CONN_TERMINATE	INFO	When a TCP connection terminates.The logged data indicates the number of bytes transmitted and received over the connection and lso the connection start and end time	"Source%s:%d-Destination%s:%d-""StartTime%s-EndTime%s-Total_bytes_send%llu-""Total_bytes_recv%llu"

TCP	OTHERCONN_DELINK	INFO	When a server side and a client side TCP connection is delinked.These are the connections which are not being tracked by netscaler like FTP,telnet etc	"Source%s:%d-Vserver%s:%d-NatIP%s:%d-""Destination%s:%d-DelinkTime%s""Total_bytes_send%u-Total_bytes_recv%u"
TCP	NAT_CONN_DELINK	INFO	When a server side and a client side TCP connection for RNAT are delinked we need to log the connection information	"Source%s:%d-Destination%s:%d-NatIP%s:%d-""Destination%s:%d-DelinkTime%s-Total_bytes_send%llu-""Total_bytes_recv%llu"
TCP	NAT_OTHERCONN_DELINK	INFO	When a server side and a client side TCP connection for RNAT are delinked we need to log the connection information	"Source%s:%d-Destination%s:%d-NatIP%s:%d-""Destination%s:%d-DelinkTime%s-Total_bytes_send%llu-""Total_bytes_recv%llu"
ROUTING	ZEBOS_CMD_EXECUTED	INFO	The ZebOS command executed.	"%s"
SNMP	TRAP_SENT	INFO	Trap Sent Information	"%s"
SNMP	TRAP_DROPPED	INFO	Trap Dropped information. Traps are dropped due to rate-limiting	"%s"
ACL	ACL_PKT_LOG	INFO	ACL Packet Log	"Source%s-->Destination%s-""ProtocolICMP-""Type%d-Code%d-""TimeStamp%d(ms)-Hitcount%d-HitRule%s-Data"
TRANSFORM	FILE_REQUEST	DEBUG	URL Transformation profile invoked	"Client%s-Profile%s-%sinto%s"
TRANSFORM	REQ_PARSE_ERROR	WARNING	URL Transformation parsing error	"Client%s-Profile%s-FailedtoparserequestURL%stransformation-URL%s"
TRANSFORM	REQ_HEADER	DEBUG	URL Transformation in a request header	"Client%s-Profile%s-Header%s-%sinto%s"
TRANSFORM	RESP_HEADER	DEBUG	URL Transformation in a response header	"Client%s-Profile%s-Header%s-%sinto%s"
TRANSFORM	BODY_FRAG	DEBUG	URL Transformation in a response body	"Client%s-Profile%s-Type%s-%sinto%s"
TRANSFORM	ACTION_MATCH	DEBUG	URL Transformation action matched URL	"Client%s-Profile%s-Action%s-%sinto%s"
TRANSFORM	ACTION_MISMATCH	DEBUG	URL Transformation action didn't match URL	"Client%s-Profile%s-Action%s-Value%s"
TRANSFORM	PCRE_ERROR	WARNING	URL Transformation regex error	"Client%s-Profile%s-Action%s-PCREerrorcode%d"

TRANSFORM	REQ_WRITE_ERROR	WARNING	URL Transformation error in a request header	"Client%s-Profile%s-Failedtowrite%srequestheader"
APPFW_RESP	APPFW_XML_XSS	WARNING	AppFw XSS violation in XML	"%sCross-sitescriptcheckfailedfor%s%s=\"%s\""
APPFW_RESP	APPFW_XML_SQL	WARNING	AppFw SQL Injection violation in XML	"%s%sKeywordcheckfailedfor%s%s=\"%s\""
APPFW_RESP	APPFW_XML_ATTACHMENT_FOUND	WARNING	Attachment Found in the XML Message.	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW_RESP	APPFW_XML_ATTACHMENT_ERR_CALLBACK_NULL	WARNING	XML Attachment CallBack is NULL but HTTP message is MIME Attachment message.	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW_RESP	APPFW_XML_ATTACHMENT_ERR_INVALIDHEADER	WARNING	String %s is supposed to be MIME Header. But it is not according to the format of Mime Header HeaderName:HeaderValue	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW_RESP	APPFW_XML_ATTACHMENT_ERR_INVALID_HEADER	WARNING	HTTP Content type should be 'application/xop+xml' or '^(text|application)/([a-zA-Z]*\+xml|xml)' but we got %s.	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW_RESP	APPFW_XML_ATTACHMENT_ERR_BOUNDARY_MISMATCH	WARNING	Boundary mismatch in mime message.	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW_RESP	APPFW_XML_ERR_NO_ATTACHMENT_BOUNDARY	WARNING	The message having content-type as 'Multipart/Related' and not having a boundary is invalid.	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW_RESP	APPFW_XML_ATTACHMENT_ERR_MAX_SIZE	WARNING	XML Message has an Attachment with size greater than the Configured Max Attachment Size.	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW_RESP	APPFW_XML_ATTACHMENT_ERR_CONTENT_TYPE	WARNING	XML Message has an Attachment with Illegal Content-Type	XML_ATTACHMENT_MSG_INVALIDHEADER
APPFW_RESP	APPFW_XML_DDOS_ERR_MSG_SEND_FAIL	WARNING	AppFw XML DDoS Send Fail Error.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPF	APPFW_XML_DOS_ERR_C	WARNING	Exceeds max	XML_DOS_MSG_MAX_ELEME

W_RESP	HAR_DATA_LENGTH		character data length.	NT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_DTD	WARNING	DTD present in the XML message.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_EXT_ENTITY	WARNING	External entities present in the XML message.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX	WARNING	AppFw XML DoS Maximum Error	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_ATTRIBUTES	WARNING	Element '%s' exceeds maximum attributes per element.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_ATTRIBUTE_NAME_LENGTH	WARNING	In element '%s' an attribute exceeds maximum name length.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_ATTRIBUTE_VALUE_LENGTH	WARNING	In element '%s' attribute '%s' exceeds maximum attribute value length.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_ELEMENTS	WARNING	Element '%s' exceeds maximum elements per message.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_ELEMENT_CHILDREN	WARNING	Parent of element '%s' exceeds maximum children at element '%s'.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_ELEMENT_DEPTH	WARNING	Element '%s' exceeds maximum element depth.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_ELEMENT_NAME_LENGTH	WARNING	Element '%s' exceeds maximum element name length.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_FILE_SIZE	WARNING	Message size exceeds max size.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_NODES	WARNING	Node '%s' exceeds maximum nodes per message.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MIN_FILE_SIZE	WARNING	Message size less than min size.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_ERR_NOT_WELLFORMED	WARNING	Message is not a well-formed XML.	XML_MSG_NOT_WELLFORMED
APPFW_RE	APPFW_XML_DOS_ERR_PI	WARNING	Processing instructions present	XML_DOS_MSG_MAX_ELEMENT_DEPTH

SP			in the XML message.	
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_NAMESPACES	WARNING	Element '%s' exceeds maximum active namespaces.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_NAMESPACEURI_LENGTH	WARNING	In element '%s' a namespace exceeds maximum uri length.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_ENTITY_EXPANSION_DEPTH	WARNING	Exceeds max entity expansion depth	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_ENTITY_EXPANSIONS	WARNING	Exceeds max number of entity expansions	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_SOAPARRAY_SIZE	WARNING	Exceeds max total SOAP array size	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_DOS_ERR_MAX_SOAPARRAY_RANK	WARNING	Exceeds max SOAP array rank	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_ERR_CUSTOM	WARNING	AppFw XML internal error	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_DDOS_CONNECT_TO_SERVER_FAILED	WARNING	AppFw XML DDoS Connect to Server Failed.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_ERR_DDOS_INTERATION_SOCKET_OPEN_FAIL	WARNING	AppFw XML DDoS Interaction socket open Failed.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_ERR_DDOS_INVALID_CONFIG_FILE	WARNING	AppFw XML DDoS Invalid Config File.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_ERR_DDOS_NO_FOLDER_INSTALLATION_PATH	WARNING	AppFw XML DDoS No Folder Installation Path.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_ERR_DDOS_OPEN_CONFIG_FILE_FAIL	WARNING	AppFw XML DDoS Failure to Open Config File.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_ERR_DOS_TRIGGERED	WARNING	Denial of Service Error.	XML_DOS_MSG_MAX_ELEMENT_DEPTH
APPFW_RESP	APPFW_XML_ERR_ENV_NOT_SET	WARNING	Environment variable QTHOME not set.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_HASH_INSERT	WARNING	Problems inserting a namespace into the hash table.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_HASH_LOOKUP	WARNING	Problems getting the key of a namespace from the hash table.	"%sXMLSecurity:%s%s%s"
APPFW_RE	APPFW_XML_ERR_INITIALIZING_TOKENIZER	WARNING	Unable to initialize XML tokenizer.	"%sXMLSecurity:%s%s%s"

SP				
APPFW_RESP	APPFW_XML_ERR_INVALID_FILE	WARNING	Unable to open the file.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_INVALID_STATE	WARNING	AppFw XML Internal State Invalid.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_INVALID_XPATH	WARNING	Invalid XPath.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_LOW_MEMORY	WARNING	AppFw XML Low memory.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_CHARDATA_LIMIT_EXCEEDED	WARNING	AppFw XML character data size exceeds the limit of 30MB	XML_GENERIC_ERR_MSG_EMPTYBODY_REQ_CODE);total=snprintf(logmsg
APPFW_RESP	APPFW_XML_ERR_MALFORMED_ADDRESS	WARNING	Malformed address	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_NO_DIME	WARNING	NS-XML APPFW supports SwA and MTOM SOAP attachments, but attachment with this message is DIME.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_OPERATION_CALLBACK	WARNING	Problems registering callbacks for operations.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_PREFIX_LENGTH_EXCEEDED	WARNING	Prefix length %d exceeded, encountered length is %d.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_READ_FAILED	WARNING	AppFw XML Read Failure	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_STREAM_POP	WARNING	Problems during pop of the node out of the XML stream.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_STREAM_PUSH	WARNING	Problems during push of the node into the XML stream.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_UNSUPPORTED_PORT	WARNING	Port in address %s is greater than 65535.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_UNSUPPORTED_PROTOCOL	WARNING	Unsupported protocol	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_VALIDATION_FAILED	WARNING	AppFw XML Validation Failed	XML_VALIDATOR_MSG_LOAD_FAILED
APPF	APPFW_XML_PACKET_PR	WARNING	AppFw XML Context	"%sXMLSecurity:%s%s%s"

W_RESP	OCESSING_ERR_CONTEXT_NULL		is NULL.	
APPFW_RESP	APPFW_XML_PACKET_PROCESSING_ERR_CONTEXT_STATE_NULL	WARNING	Context user state is NULL; internal error.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_PACKET_PROCESSING_ERR_MESSAGE_CONFIG_NULL	WARNING	Message config struct is NULL.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATION_ERR_ABSTRACT_ELEMENT	WARNING	Cannot instantiate abstract element	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_ABSTRACT_TYPE	WARNING	Cannot instantiate abstract type '%s', for element '%s'.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_ADDHEADERS	WARNING	Additional soap header %s present in soap message.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_ATTRIBUTE_MAX_OCCURS	WARNING	Attribute '%s' appears more than once in element '%s'.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_ATTRIBUTE_MIN_OCCURS	WARNING	Required attribute missing in element	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_COMPILED_WSDL	WARNING	Compiled WSDL file is corrupt.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_CONTENT_MODEL_VIOLATED	WARNING	Content model of element '%s' not satisfied.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_CORRUPT_COMPILED_WSDL	WARNING	Compiled WSDL file is corrupt.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATION_ERR_CORRUPT_SCHEMA	WARNING	Error compiling the schema	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATION_ERR_DATATYPE_ENGINE_INIT	WARNING	Initialization of the datatype engine failed.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATION_ERR_INTERNAL	WARNING	Internal corruption of WSDL in-memory structure.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATION_ERR_INVALID_ATTRIBUTE	WARNING	Attribute '%s' is invalid.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_INVALID_COMBINATION	WARNING	Invalid configuration for soap validation.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATION_ERR_INVALID_COMPILED_WSDL	WARNING	Not able to open compiled WSDL.	"%sXMLSecurity:%s%s%s"
APPF	APPFW_XML_VALIDATION_	WARNING	Element '%s' has	XML_VALIDATOR_MSG_LOAD

W_RESP	ERR_INVALID_CONTENT_MODEL		invalid content model.	_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_INVALID_DATATYPE	WARNING	Data type is invalid.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_INVALID_ELEMENT	WARNING	Invalid element.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_INVALID_FILE	WARNING	Not able to open the file.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATION_ERR_INVALID_TYPE_SUBSTITUTION	WARNING	Did not get expected type for element '%s', got '%s'.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_LOADING	WARNING	Unable to load validation engine.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATION_ERR_MAX	WARNING	AppFw XML Validation Max Error.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATION_ERR_NOSERVICEURL	WARNING	Service Url is not present or NULL.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_NOT_SUPPORTED	WARNING	Feature not supported.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_SOAP_BODY	WARNING	Soap Body structure check failed.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATION_ERR_SOAP_ENVELOPE	WARNING	Soap Envelope structure check failed.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATION_ERR_SOAP_HEADER	WARNING	Soap Header structure check failed.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATION_ERR_UNBOUNDED_PREFIX	WARNING	Prefix '%s' is unbounded.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_LOAD_ERR_CONTENTS_CANNOT_BE_NIL	WARNING	Element '%s' cannot be nil.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_LOAD_ERR_NIL_WITH_CONTENTS	WARNING	Element '%s' is nil, cannot have contents.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_REX_STACK_OVERFLOW	WARNING	Level of recursion more than maximum allowed depth.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATION_ERR_REX_STACK_EMPTY	WARNING	Trying to pop from an empty stack.	"%sXMLSecurity:%s%s%s"
APPFW_RE	APPFW_XML_VALIDATION_ERR_SOAPBODY_EMPTY	WARNING	Both SOAP Body and SOAP Header	XML_VALIDATOR_MSG_LOAD_FAILED

SP			are empty in the SOAP request.	
APPFW_RESP	APPFW_XML_GENERIC_ERR_EMPTYBODY_REQ	WARNING	Request body is empty in the XML request.	XML_GENERIC_ERR_MSG_EMPTYBODY_REQ_CODE);total=snprintf(logmsg
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_ELEMENT_INVALID_DATATYPE_VALUE	WARNING	Value should be of type '%s'.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_ELEMENT_INVALID_LOCATION	WARNING	Element '%s' cannot appears at this location.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_FACET_MISMATCH	WARNING	Facet mismatch.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_FAILED	WARNING	AppFw XML Validator Load Failed.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_INVALID_ATTRIBUTE_VALUE	WARNING	Attribute '%s' has invalid value '%s'.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_INVALID_DATATYPE	WARNING	Invalid schema datatype.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_INVALID_SCHEMA_NODE_TYPE	WARNING	Invalid schema node type.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_INVALID_VALUE_FOR_FIXED	WARNING	Value '%s' does not match FIXED constraint '%s'.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_LIST_LENGTH_GT_MAX	WARNING	List length is greater than max allowed.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_LIST_LENGTH_INVALID	WARNING	List length is invalid.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_LIST_LENGTH_LT_MIN	WARNING	List length is lesser than min allowed.	XML_VALIDATOR_MSG_LOAD_FAILED
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_MAX	WARNING	AppFw XML Validation Maximum Load Error.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_REQUIRED_ATTRIBUTE	WARNING	Missing require attribute '%s' in element '%s'.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_SCHEMA_COMPILATION	WARNING	Error code in the compiled Schema is being ignored.	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_VALIDATOR_LOAD_ERR_WSDL_COMPILATION	WARNING	Error code in the compiled WSDL is being ignored.	"%sXMLSecurity:%s%s%s"
APPFW_RE	APPFW_XML_WSI_ERR_ACCELEMENTNAMESPACED	WARNING	R2735: A MESSAGE	XML_WSI_MSG_BODY_ENV_NAMESPACE

SP			described with an rpc-literal binding MUST place the part accessor elements for parameters and return value in no namespace. Element '%s' must be unqualified.	
APPFW_RESP	APPFW_XML_WSI_ERR_ARRAYTYPE	WARNING	R2113: A MESSAGE containing serialized arrays MUST NOT include the soapenc:arrayType attribute. Element '%s' must not include the soapenc:arrayType attribute.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_BAD_ENV_NAMESPACE	WARNING	R1015: A RECEIVER MUST generate a fault if they encounter a message whose document element has a local name of "Envelope" but a namespace name that is not "http://schemas.xmlsoap.org/soap/envelope/" or "http://www.w3.org/2003/05/soap-envelope". We got namespace '%s' in SOAP Request.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_BINDINGFAULTRESP	WARNING	R2740: The response envelope contained soap:Fault element(s), but they were not defined in the WSDL description. Element '%s' should be defined as soap:fault in WSDL description.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_BODY_CHILD_NAMESPACE	WARNING	R1014: The children of the soap:Body element in a MESSAGE MUST be namespace	XML_WSI_MSG_BODY_ENV_NAMESPACE

			qualified. Unqualified children of soap:Body is '%s'.	
APPFW_RESP	APPFW_XML_WSI_ERR_BODY_ENV_NAMESPACE	WARNING	BP1201: The envelope does not use SOAP 1.1 or SOAP 1.2, i.e. does not have a document element named "Envelope" or a namespace value of http://schemas.xmlsoap.org/soap/envelope/ or http://www.w3.org/2003/05/soap-envelope. We got namespace '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_CHILDAFTERBODY	WARNING	R1011: A MESSAGE MUST NOT have any element children of soap:Envelope following the soap:Body element. Element '%s' should not appear after 'soap:Body' element.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_CLAIM_MUSTUNDERSTAND	WARNING	R0007: A SENDER MUST NOT use the soap:mustUnderstand attribute when sending a SOAP header block containing a conformance claim. soap:mustUnderstand attribute is present on element '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_CTXT_NULL	WARNING	AppFw XML WSI Internal Context NULL	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_DOCTYPEALLOWED	WARNING	R1008: A MESSAGE MUST NOT contain a Document Type Declaration. DOCTYPE name is '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_DOT_NOTATION	WARNING	R1031: When a MESSAGE contains a faultcode element the content of that	XML_WSI_MSG_BODY_ENV_NAMESPACE

			element SHOULD NOT use of the SOAP 1.1 "dot" notation to refine the meaning of the Fault. Data '%s' should not contain 'DOT'(.) in it.	
APPFW_RESP	APPFW_XML_WSI_ERR_ENCODINGSTYLE	WARNING	R1005: A MESSAGE MUST NOT contain soap:encodingStyle attribute on any of the elements whose namespace is the same as the namespace of the qualified document element 'Envelope'. 'soap:encodingStyle' attribute should not be present on element '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_ENCODINGSTYLECHILD	WARNING	R1006: A MESSAGE MUST NOT contain soap:encodingStyle attributes on any element that is a child of soap:Body. 'soap:encodingStyle' attribute should not be present on immidiate child '%s' of soap:Body.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_ENCODINGSTYLEGRANDCHILD	WARNING	R1007: A MESSAGE described in an rpc-literal binding MUST NOT contain soap:encodingStyle attribute on any elements are grandchildren of soap:Body. 'soap:encodingStyle' attribute should not be present on grandchild '%s' of soap:Body.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_ENVELEMENTSNOATTRIBUTES	WARNING	R1032: The soap:Envelope, soap:Header, and soap:Body elements in an ENVELOPE	XML_WSI_MSG_BODY_ENV_NAMESPACE

			MUST NOT have attributes in the same namespace as that of the qualified document element 'Envelope'. Attribute '%s' should not be in the same namespace as that of the qualified document element 'Envelope'.	
APPFW_RESP	APPFW_XML_WSI_ERR_ENVNONAMESPACE	WARNING	R1033: An ENVELOPE SHOULD NOT contain the namespace declaration xmlns:xml="http://www.w3.org/XML/1998/namespace".	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_GOODRESPONSE200	WARNING	R1111: An INSTANCE SHOULD use a "200 OK" HTTP status code for responses that contain a SOAP message that is not a SOAP fault. We should not get 'soap:Fault' element when HTTP response code is '200 OK'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_HEADER_HAS_WSICLAIM	WARNING	R0005: A MESSAGE's conformance claims MUST be carried as SOAP header blocks. Element '%s' should be immidiate children of soap:Header.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_HTTP	WARNING	AppFw XML WSI HTTP Error	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_ISHTTPPOST	WARNING	R1132: A HTTP request MESSAGE MUST use the HTTP POST method. We got '%s' HTTP method.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RE	APPFW_XML_WSI_ERR_ISUTF8OR16	WARNING	R1012: A MESSAGE MUST	XML_WSI_MSG_BODY_ENV_NAMESPACE

SP			be serialized as either UTF-8 or UTF-16. We got encoding '%s'.	
APPFW_RESP	APPFW_XML_WSI_ERR_MSGHASALLHEADERS	WARNING	R2738: A MESSAGE MUST include all soapbind:headers specified on a wsdl:input or wsdl:output of a wsdl:operation of a wsdl:binding that describes it.Wsdl header %s is not present in soap message.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_MUSTUNDERSTAND	WARNING	R1013: A MESSAGE containing a soap:mustUnderstand attribute MUST only use the lexical forms "0" and "1". Value of 'soap:mustUnderstand' attribute is '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_NODEPLOYED	WARNING	Resource id of deployment is NULL.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_NOENVELOPEWSDLMATCH	WARNING	BP1701: The envelope does not conform to the SOAP schema located at 'http://schemas.xmlsoap.org/soap/envelope/' or 'http://www.w3.org/2003/05/soap-envelope'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_NONPOSTREQUEST	WARNING	R1114: An INSTANCE SHOULD use a "405 Method not Allowed" HTTP status code if the request method was not "POST". We got '%d' HTTP status code.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_NONXMLREQUEST	WARNING	R1115: An INSTANCE SHOULD use a "415 Unsupported Media	XML_WSI_MSG_BODY_ENV_NAMESPACE

			Type" HTTP status code if a HTTP request message's Content-Type header field-value is not permitted by its WSDL description. we got '%d' HTTP status code.	
APPFW_RESP	APPFW_XML_WSI_ERR_NOPORTURL	WARNING	Port URL is NULL.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_NOREQWSDLMATCH	WARNING	BP1011: The content of the request envelope does not match the wsdl:message definition.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_NORESPWSDLMATCH	WARNING	BP1013 The content of the response envelope does not match the wsdl:message definition.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_NOWSDLDEPLOYED	WARNING	Deployed resource is not WSDL.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_ONEWAYRESPONSE	WARNING	R2714: For one-way operations, an INSTANCE MUST NOT return a HTTP response that contains a SOAP envelope. Specifically, the HTTP response entity-body must be empty. we got the element soap:Envelope.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_RESPONSESTATUS200OR202	WARNING	R1112: An INSTANCE SHOULD use either a "200 OK" or "202 Accepted" HTTP status code for a response that does do not contain a SOAP message but indicates successful HTTP outcome of a request. We got '%d' HTTP response code.	XML_WSI_MSG_BODY_ENV_NAMESPACE

APPFW_RESP	APPFW_XML_WSI_ERR_RESPONSEWRAPPED	WARNING	R2729: A MESSAGE described with an rpc-literal binding that is a response message MUST have a wrapper element whose name is the corresponding wsdl:operation name suffixed with the string "Response". Element name should be '%sResponse' but got '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_SOAPACTIONHEADERMATCH	WARNING	R2744: A HTTP request MESSAGE MUST contain a SOAPAction HTTP header field with a quoted value equal to the value of the soapAction attribute of soapbind:operation, if present in the corresponding WSDL description. Expected '%s' soapAction but got '%s' soapAction in HTTP header.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_SOAPACTIONQUOTED	WARNING	R1109: The value of the SOAPAction HTTP header field in a HTTP request MESSAGE MUST be a quoted string. We got '%s' SOAPAction HTTP header.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_SOAPFAULTALLOWEDCHILD	WARNING	R1000: When a MESSAGE contains a soap:Fault element, that element MUST NOT have element children other than faultcode, faultstring, faultactor and detail. Element '%s' is not a allowed child of 'soap:Fault'.	XML_WSI_MSG_BODY_ENV_NAMESPACE

APPFW_RESP	APPFW_XML_WSI_ERR_SOAPFAULTCHILDQ	WARNING	R1001: When a MESSAGE contains a soap:Fault element its element children MUST be unqualified. 'soap:Fault' child '%s' should be unqualified.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_SOAPFAULTINHTTP	WARNING	R1126: An INSTANCE MUST use a "500 Internal Server Error" HTTP status code if the response message is a SOAP Fault. We got '%s' HTTP response code.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_SOAPFAULTNONENV	WARNING	R1003: A RECEIVER MUST accept fault messages that have any number of qualified or unqualified attributes, including zero, appearing on the detail element. The namespace of qualified attributes can be anything other than the namespace of the qualified document element 'Envelope'. Namespace of attribute '%s' should not be the same as that of the qualified document element 'Envelope'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_SOAPGOODXML10	WARNING	BP1601: The soap:Envelope or soap:Body does not conform to XML 1.0. Error is '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_STDFAULTCODE	WARNING	R1004: When a MESSAGE contains a faultcode element the content of that element SHOULD be one of the fault codes defined in SOAP 1.1 or a namespace qualified	XML_WSI_MSG_BODY_ENV_NAMESPACE

			fault code. 'faultcode' '%s' is not defined in SOAP 1.1 or it is not namespace qualified.	
APPFW_RESP	APPFW_XML_WSI_ERR_USEHTTP10OR11	WARNING	R1141: A MESSAGE MUST be sent using either HTTP/1.1 or HTTP/1.0. We got HTTP version '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_USEHTTP11	WARNING	R1140: A MESSAGE SHOULD be sent using HTTP/1.1. We got HTTP version '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_WSICLAIMSWELLFORMED	WARNING	R0004: A MESSAGE MAY contain conformance claims, as specified in the conformance claim schema. Either 'conformsTo' attribute is absent or 'soap:mustUnderstand' attribute is present on element '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_WSI_LIST_NULL	WARNING	AppFw XML WSI List Null.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_XMLPI	WARNING	R1009: A MESSAGE MUST NOT contain Processing Instructions. Name of Processing Instruction is '%s'.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RESP	APPFW_XML_WSI_ERR_XSINIL	WARNING	R2211: A MESSAGE described with an rpc-literal binding MUST NOT have the xsi:nil attribute with a value of "1" or "true" on the part accessors. Element '%s' must not have the xsi:nil attribute.	XML_WSI_MSG_BODY_ENV_NAMESPACE
APPFW_RE	APPFW_XML_XSD_COMPILE_INIT_ERR	WARNING	Error during initialization	"%sXMLSecurity:%s%s%s"

SP				
APPFW_RESP	APPFW_XML_XSD_COMPILE_LOADXSD_ERR	WARNING	AppFw XML XSDLOAD Failed during Compile	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_XSD_COMPILE_NOMODEL_ERR	WARNING	No XSModel to print	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_XSD_COMPILE_PARSE_ERR	INFO	Error during parsing	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_XSD_COMPILE_UNEXPECTED_ERR	WARNING	Unexpected exception during parsing	"%sXMLSecurity:%s%s%s"
APPFW_RESP	APPFW_XML_ERR_SOAP_FAULT	WARNING	Message contains SOAP Fault.	XML_MSG_SOAP_FAULT);total =snprintf(logmsg
APPFW_RESP	APPFW_XML_SOAP_FAULT_CONTENTS	WARNING	Dumps the SOAP Fault contents to Audit log.	XML_MSG_SOAP_FAULT);total =snprintf(logmsg
AAATM	LOGIN	INFO	Login to AAA TM vserver succeeds	"User%s-Client_ip%s-""Nat_ip%s-Vserver%s:%d-Browser_type\"%s\"-Group(s)\"%s\""
AAATM	LOGOUT	INFO	AAA TM session logged out	"User%s-""Client_ip%s-Nat_ip%s-""Vserver%s:%d-""Start_time\"%s\"-End_time\"%s\"-Duration%s-""Http_resources_accessed%s-""Total_TCP_connections%d-""Total_policies_allowed%d-Total_policies_denied%d-""Total_bytes_send%s-Total_bytes_recv%s-""Total_compressedbytes_send%s-Total_compressedbytes_recv%s-""Compression_ratio_send%d.%02u%%-""Compression_ratio_recv%d.%02u%%-""LogoutMethod\"%s\"-Group(s)\"%s\""
AAATM	HTTPREQUEST	DEBUG	A AAA TM session receives a HTTP request	"%sUser%s:Group(s)%s:Vserver%s:%d-%s%s%s%s"
AAATM	HTTP_RESOURCEACCESS_DENIED	NOTICE	A http resource access is denied by policy engine. The denied policy name is captured in the log message.	"User%s-Vserver%s:%d-Total_bytes_send%d-Remote_host%s-""Denied_url%s-Denied_by_policy\"%s\"-Group(s)\"%s\""
ROUTING	PAL	VARIABLE		
PITBO	PITBOSS	INFO	Pitboss watch is	Adding pitboss watch on (%d)

SS			added on a process with the process id pid	
PITBOSS	PITBOSS	INFO	Pitboss watch is deleted on a process with the process id pid	Deleting watch on (%d)
PITBOSS	PB_SYSTEM_RESTART	ALERT	Process with pid has reached maximum number of restarts.Therefore the systemis being restarted	proc (%d) (%s) has had its maximum number of restarts (%d), rebooting the system
PITBOSS	PB_PROCESS_RESTART	ALERT	Process with pid is being restarted.The message indicates the number of times the process has been restarted	Restarting process old pid (%d) action (%s)
ROUTING	ROUTE_ADVERTISED	INFO	Route Advertised	ROUTE (%s %s %s) - ADVERTISED
ROUTING	ROUTE_WITHDRAWN	INFO	Route Withdrawn	ROUTE (%s %s %s) - WITHDRAWN
ROUTING	ROUTE_RELEARN		Route Relearnt	RELEARN (0x%x)
ROUTING	ROUTE_HASTATE	INFO	HA state change	HASTATE (0x%x)
CVPN	CVPN_INPUT_URL	DEBUG	The input URL before rewriting	HTML_URL %s
CVPN	CVPN_REWRITTEN_URL	DEBUG	The rewritten url	REWRITTEN_URL %.*s
CVPN	CVPN_PCRE_ERROR	DEBUG	PCRE Error	Regex %.*s : PCRE_ERROR %d
CVPN	CVPN_MATCHED_URL	DEBUG	The matched url	MATCHED_URL %.*s

Hardware Installation

2015-05-17 05:02:19 UTC

Contents

Hardware Installation

The following sections describe the hardware installation and initial configuration for all NetScaler hardware platforms.

Introduction to the Hardware Platforms	Describes the NetScaler hardware platforms and provides detailed information about each platform and its components.
Preparing for Installation	Describes how to unpack the NetScaler appliance and prepare the site and rack for installing the appliance. Lists the cautions and warnings that you should review before you install the appliance.
Installing the Hardware	Describes the steps to install the rails, mount the hardware, connect the cables, and turn on the appliance.
Initial Configuration	Describes how to perform initial configuration of your NetScaler appliance and assign management and network IP addresses.
Lights Out Management Port of the NetScaler Appliance	Describes the different operations you can perform on your NetScaler appliance by using the Lights Out Management Port.

For information about NetScaler hardware and software compatibility and the supported upgrade and downgrade paths, see http://support.citrix.com/article/CTX113357.

Introduction to the Hardware Platforms

The NetScaler hardware platforms range from the single processor MPX 5500 platform to the high-capacity, MPX 17550/19550/20550/21550 hardware platform. The various NetScaler hardware platforms are similar in that they use the same types of components, but different models provide different hardware capabilities. All NetScaler hardware platforms support the NetScaler software.

Some of the hardware platforms are available as dedicated application firewall appliances or secure application access appliances.

Introduction to the Hardware Platforms

The NetScaler hardware platforms range from the single processor MPX 5500 platform to the high-capacity, MPX 17550/19550/20550/21550 hardware platform. The various NetScaler hardware platforms are similar in that they use the same types of components, but different models provide different hardware capabilities. All NetScaler hardware platforms support the NetScaler software.

Some of the hardware platforms are available as dedicated application firewall appliances or secure application access appliances.

Common Hardware Components

Each platform has front panel and back panel hardware components. The front panel has an LCD display and an RS232 serial console port. The number, type, and location of ports—copper Ethernet, copper and fiber 1G SFP, 10G SFP+, and XFP—vary by hardware platform. The back panel provides access to the fan and the field replaceable units (power supplies, CompactFlash card, and solid-state and hard-disk drives).

LCD Display

The LCD display on the front of every appliance displays messages about the current operating status of the appliance. These messages communicate whether your appliance has started properly and is operating normally. If the appliance is not operating normally, the LCD displays troubleshooting messages.

The LCD displays real-time statistics, diagnostic information, and active alerts. The dimensions of the LCD limit the display to two lines of 16 characters each, causing the displayed information to flow through a sequence of screens. Each screen shows information about a specific function.

The LCD has a neon backlight. Normally, the backlight glows steadily. When there is an active alert, it blinks rapidly. If the alert information exceeds the LCD screen size, the backlight blinks at the beginning of each display screen. When the appliance shuts down, the backlight remains on for one minute and then automatically turns off.

There are nine types of display screens on the LCD display. The first two screens in the following list, the booting screen and the startup screen, appear when your appliance is starting up. The other screens, except the out-of-service screen, can appear while the appliance is operating. They show configuration information, alerts, HTTP information, network traffic information, CPU load information, and port information for your appliance.

Booting Screen.

The booting screen is displayed immediately after the appliance is turned on. The first line displays the hardware platform, as shown in the following figure.

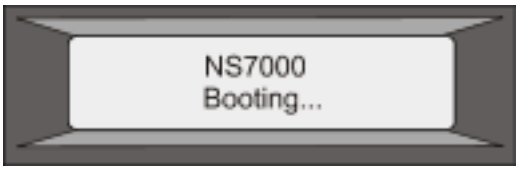


Figure 1. LCD Booting Screen

The newer MPX appliances display NSMPX followed by the platform number in the first line. For example, the MPX 7500/9500 appliances display NSMPX-7500. To view the model number, at the NetScaler command line, type show license. Scroll to the end of the command output to view the model number.

Startup Screen.

The startup screen is displayed for a few seconds after the appliance successfully begins operation. The first line displays the hardware platform, and the second line displays the software version and build number, as shown in the following figure.

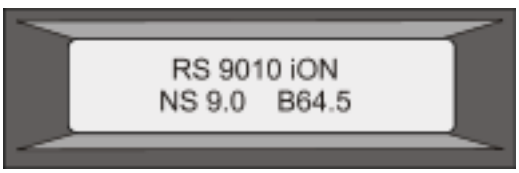


Figure 2. LCD Startup Screen

Out-of-Service Screen.

The out-of-service screen is displayed when the appliance has undergone a controlled shutdown, as shown in the following figure.

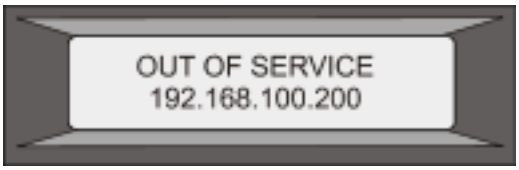


Figure 3. LCD Out-of-service Screen

Configuration Screen.

The first line displays the appliance status (STA, PRI, or SEC) and uptime. STA indicates that the appliance is in standalone mode, PRI indicates that the appliance is a primary node in a high availability (HA) pair, and SEC indicates that the appliance is a secondary node in an HA pair. Appliance uptime is displayed in HH:MM format. The second line displays the IP address of the appliance, as shown in the following figure.

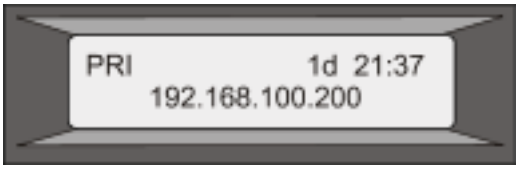


Figure 4. LCD Configuration Screen

Alert Screen.

The first line displays the appliance status (STA, PRI, or SEC). STA indicates that the appliance is in standalone mode, PRI indicates that the appliance is a primary node in a high availability (HA) pair, and SEC indicates that the appliance is a secondary node in an HA pair. The second line displays the IP address of the appliance.

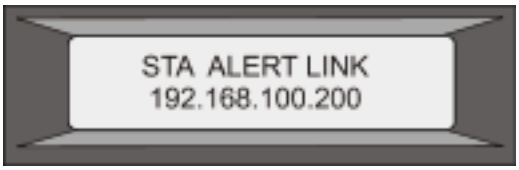


Figure 5. LCD Known Alert Screen

HTTP Statistics Screen.

The first line displays the rate of HTTP GETS per second. The second line displays the rate of HTTP POSTS per second, as shown in the following figure.

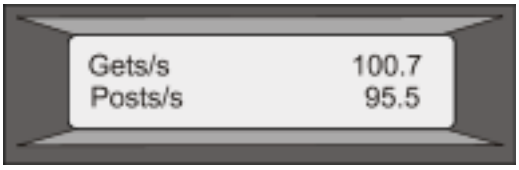


Figure 6. LCD HTTP Statistics Screen

Network Traffic Statistics Screen.

The first line displays the rate at which data is received, in megabits per second. The second line displays the rate of data transmission, in megabits per second, as shown in the following figure.

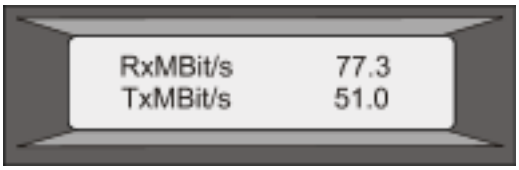


Figure 7. LCD Network Traffic Statistics Screen

CPU Load, Memory, and Connections Screen.

The first line displays CPU utilization and memory utilization as percentages. The second line displays the ratio of the number of server connections to the number of client connections.

Note: If the number of server or client connections exceeds 99,999, the number is displayed in thousands, indicated by the letter K.

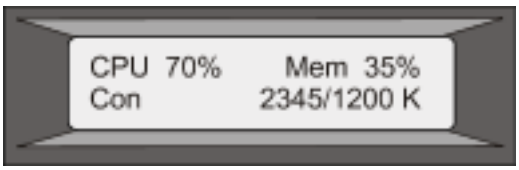


Figure 8. LCD CPU Load, Memory, and Connections Screen

Port Information Screen.

The S row displays port speed, flow control, and duplex information. The R row displays megabits received per second on the interface. The first port in each row is the management port.

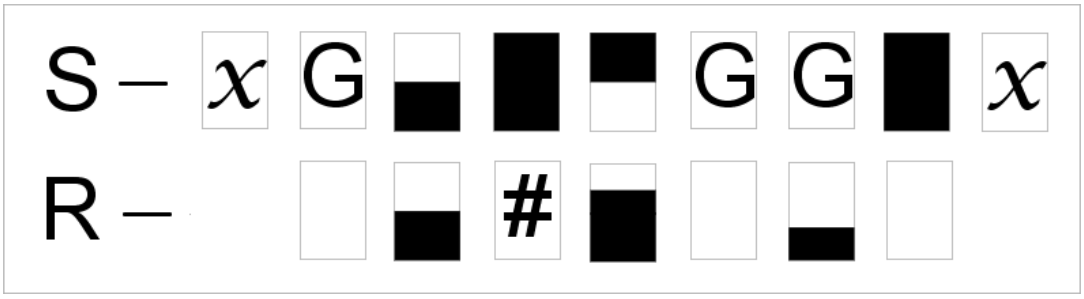


Figure 9. Port Information for an 8-port Appliance

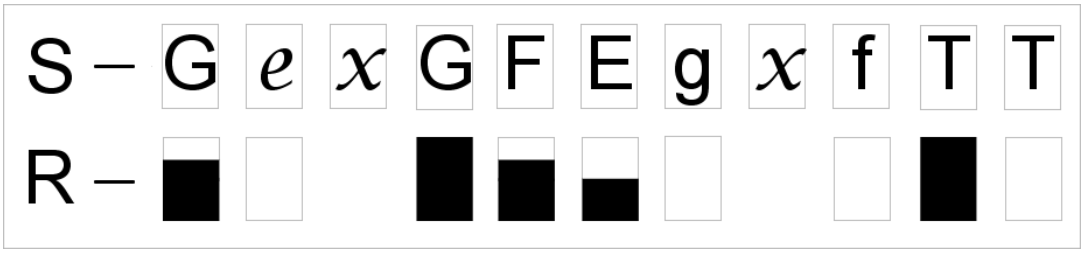


Figure 10. Port Information for a 10-port Appliance

The following table defines the various abbreviations and symbols that appear in the S row of the port information screen.

Table 1. Port Abbreviations and Symbols for S Row

S row abbreviation/symbol	Indicates
	A rate of 10 megabits per second, full duplex mode, and flow control OFF.

	A rate of 100 megabits per second, full duplex mode, and flow control OFF.
	A rate of 1 gigabit per second, full duplex mode, and flow control OFF.
	A rate of 10 gigabits per second, full duplex mode, and flow control OFF.
	A disconnected port. **Note:** The R row does not display an abbreviation or symbol for a disconnected port.
	Receive flow control regardless of speed or duplex mode.
	Transmit flow control regardless of speed or duplex mode.
	Receive and transmit flow control regardless of speed or duplex mode.
	A rate of 10 megabits per second, half duplex mode, and flow control OFF.

	A rate of 100 megabits per second, half duplex mode, and flow control OFF.
	A rate of 1 gigabit per second, half duplex mode, and flow control OFF.

The following table defines the various abbreviations and symbols that appear in the R row of the port information screen.

Table 2. Port Abbreviations and Symbols for R Row

R row abbreviation/symbol	Indicates
	The port is disabled.
	Receive speed is about 10% of line speed.
	Receive speed is about 50% of line speed.
	Receive speed is about 75% of line speed.
	Receive speed is about 100% of line speed.

Ports

Ports are used to connect the appliance to external devices. NetScaler appliances support RS232 serial ports, 10/100/1000Base-T copper Ethernet ports, 1-gigabit copper and fiber 1G SFP ports, and 10-gigabit fiber SFP+ ports. All NetScaler appliances have a combination of some or all of these ports. For details on the type and number of ports available on your appliance, see the section describing that platform.

RS232 Serial Port

The RS232 serial console port provides a connection between the appliance and a computer, allowing direct access to the appliance for initial configuration or troubleshooting.

All hardware platforms ship with an appropriate serial cable used to connect your computer to the appliance. For instructions on connecting your computer to the appliance, see "Installing the Hardware."

Copper Ethernet Ports

The copper Ethernet ports installed on many models of the appliance are standard RJ45 ports.

There are two types of copper Ethernet ports that may be installed on your appliance:

10/100BASE-T port

The 10/100BASE-T port has a maximum transmission speed of 100 megabits per second (Mbps). Most platforms have at least one 10/100BASE-T port.

10/100/1000BASE-T port

The 10/100/1000BASE-T port has a maximum transmission speed of 1 gigabit per second, ten times faster than the other type of copper Ethernet port. Most platforms have at least one 10/100/1000Base-T port.

To connect any of these ports to your network, you plug one end of a standard Ethernet cable into the port and plug the other end into the appropriate network connector.

Management Ports

Management ports are standard copper Ethernet ports (RJ45), which are used for direct access to the appliance for system administration functions.

1G SFP, 10G SFP+, and XFP Ports

A 1G SFP port can operate at a speed of 1 Gbps. It accepts either a copper 1G SFP transceiver, for operation as a copper Ethernet port, or a fiber 1G SFP transceiver for operation as a fiber optic port.

The 10G SFP+ and XFP ports are high-speed ports that can operate at speeds of up to 10 Gbps. You need a fiber optic cable to connect to a 10G SFP+ or XFP port. If the other end of the fiber optic cable is attached to a 1G SFP port, the 10G SFP+ port automatically negotiates to match the speed of the 1G SFP port.

The following tables list the maximum distance specifications for NetScaler pluggable media (1G SFP, 10G SFP+, and XFP transceivers).

Note: The tables are categorized by 1G pluggable media and 10G pluggable media.

The 10G SFP+ modules are dual-speed capable and support both 1G and 10G, depending on the peer switch that the model connects to. These are listed in both tables.

Both tables have the following columns:

- SKU: Citrix maintains multiple SKUs for the same part.
- Description: The price list description of the part.
- Transmit Wavelength: The nominal transmit wavelength.
- Cable/Fiber Type: Fiber characteristics affect the maximum transmit distance achievable. This is especially true with 10G on multi-mode fiber (MMF), where various dispersion components become dominant. For more information, see http://www.thefoa.org/tech/ref/basic/fiber.html.
- Typical Reach: Maximum transmit distance.
- Products: Some chassis are available with different media options. Use the appropriate data sheet to confirm that your particular chassis type supports the media.

1G Pluggable Media

The following table lists the maximum distance specifications for 1G transceivers.

Table 1. Copper 1G SFP Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Cable Type	Typical Reach (m)	Products

EW3A0000235, EW3B0000235, EW3C0000235, EW3D0000235, EW3E0000235, EW3F0000235, EW3P0000143, EW3X0000235, EW3Z0000087	Citrix NetScaler 1G SFP Ethernet Copper (100m) - **4 Pack**	n/a	Category 5 (Cat-5) Copper Cable	100 m	MPX 7500/9500, MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, 9010 FIPS

Table 2. Short Reach Fiber 1G SFP Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products
EW3A0000234, EW3B0000234, EW3C0000234, EW3D0000234, EW3E0000234, EW3F0000234, EW3P0000142, EW3X0000234, EW3Z0000086	Citrix NetScaler 1G SFP Ethernet SX (300m) - **4 Pack**	850nm (nominal)	50/125um MMF, 2000MHz-km (OM3)	550 m	MPX 7500/9500, MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, 9010 FIPS
			50/125um MMF, 500MHz-km (OM2)	550 m	
			50/125um MMF, 400MHz-km	550 m	
			62.5/125um MMF, 200MHz-km (OM1)	300 m	
			62.5/125um MMF, 160MHz-km	300 m	

Table 3. Short Reach Fiber 1G SFP Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products

EW3A0000710, EW3B0000710, EW3C0000710, EW3D0000710, EW3E0000710, EW3F0000710, EW3P0000557, EW3X0000710, EW3Z0000585	Citrix NetScaler 1G SFP Ethernet Short Range (300m) - **Single**	850nm (nominal)	50/125um MMF, 2000MHz-km (OM3)	550 m	MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, MPX 17500/19500/21500, MPX 11500/13500/14500/16500/18500/20500,
			50/125um MMF, 500MHz-km (OM2)	550 m	
			50/125um MMF, 400MHz-km	550 m	
			62.5/125um MMF, 200MHz-km (OM1)	275 m	
			62.5/125um MMF, 160MHz-km	220 m	

Table 4. Long Reach Fiber 1G SFP Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products
EW3A0000712, EW3B0000712, EW3C0000712, EW3D0000712, EW3E0000712, EW3F0000712, EW3P0000559, EW3X0000712, EW3Z0000587	Citrix NetScaler 1G SFP Ethernet LX - **Single**	1310nm (nominal)	9/125um SMF	10 km	MPX 7500/9500, MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, 9010 FIPS

Table 5. Long Reach Fiber 1G SFP Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products
EW3A0000711, EW3B0000711, EW3C0000711, EW3D0000711, EW3E0000711, EW3F0000711, EW3P0000558, EW3X0000711, EW3Z0000586	Citrix NetScaler 1G SFP Ethernet Long Range (10km) - **Single**	1310nm (nominal)	9/125um SMF	10 km	MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, MPX 17500/19500/21500, MPX 11500/13500/14500/16500/18500/20500,

10 GE Pluggable Media

The following table lists the maximum distance specifications for 10G transceivers.

Table 6. Short Reach Fiber 10G SFP+ Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products
EW3A0000710, EW3B0000710, EW3C0000710, EW3D0000710, EW3E0000710, EW3F0000710, EW3P0000557, EW3X0000710, EW3Z0000585	Citrix NetScaler 10G SFP+ Ethernet Short Range (300m) - **Single**	850nm (nominal)	50/125um MMF, 2000MHz-km (OM3)	300 m	MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, MPX 17500/19500/21500, MPX 11500/13500/14500/16500/18500/20500, MPX 17550/19550/20550/21550
			50/125um MMF, 500MHz-km (OM2)	82 m	
			50/125um MMF, 400MHz-km	66 m	
			62.5/125um MMF, 200MHz-km (OM1)	33 m	
			62.5/125um MMF, 160MHz-km	26 m	

Table 7. Short Reach XFP (10G) Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products
EW3A0000713, EW3B0000713, EW3C0000713, EW3D0000713, EW3E0000713, EW3F0000713, EW3P0000560, EW3X0000713, EW3Z0000588	Citrix NetScaler XFP Short Range 10 Gigabit Ethernet(300m) - **Single**	850nm (nominal)	50/125um MMF, 2000MHz-km (OM3)	300 m	MPX 15000/17000
			50/125um MMF, 500MHz-km (OM2)	82 m	
			50/125um MMF, 400MHz-km	66 m	
			62.5/125um MMF, 200MHz-km (OM1)	33 m	
			62.5/125um MMF, 160MHz-km	26 m	

Table 8. Long Reach Fiber 10G SFP+ Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products
EW3A0000711, EW3B0000711, EW3C0000711, EW3D0000711, EW3E0000711, EW3F0000711, EW3P0000558, EW3X0000711, EW3Z0000586	Citrix NetScaler 10G SFP+ Ethernet Long Range (10km) - **Single**	1310nm (nominal)	9/125um SMF	10 km	MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, MPX 17500/19500/21500, MPX 11500/13500/14500/16500/18500/20500, MPX 17550/19550/20550/21550

Table 9. Long Reach Fiber XFP (10G) Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products
EW3A0000714, EW3B0000714, EW3C0000714, EW3D0000714, EW3E0000714, EW3F0000714, EW3P0000561, EW3X0000714, EW3Z0000589	Citrix NetScaler XFP Long Range 10 Gigabit Ethernet(10 km) - **Single**	1310nm (nominal)	9/125um SMF	10 km	MPX 15000/17000

LED Port-Status Indicators

Note: This section applies to the MPX 5500, MPX 5550/5650, MPX 7500/9500, MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, MPX 17500/19500/21500, MPX 11500/13500/14500/16500/18500/20500, and MPX 17550/19550/20550/21550 appliances.

The port LEDs show whether a link is established and traffic is flowing through the port. The following table describes the LED indicators for each port. There are two LED indicators for each port type.

Table 10. LED port-status indicators

Port Type	LED Location	LED Function	LED Color	LED Indicates

10G SFP+ (10 Gbps)	Left	Link/ Activity	Off	No link.
			Solid green	Link is established but no traffic is passing through the port.
			Blinking green	Traffic is passing through the port.
	Right	Speed	Off	No connection.
			Solid green	Traffic rate of 10 gigabits per second.
1G SFP (1 Gbps)	Left	Link/ Activity	Off	No link.
			Solid green	Link is established but no traffic is passing through the port.
			Blinking green	Traffic is passing through the port.
	Right	Speed	Off	No connection.
			Yellow	Traffic rate of 1 gigabit per second.
Ethernet (RJ45)	Left	Speed	Off	No connection, or a traffic rate of 10 megabits per second (Mbps).
			Green	Traffic rate of 100 Mbps.
			Yellow	Traffic rate of 1 gigabit per second.
	Right	Link/ Activity	Off	No link.
			Solid green	Link is established but no traffic is passing through the port.
			Blinking green	Traffic is passing through the port.

Management (RJ45)	Left	Speed	Off	No connection, or a traffic rate of 10 megabits per second (Mbps).
			Green	Traffic rate of 100 Mbps.
			Amber	Traffic rate of 1 gigabit per second.
	Right	Link/ Activity	Off	No link.
			Solid yellow	Link is established but no traffic is passing through the port.
			Blinking yellow	Traffic is passing through the port.

Field Replaceable Units

Citrix NetScaler field replaceable units (FRU) are NetScaler components that can be quickly and easily removed from the appliance and replaced by the user or a technician at the user's site. The FRUs in a NetScaler appliance can include a CompactFlash card, DC or AC power supplies, and solid-state or hard-disk drives, and a direct attach cable (DAC).

Note: The solid-state or hard-disk drive stores your configuration information, which has to be restored from a backup after replacing the unit.

Power Supply

For appliances containing two power supplies, the second power supply acts as a backup.

The appliance ships with a standard power cord that plugs into the appliance's power supply and an NEMA 5-15 plug on the other end for connecting to the power outlet on the rack or in the wall.

For power-supply specifications, see "Hardware Platforms," which describes the various platforms and includes a table summarizing the hardware specifications.

Note: If you suspect that a power-supply fan is not working, please see the description of your platform. On some platforms, what appears to be the fan does not turn, and the actual fan turns only when necessary.

For each power supply, a bicolor LED indicator shows the condition of the power supply. The LEDs of the AC power supplies for MPX 15000 and 17000 appliances are different from the LEDs of the other appliances.

Table 1. LED Power Supply Indicators

Power Supply Type	LED Color	LED Indicates
AC	OFF	No power to any power supply.
	Flashing RED	No power to this power supply.
	Flashing GREEN	Power supply is in standby mode.
	GREEN	Power supply is functional.
	RED	Power supply failure.
DC	OFF	No power to any power supply.
	Flashing RED	No power to this power supply.
	Flashing BLUE	Power supply is in standby mode.
	BLUE	Power supply is functional.
	RED	Power supply failure.

MPX 15000 and 17000	OFF	Power supply is not plugged in to a power source. If the LED is off when the power supply is plugged in, the power supply has a malfunction.
	AMBER	Power supply has been plugged in for less than a few seconds. If the LED does not turn GREEN, the power supply has a malfunction.
	GREEN	Power supply is functioning properly.
	BLINKING	Power supply has a malfunction

Note: The power supply on the NetScaler MPX 5500 and MPX 5550/5650 appliances is not field replaceable.

Electrical Safety Precautions for Power Supply Replacement

- Make sure that the appliance has a direct physical connection to earth ground during normal use. When installing or repairing an appliance, always connect the ground circuit first and disconnect it last.
- Always unplug any appliance before performing repairs or upgrades.
- Never touch a power supply when the power cord is plugged in. As long as the power cord is plugged in, line voltages are present in the power supply even if the power switch is turned off.

Replacing an AC Power Supply

Citrix NetScaler MPX platforms can accommodate two power supplies. All NetScaler appliances function properly with a single power supply. The other power supplies serves as a backup. All power supplies must be of the same type (AC or DC).

Note: If the appliance has only one power supply, you have to shut down the appliance before replacing the power supply. If the appliance has two power supplies, you can replace one power supply without shutting down the appliance, provided the other power supply is working.

To install or replace an AC power supply on a Citrix NetScaler appliance

1. Align the semicircular handle perpendicular to the power supply. Loosen the thumbscrew and press the lever toward the handle and pull out the existing power supply, as shown in the following figure.

Note: The illustration in the following figures might not represent the actual NetScaler appliance.

Figure 1. Removing the Existing AC Power Supply

2. Carefully remove the new power supply from its box.
3. On the back of the appliance, align the power supply with the power supply slot.
4. Insert the power supply into the slot and press against the semicircular handle until you hear the power supply snap into place.

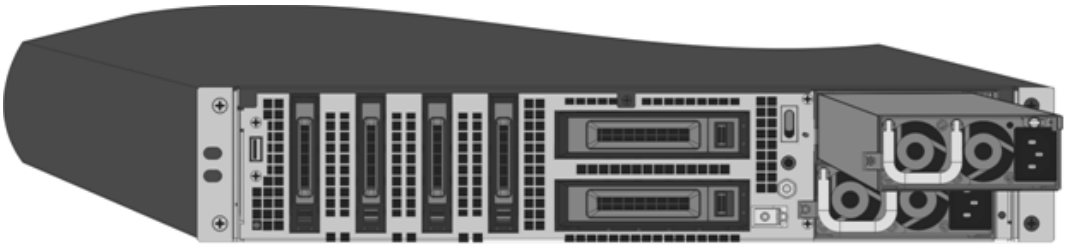


Figure 2. Inserting the Replacement AC Power Supply

5. Connect the power supply to a power source. If connecting all power supplies, plug separate power cords into the power supplies and connect them to separate wall sockets.

Note: NetScaler appliances emit a high-pitched alert if one power supply fails or if you connect only one power cable to an appliance in which two power supplies are installed. To silence the alarm, press the small red button on the back panel of the appliance. The disable alarm button is functional only when the appliance has two power supplies.

Replacing a DC Power Supply

Citrix NetScaler MPX platforms can accommodate two power supplies. All NetScaler appliances function properly with a single power supply. The other power supplies serves as a backup. All power supplies must be of the same type (AC or DC).

Note: If the appliance has only one power supply, you have to shut down the appliance before replacing the power supply. If the appliance has two power supplies, you can replace one power supply without shutting down the appliance, provided the other power supply is working.

To install or replace a DC power supply on a Citrix NetScaler appliance

1. Loosen the thumbscrew and press the lever towards the handle and pull out the existing power supply, as shown in the following figure.

   Note: The illustration in the following figures might not represent the actual NetScaler appliance.

   Figure 3. Removing the Existing DC Power Supply
2. Carefully remove the new power supply from its box.

3. On the back of the appliance, align the power supply with the power supply slot.

4. Insert the power supply into the slot while pressing the lever towards the handle. Apply firm pressure to insert the power supply firmly into the slot.

   Figure 4. Inserting the Replacement DC Power Supply
5. When the power supply is completely inserted into its slot, release the lever.

6. Connect the power supply to a power source. If connecting all power supplies, plug separate power cords into the power supplies and connect them to separate wall sockets.

Note: NetScaler appliances emit a high-pitched alert if one power supply fails or if you connect only one power cable to an appliance in which two power supplies are installed. To silence the alarm, press the small red button on the back panel of the appliance. The disable alarm button is functional only when the appliance has two power supplies.

CompactFlash Card

The NetScaler software is stored on either the solid-state drive or the CompactFlash card. The following MPX platforms store the NetScaler software on the CompactFlash card:

- Citrix NetScaler MPX 5500
- Citrix NetScaler MPX 7500 and MPX 9500
- Citrix NetScaler MPX 9700, MPX 10500, MPX 12500, and MPX 15500
- Citrix NetScaler MPX 15000
- Citrix NetScaler MPX 17000

Note: The CompactFlash card is mounted as /flash on the above platforms.

The CompactFlash card specifications vary by NetScaler hardware platform. A CompactFlash card from one platform does not necessarily work on a different platform.

Replacing a CompactFlash Card

Note: These instructions apply to the Citrix® NetScaler® MPX 5500, MPX 7500/9500, MPX 9700/10500/12500/15500, MPX 15000, and MPX 17000 appliances only.

Replacement CompactFlash cards contain a preinstalled version of the NetScaler software and a generic configuration file (ns.conf), but they do not contain SSL-related certificates and keys, or custom boot settings. Configuration files and customized settings must be restored from a backup storage location at the customer site, if available. The files to be restored might include:

- /flash/nsconfig/ns.conf: The current configuration file.
- /flash/nsconfig/ZebOS.conf: The ZebOS configuration file.
- /flash/nsconfig/license: The licenses for the NetScaler features.
- /flash/nsconfig/ssl: The SSL certificates and keys required for encrypting data to clients or to backend servers.
- /nsconfig/rc.netscaler: Customer-specific boot operations (optional).

Note: Verify that the card you receive is the correct type for your NetScaler appliance.

To replace a CompactFlash card

1. At the NetScaler command prompt, exit to the shell prompt. Type:

   shell

2. Shut down the NetScaler appliance by typing one of the following commands at the shell prompt.

   - On an MPX appliance, type:

     shutdown -p now

   - On a non-MPX appliance, type:

     shutdown

3. Locate the CompactFlash slot on the back panel of the appliance.

4. Disengage the CompactFlash by pushing the lever to the right of the CompactFlash slot. If necessary, use a pen or small screwdriver to push the lever in fully. Pull the existing flash card out of the slot.

   Note: The illustration in the following figures might not represent the actual NetScaler appliance.

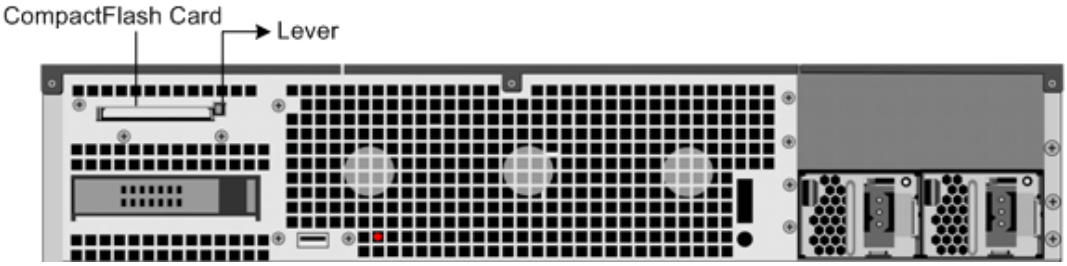


Figure 1. Removing the Existing CompactFlash Card

5. Insert the new flash card received from Citrix.

   Important: When you insert the card, make sure that the arrow on top of the card is pointing toward the CompactFlash slot. Position the connector grid on the edge of the CompactFlash card to meet the matching connector pins inside the CompactFlash slot.

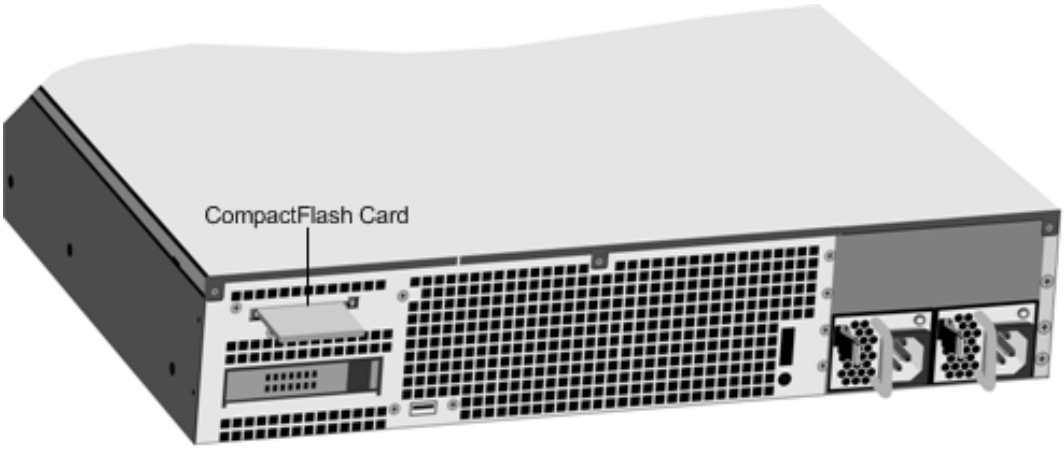


Figure 2. Inserting the Replacement CompactFlash Card

6. Turn on the NetScaler appliance.

   When the appliance starts, it no longer has the previous working configuration. Therefore, the appliance is reachable only through the default IP address of 192.168.100.1/16, or through the console port.

7. Perform the initial configuration of the appliance, as described in "Initial Configuration." Log on to the default IP address by using a web browser, or connect to the serial console by using a console cable, to perform the initial configuration.

8. Upload a platform license and any optional feature licenses, including universal licenses, to the NetScaler appliance. For more information, see the licensing chapter of the "Getting Started with Citrix NetScaler."

9. Once the correct NetScaler software version is loaded, you can restore the working configuration. Copy a previous version of the ns.conf file to the /nsconfig directory by using an SCP utility or by pasting the previous configuration into the /nsconfig/ns.conf file from the NetScaler command prompt. To load the new ns.conf file, restart the NetScaler appliance by entering the reboot command at the NetScaler command prompt.

Solid-State Drive

A solid-state drive (SSD) is a high-performance device that stores data in solid-state flash memory. The MPX solid-state drives contain the boot loader configuration file, configuration file (ns.conf), licenses, and for some models, the NetScaler software and the user data.

The NetScaler software is stored on either the SSD or the CompactFlash card. The following MPX platforms store the NetScaler software on the SSD. The SSD is mounted as /flash.

- Citrix NetScaler MPX 5550 and MPX 5650
- Citrix NetScaler MPX 8200, MPX 8400, MPX 8600, and MPX 8800
- Citrix NetScaler MPX 11500, MPX 13500, MPX 14500, MPX 16500, MPX 18500, and MPX 20500
- Citrix NetScaler MPX 17500, MPX 19500, and MPX 21500
- Citrix NetScaler MPX 17550, MPX 19550, MPX 20550, and MPX 21550
- Citrix NetScaler MPX 24100 and MPX 24150

Note: On the MPX 5550/5650 and MPX 8200/8400/8600/8800 appliances, both /flash and /var are mounted from different partitions of the same SSD drive.

Replacing a Solid-State Drive

Note: These instructions apply to the Citrix NetScaler MPX 5550/5650, MPX 8200/8400/8600/8800, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances.

Replacement solid-state drives (SSDs) contain a pre-installed version of the NetScaler software and a generic configuration file (ns.conf), but they do not contain SSL-related certificates and keys, or custom boot settings. Configuration files and customized settings must be restored to a replacement drive from a backup storage location at the customer site, if available. The files to be restored might include:

- /flash/nsconfig/ns.conf: The current configuration file.
- /flash/nsconfig/ZebOS.conf: The ZebOS configuration file.
- /flash/nsconfig/license: The licenses for the NetScaler features.
- /flash/nsconfig/ssl: The SSL certificates and keys required for encrypting data to clients or to backend servers.
- /nsconfig/rc.netscaler: Customer-specific boot operations (optional).

To replace a solid-state drive

1. At the NetScaler command prompt, exit to the shell prompt. Type:

   shell

2. Shut down the NetScaler appliance by typing the following command at the shell prompt:

   shutdown -p now

3. Locate the SSD on the back panel of the appliance. Push the safety latch of the drive cover to the right or down, depending on the platform, while pulling out on the drive handle to disengage. Pull out the faulty drive.

   Note: The illustration in the following figures might not represent the actual NetScaler appliance.

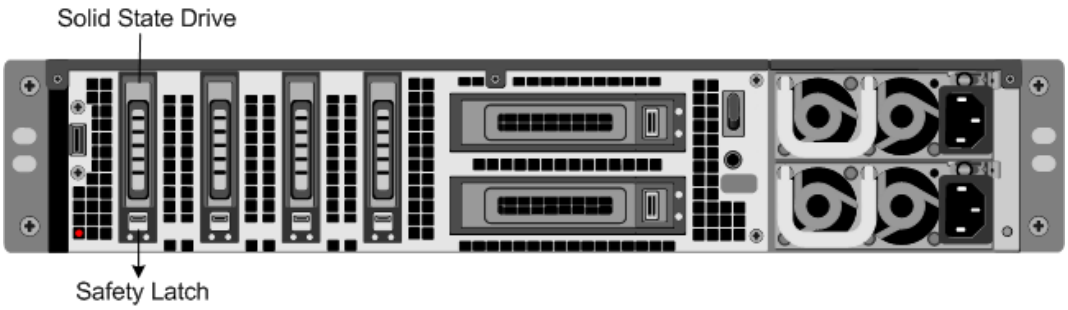


Figure 1. Removing the Existing Solid-State Drive

4. Verify that the replacement SSD is the correct type for the platform.

5. Pick up the new SSD, open the drive handle fully to the left or up, and insert the drive into the slot as far as possible. To seat the drive, close the handle flush with the rear of the appliance so that the drive locks securely into the slot.

   Important: When you insert the drive, make sure that the Citrix product label is at the top if the drive is inserted horizontally or at the right if the drive is inserted vertically.

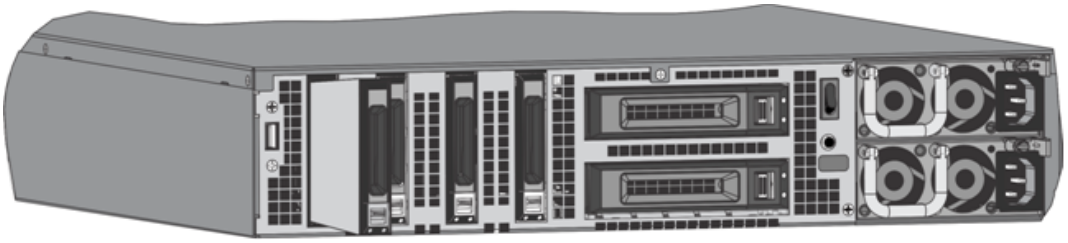


Figure 2. Inserting the Replacement Solid-State Drive

6. Turn on the NetScaler appliance. When the appliance starts, it no longer has the previous working configuration. Therefore, the appliance is reachable only through the default IP address of 192.168.100.1/16, or through the console port.

7. Perform the initial configuration of the appliance, as described in "Initial Configuration." Log on to the default IP address by using a web browser, or connect to the serial console by using a console cable, to perform the initial configuration.

8. Upload a platform license and any optional feature licenses, including universal licenses, to the NetScaler appliance. For more information, see the licensing chapter of the "Getting Started with Citrix NetScaler."

9. Once the correct NetScaler software version is loaded, you can restore the working configuration. Copy a previous version of the ns.conf file to the /nsconfig directory by using an SCP utility or by pasting the previous configuration into the /nsconfig/ns.conf file from the NetScaler command prompt. To load the new ns.conf file, you must restart the NetScaler appliance by entering the reboot command at the NetScaler command prompt.

Hard Disk Drive

A hard disk drive (HDD) stores logs and other data files. Files stored on the HDD include the newnslog files, dmesg and messages files, and any core/crash files. The HDD comes in various capacities, depending on the Citrix NetScaler platform. Hard drives are used for storing files required at runtime. An HDD is mounted as /var.

The following MPX platforms support HDD:

- Citrix NetScaler MPX 9700, MPX 10500, MPX 12500, and MPX 15500
- Citrix NetScaler MPX 11500, MPX 13500, MPX 14500, MPX 16500, MPX 18500, and MPX 20500
- Citrix NetScaler MPX 15000
- Citrix NetScaler MPX 17000
- Citrix NetScaler MPX 17500, MPX 19500, and MPX 21500
- Citrix NetScaler MPX 17550, MPX 19550, MPX 20550, and MPX 21550
- Citrix NetScaler MPX 24100 and MPX 24150

Replacing a Hard Disk Drive

A hard disk drive (HDD) stores log files and other user files. Collection of new log files begins upon boot-up with the new HDD. Product documentation can be downloaded from "MyCitrix.com" and reinstalled to the /var/netscaler/doc location.

To install a hard disk drive

1. At the NetScaler command prompt, exit to the shell prompt. Type:

   shell

2. Shut down the NetScaler appliance by typing one of the following commands at the shell prompt.

   - On an MPX appliance, type:

     shutdown -p now

   - On a non-MPX appliance, type:

     shutdown

3. Locate the hard disk drive on the back panel of the appliance.
4. Verify that the replacement hard disk drive is the correct type for the NetScaler platform.

5. Disengage the hard disk drive by pushing the safety latch of the drive cover to the right or down, depending on the platform, while pulling out on the drive handle to disengage. Pull out the faulty drive.

   Note: The illustration in the following figures might not represent the actual NetScaler appliance.

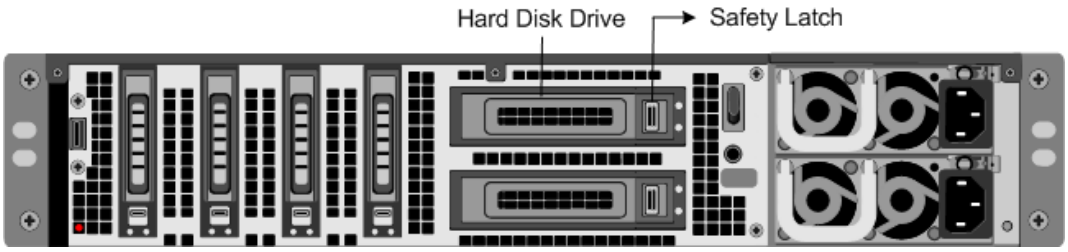


Figure 1. Removing the Existing Hard Disk Drive

6. Pick up the new disk drive, open the drive handle fully to the left, and insert the new drive into the slot as far as possible. To seat the drive, close the handle flush with the rear of the appliance so that the hard drive locks securely into the slot.

   Important: When you insert the drive, make sure that the Citrix product label is at the top.

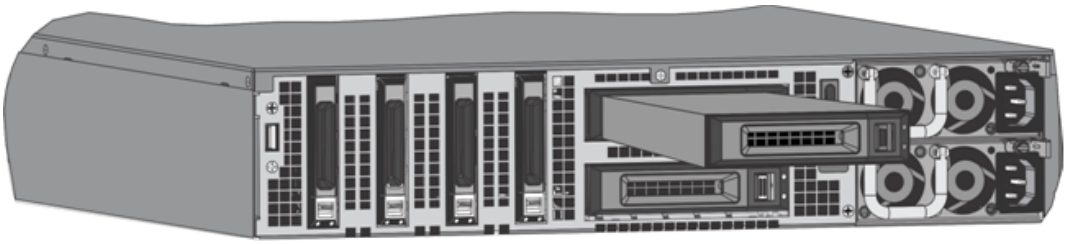


Figure 2. Inserting the Replacement Hard Disk Drive

7. Turn on the NetScaler appliance. The appliance starts the NetScaler software and reads the configuration file from the CompactFlash card.

Direct Attach Cable

A direct attach cable (DAC) assembly is a high performance integrated duplex data link for bi-directional communication. The cable is compliant with the IPF MSA (SFF-8432) for mechanical form factor and SFP+ MSA for direct attach cables. The cable, which can be up to 5 meters long, is data-rate agnostic. Supporting speeds in excess of 10 Gbps, it is a cost-effective alternative to optical links (SFP+ transceivers and fiber optic cables.) The transceiver with DAC is hot-swappable. You can insert and remove the transceiver with the attached cable without shutting down the appliance. The Citrix NetScaler appliance supports only passive DAC.

Important:

- DAC is supported only on 10G ports. Do not insert a DAC into a 1G port.
- Do not attempt to unplug the integrated copper cable from the transceiver and insert a fiber cable into the transceiver.

Installing a Direct Attach Cable

Note: The illustrations in the following figures are only for reference and might not represent the actual NetScaler appliance.

To install or remove a direct attach cable

1. To install the DAC, slide it into the 10G port on the appliance, as shown in the following figure. You will hear a click when the DAC properly fits into the port.

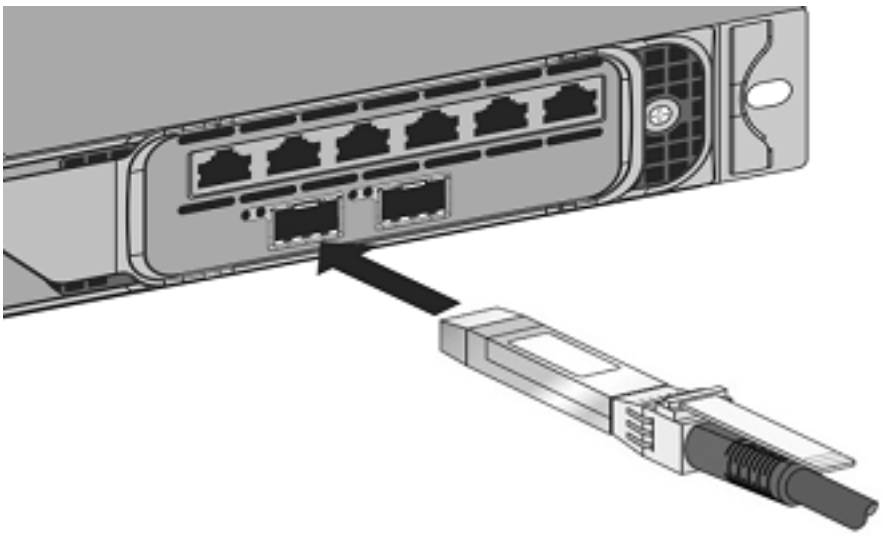


Figure 1. Inserting a DAC into the 10G port

2. To remove the DAC, pull the tab on the top of the DAC, and then pull the DAC out of the port, as shown in the following figure.

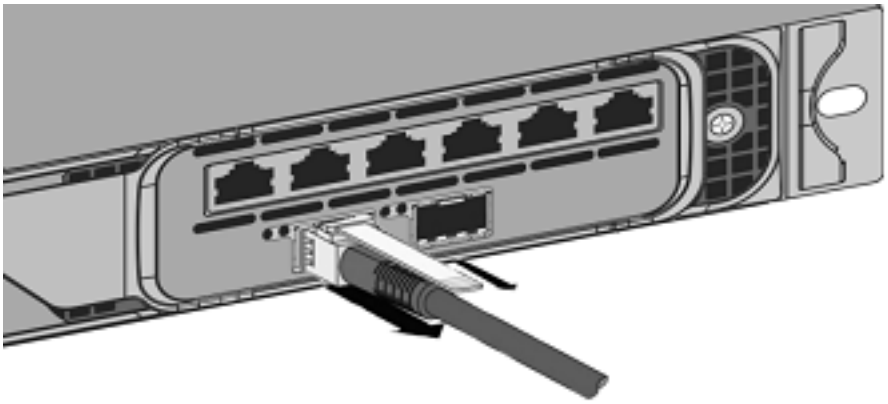


Figure 2. Removing a DAC from the 10G port

Hardware Platforms

The various NetScaler hardware platforms offer a wide range of features, communication ports, and processing capacities. All the MPX platforms have multicore processors.

Citrix NetScaler MPX 5500

The Citrix NetScaler MPX 5500 is a 1U appliance, with 1 dual-core processor, and 4 gigabytes (GB) of memory.

The following figure shows the front panel of the MPX 5500.

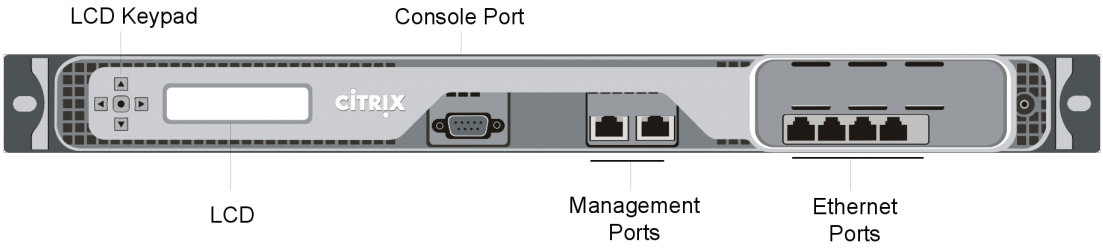


Figure 1. Citrix NetScaler MPX 5500, front panel

The MPX 5500 has the following ports:

- RS232 serial console port.
- Two 10/100/1000Base-T copper Ethernet management ports, numbered 0/1 and 0/2 from left to right. You can use these ports to connect directly to the appliance for system administration functions.
- Four 10/100/1000Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, and 1/4 from left to right.

Note: The network port numbers on all appliances consist of two numbers separated by a forward slash. The first number is the port adapter slot number. The second number is the interface port number. Ports on appliances are numbered sequentially starting with 1.

The following figure shows the back panel of the MPX 5500.

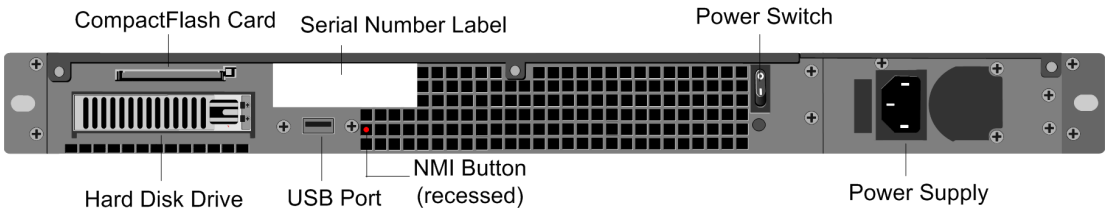


Figure 2. Citrix NetScaler MPX 5500, back panel

The following components are visible on the back panel of the MPX 5500:

- Four GB removable CompactFlash card that is used to store the NetScaler software.
- Power switch, which turns off power to the MPX 5500, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.

- Removable hard-disk drive (HDD) that is used to store user data. Appliances shipped before February, 2012 store user data on a HDD. In appliances shipped after February, 2012, a solid-state drive replaces the HDD. Both types of drive have the same functionality and support the same software releases.

- USB port (reserved for a future release).

- Non-maskable interrupt (NMI) Button that is used at the request of Technical Support and produces a core dump on the NetScaler. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.

- Power supply rated at 300 watts, 110-220 volts. The power-supply fan is designed to turn on only when the internal temperature of the power supply reaches a certain value. You cannot see the fan turning on the back panel. What you can see is the fixed part of the fan that holds the spinning motor.

For information about installing the rails, rack mounting the hardware, and connecting the cables, see "Installing the Hardware."

For information about performing initial configuration of your appliance, see "Initial Configuration."

Citrix NetScaler MPX 5550 and MPX 5650

The Citrix NetScaler models MPX 5550 and MPX 5650 are 1U appliances. Each model has one quad-core processor and 8 gigabytes (GB) of memory.

The following figure shows the front panel of the MPX 5550/5650 appliance.

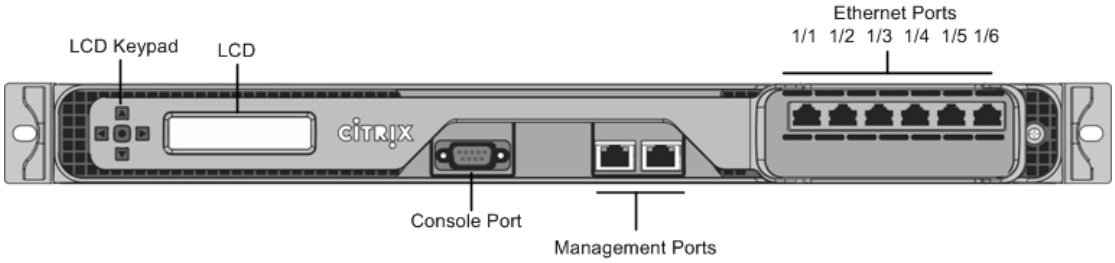


Figure 1. Citrix NetScaler MPX 5550/5650, front panel

Depending on the model, the appliance has the following ports:

- RS232 serial console port.
- Two 10/100/1000Base-T copper Ethernet management ports (RJ45), numbered 0/1 and 0/2 from left to right. The management port is used to connect directly to the appliance for system administration functions.
- Six 10/100/1000Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, 1/4, 1/5, and 1/6 from left to right.

The following figure shows the back panel of the MPX 5550/5650 appliance.

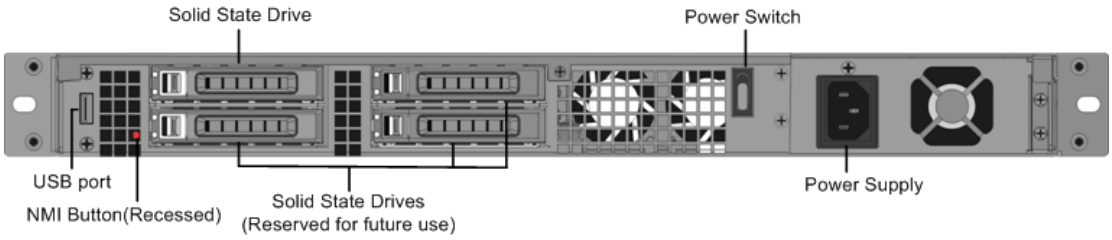


Figure 2. Citrix NetScaler MPX 5550/5650 appliance, back panel

The following components are visible on the back panel of the MPX 5550/5650 appliance:

- 160 GB removable solid-state drive, which is used to store the NetScaler software and the user data.
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.

- USB port (reserved for a future release).
- Non-maskable interrupt (NMI) button, which is used at the request of Technical Support to produce a NetScaler core dump. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Single power supply, rated at 300 watts, 110-220 volts.

For information about installing the rails, rack mounting the hardware, and connecting the cables, see "Installing the Hardware."

For information about performing initial configuration of your appliance, see "Initial Configuration."

Citrix NetScaler MPX 7500 and MPX 9500

The Citrix NetScaler MPX 7500/9500 are 1U appliances, each with 1 quad-core processor, and 8 gigabytes (GB) of memory. The MPX 7500/9500 appliances are available in two port configurations: 8x10/100/1000Base-T copper Ethernet ports and 4x1G SFP + 4x10/100/1000Base-T copper Ethernet ports.

The following figure shows the front panel of the MPX 7500/9500 (8x10/100/1000Base-T copper Ethernet ports) appliances.

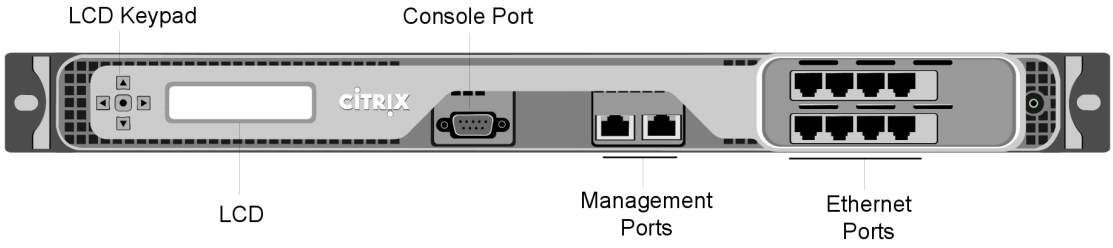


Figure 1. Citrix NetScaler MPX 7500/9500 (8x10/100/1000Base-T copper Ethernet ports), front panel

The following figure shows the front panel of the MPX 7500/9500 (4x1G SFP + 4x10/100/1000Base-T copper Ethernet ports) appliances.

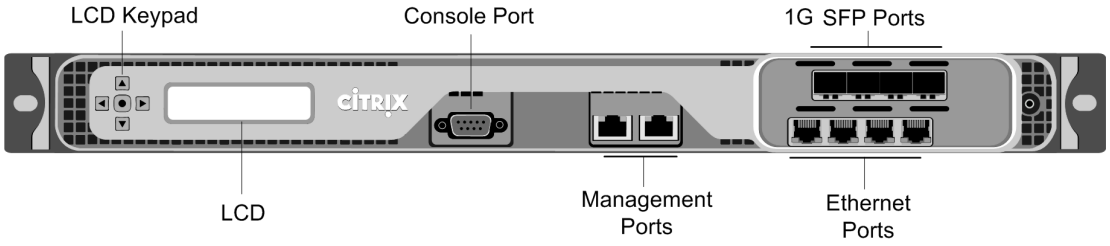


Figure 2. Citrix NetScaler MPX 7500/9500 (4x1G SFP + 4x10/100/1000Base-T copper Ethernet ports), front panel

Depending on the model, the appliance has the following ports:

- RS232 serial console port.
- Two 10/100/1000Base-T copper Ethernet management ports, numbered 0/1 and 0/2 from left to right. These ports are used to connect directly to the appliance for system administration functions.
- Network Ports

- MPX 7500/9500 (8x10/100/1000Base-T copper Ethernet ports). Eight 10/100/1000Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, and 1/4 on the top row from left to right, and 1/5, 1/6, 1/7, and 1/8 on the bottom row from left to right.

- MPX 7500/9500 (4x1G SFP + 4x10/100/1000Base-T copper Ethernet ports). Four 1-gigabit copper or fiber 1G SFP ports numbered 1/1, 1/2, 1/3, and 1/4 on the top row from left to right, and four 10/100/1000BASE-T copper Ethernet ports (RJ45) numbered 1/5, 1/6, 1/7, and 1/8 on the bottom row from left to right.

The following figure shows the back panel of the MPX 7500/9500 appliance.

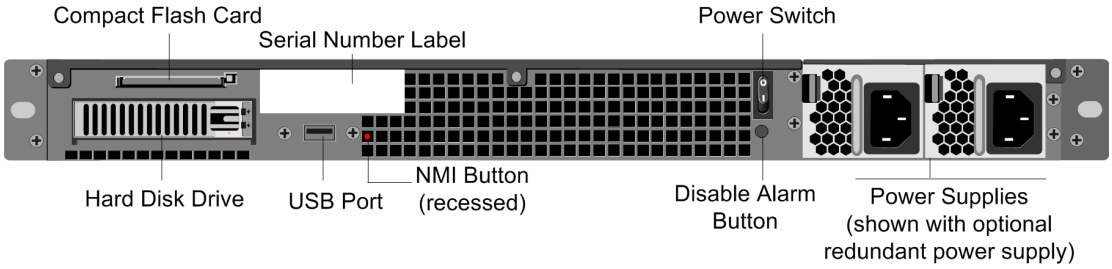


Figure 3. Citrix NetScaler MPX 7500/9500, back panel

The following components are visible on the back panel of the MPX 7500/9500:

- Four-gigabyte removable CompactFlash card that is used to store the NetScaler software.

- Power switch, which turns off power to the MPX 7500/9500, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.

- Removable hard-disk drive (HDD) that is used to store user data. Appliances shipped before February, 2012 store user data on a HDD. In appliances shipped after February, 2012, a solid-state drive replaces the HDD. Both types of drive have the same functionality and support the same software releases.

- USB port (reserved for a future release).

- Non-maskable interrupt (NMI) button that is used at the request of Technical Support and produces a core dump on the appliance. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.

- Disable alarm button. This button is functional only when the appliance has two power supplies.

  Press this button to stop the power alarm from sounding when you have plugged the MPX 7500/9500 into only one power outlet or when one power supply is malfunctioning and you want to continue operating the MPX 7500/9500 until it is repaired.

For information about installing the rails, rack mounting the hardware, and connecting the cables, see "Installing the Hardware."

For information about performing initial configuration of your appliance, see "Initial Configuration."

Citrix NetScaler MPX 8200, MPX 8400, MPX 8600, and MPX 8800

The Citrix NetScaler models MPX 8200, MPX 8400, MPX 8600, and MPX 8800 are 1U appliances. Each model has one quad-core processor and 32 gigabytes (GB) of memory. The MPX 8005/8015/8200/8400/8600/8800 appliances are available in two port configurations:

- Six 10/100/1000Base-T copper Ethernet ports and six 1G SFP ports (6x10/100/1000Base-T copper Ethernet ports + 6x1G SFP)
- Six 10/100/1000Base-T copper Ethernet ports and two 10G SFP+ ports (6x10/100/1000Base-T copper Ethernet ports + 2x10G SFP+)

The following figure shows the front panel of the MPX 8005/8015/8200/8400/8600/8800 (6x10/100/1000Base-T copper Ethernet ports + 6x1G SFP) appliance.

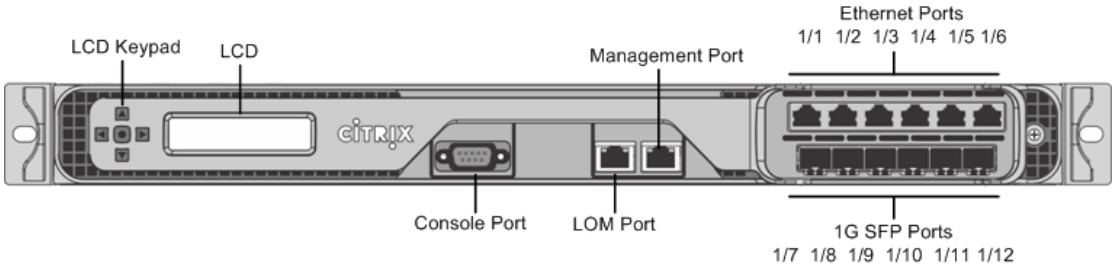


Figure 1. Citrix NetScaler MPX 8005/8015/8200/8400/8600/8800 (6x10/100/1000Base-T copper Ethernet ports + 6x1G SFP), front panel

The following figure shows the front panel of the MPX 8005/8015/8200/8400/8600/8800 (6x10/100/1000Base-T copper Ethernet ports + 2x10G SFP+) appliance.

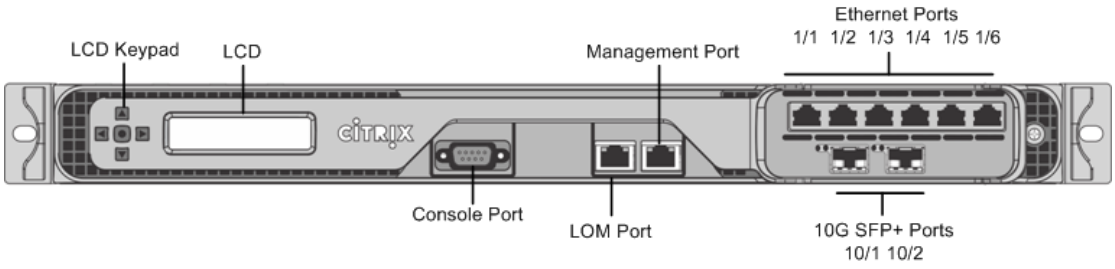


Figure 2. Citrix NetScaler MPX 8005/8015/8200/8400/8600/8800 (6x10/100/1000Base-T copper Ethernet ports + 2x10G SFP+), front panel

Depending on the model, the appliance has the following ports:

- RS232 serial console port.
- One 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the NetScaler

software.

- One 10/100/1000Base-T copper Ethernet management port (RJ45), numbered 0/1. The management port is used to connect directly to the appliance for system administration functions.

- Network Ports

  - MPX 8005/8015/8200/8400/8600/8800 (6x10/100/1000Base-T copper Ethernet ports + 6x1G SFP). Six 10/100/1000BASE-T copper Ethernet ports (RJ45) numbered 1/1, 1/2, 1/3, 1/4, 1/5, and 1/6 on the top row from left to right, and six 1-gigabit copper or fiber 1G SFP ports numbered 1/7, 1/8, 1/9, 1/10, 1/11, and 1/12 on the bottom row from left to right.

  - MPX 8005/8015/8200/8400/8600/8800 (6x10/100/1000Base-T copper Ethernet ports + 2x10G SFP+). Six 10/100/1000BASE-T copper Ethernet ports (RJ45) numbered 1/1, 1/2, 1/3, 1/4, 1/5, and 1/6 on the top row from left to right and two 10-gigabit SFP+ ports numbered 10/1 and 10/2 on the bottom row from left to right.

The following figure shows the back panel of the MPX 8005/8015/8200/8400/8600/8800 appliance.

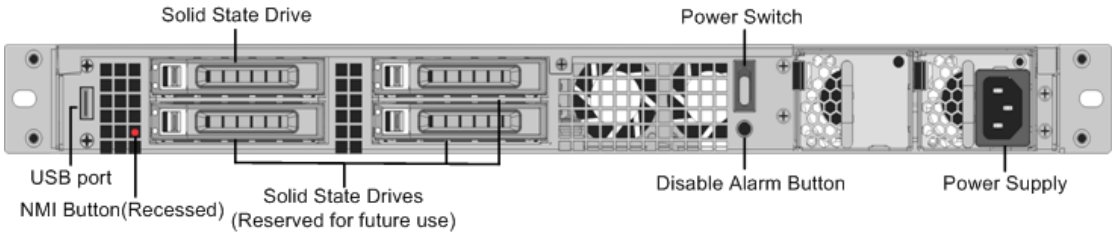


Figure 3. Citrix NetScaler MPX 8005/8015/8200/8400/8600/8800 appliance, back panel

The following components are visible on the back panel of the MPX 8005/8015/8200/8400/8600/8800 appliance:

- 256 GB removable solid-state drive, which is used to store the NetScaler software and the user data.

- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.

- USB port (reserved for a future release).

- Non-maskable interrupt (NMI) button, which is used at the request of Technical Support to produce a NetScaler core dump. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.

- Disable alarm button, which is nonfunctional. This button is functional only if you install a second power supply.

  Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.

- Single power supply, rated at 450 watts, 110-220 volts.

For information about installing the rails, rack mounting the hardware, and connecting the cables, see "Installing the Hardware."

For information about performing initial configuration of your appliance, see "Initial Configuration."

Citrix NetScaler MPX 9700, MPX 10500, MPX 12500, and MPX 15500

The Citrix NetScaler MPX 9700/10500/12500/15500 are 2U appliances, each with 2 quad-core processors, and 16 gigabytes (GB) of memory. All these appliances are also available in a 10G model and a FIPS model.

The following figure shows the front panel of the MPX 9700/10500/12500/15500.

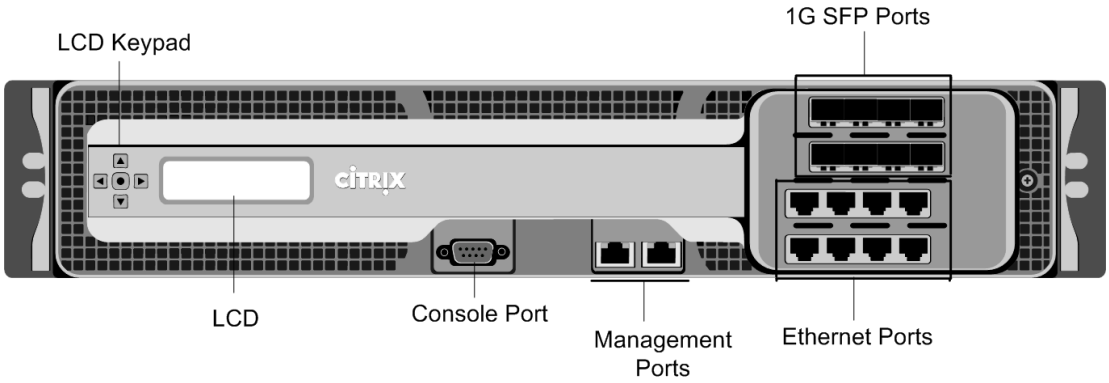


Figure 1. Citrix NetScaler MPX 9700/10500/12500/15500, front panel

The following figure shows the front panel of the MPX 9700/10500/12500/15500 10G.

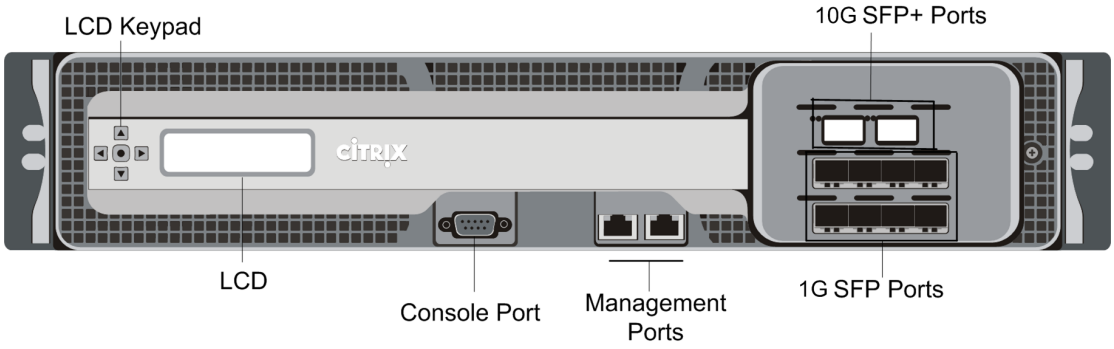


Figure 2. Citrix NetScaler MPX 9700/10500/12500/15500 10G, front panel

The following figure shows the front panel of the MPX 9700/10500/12500/15500 FIPS.

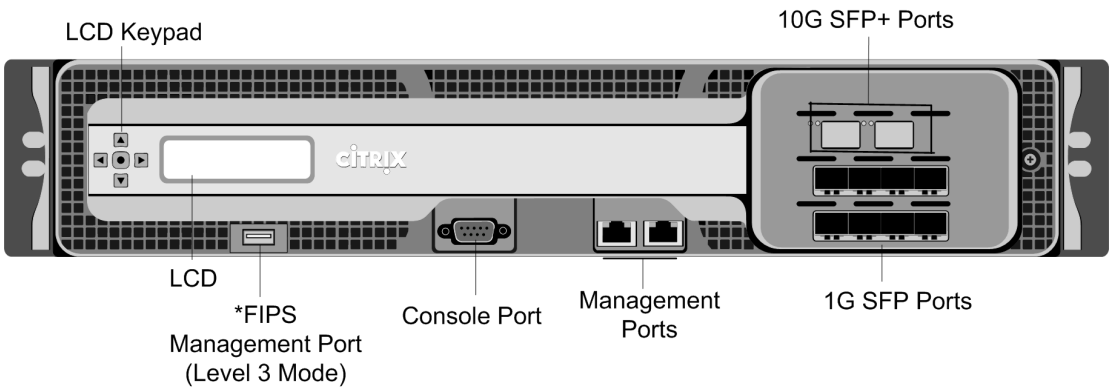


Figure 3. Citrix NetScaler MPX 9700/10500/12500/15500 FIPS, front panel

*The FIPS Management Port (Level 3 Mode) is reserved for a future release.

Caution: Do not insert a USB device into the FIPS Management Port. This will cause the FIPS card to fail.

Depending on the model, the appliance has the following ports:

- FIPS Management Port (reserved for a future release).
- RS232 serial Console Port.
- Two 10/100/1000Base-T copper Ethernet Management Ports (RJ45), numbered 0/1 and 0/2 from left to right. These ports are used to connect directly to the appliance for system administration functions.
- Network Ports
  - MPX 9700/10500/12500/15500. Eight copper or fiber 1G SFP ports numbered 1/1, 1/2, 1/3, and 1/4 on the first row from left to right, and 1/5, 1/6, 1/7, and 1/8 on the second row from left to right. Eight 10/100/1000BASE-T copper Ethernet Ports (RJ45) numbered 1/9, 1/10, 1/11, and 1/12 on the third row from left to right, and 1/13, 1/14, 1/15, and 1/16 on the fourth row from left to right.
  - MPX 9700/10500/12500/15500 10G and MPX 9700/10500/12500/15000 FIPS. Two 10G SFP+ Ports numbered 10/1 and 10/2 on the top row, eight 1-gigabit copper or fiber 1G SFP Ports numbered 1/1, 1/2, 1/3, and 1/4 on the middle row from left to right, and 1/5, 1/6, 1/7, and 1/8 on the bottom row from left to right.

Important: The 10-gigabit ports on this appliance are labeled 10/1 and 10/2.

The following figure shows the back panel of the MPX 9700/10500/12500/15500 appliances, including the 10G model and FIPS model.

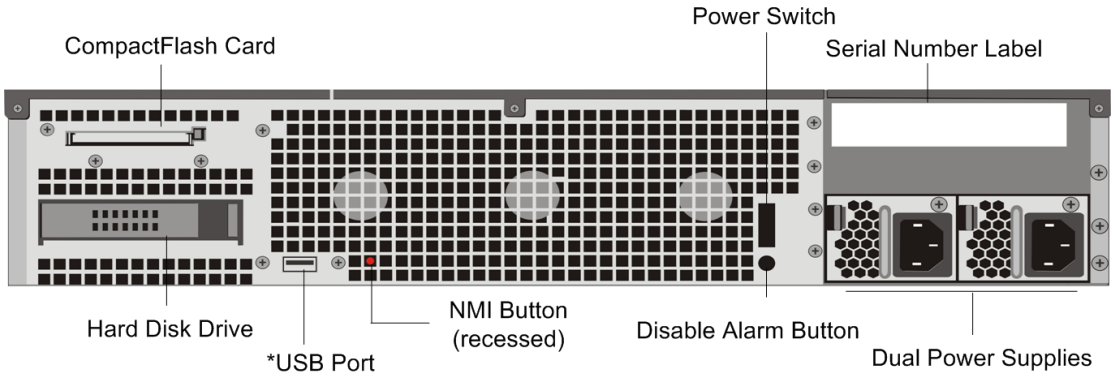


Figure 4. Citrix NetScaler MPX 9700/10500/12500/15500, MPX 9700/10500/12500/15500 FIPS, and MPX 9700/10500/12500/15500 10G, back panel

*The USB Port is reserved for a future release.

The following components are visible on the back panel of the MPX 9700/10500/12500/15500, including the 10G model and FIPS model:

- Four GB removable CompactFlash Card that is used to store the NetScaler software.
- Power Switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Removable Hard Disk Drive that is used to store user data.
- USB Port (reserved for a future release).
- Non-maskable interrupt (NMI) Button that is used at the request of Technical Support and produces a core dump on the NetScaler. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Disable Alarm Button. This button is functional only when the appliance has two power supplies.

  Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual Power Supplies, each rated at 450 watts, 110-220 volts.

For information about installing the rails, rack mounting the hardware, and connecting the cables, see "Installing the Hardware."

For information about performing initial configuration of your appliance, see "Initial Configuration."

Citrix NetScaler MPX 11500, MPX 13500, MPX 14500, MPX 16500, MPX 18500, and MPX 20500

The Citrix NetScaler models MPX 11500/13500/14500/16500/18500/20500 are 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 48 gigabytes (GB) of memory.

The following figure shows the front panel of the MPX 11500/13500/14500/16500/18500/20500 appliance.

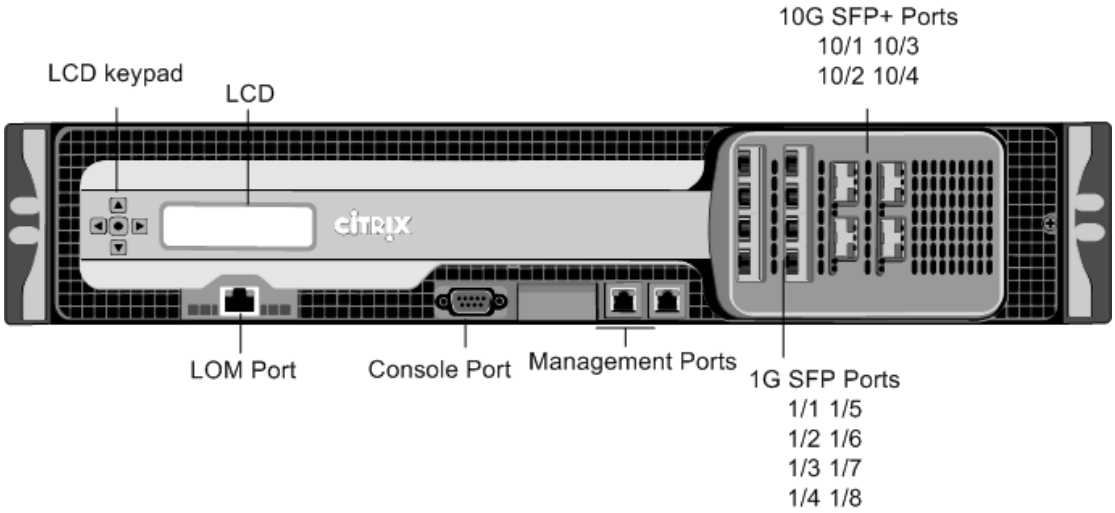


Figure 1. Citrix NetScaler MPX 11500/13500/14500/16500/18500/20500 appliance, front panel

The MPX 11500/13500/14500/16500/18500/20500 appliances have the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the NetScaler software.

  Note: The LEDs on the LOM port are not operational by design.

- RS232 serial console port.

- Two 10/100/1000Base-T copper Ethernet management ports (RJ45), numbered 0/1 and 0/2 from left to right. These ports are used to connect directly to the appliance for system administration functions.

- Eight 1G SFP ports numbered 1/1, 1/2, 1/3, 1/4 from top to bottom in the first column, and 1/5, 1/6, 1/7, and 1/8 from top to bottom in the second column.

- Four 10G SFP+ ports numbered 10/1 and 10/2 from top to bottom in the first column, and 10/3 and 10/4 from top to bottom in the second column.

The following figure shows the back panel of the MPX 11500/13500/14500/16500/18500/20500 appliance.

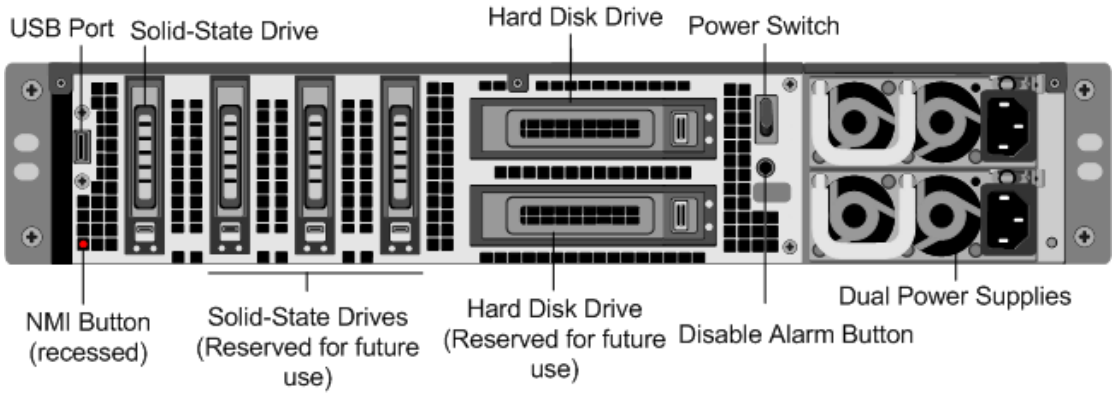


Figure 2. Citrix NetScaler MPX 11500/13500/14500/16500/18500/20500 appliance, back panel

The following components are visible on the back panel of the MPX 11500/13500/14500/16500/18500/20500 appliance:

- 160 GB removable solid-state drive that is used to store the NetScaler software.
- USB port (reserved for a future release).
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Non-maskable interrupt (NMI) Button that is used at the request of Technical Support and produces a core dump on the NetScaler. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Two removable hard-disk drives that are used to store user data.
- Disable alarm button. This button is functional only when the appliance has two power supplies.

  Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual power supplies, each rated at 650 watts, 110-220 volts.

For information about installing the rails, rack mounting the hardware, and connecting the cables, see "Installing the Hardware."

For information about performing initial configuration of your appliance, see "Initial Configuration."

Citrix NetScaler MPX 15000

The Citrix NetScaler MPX 15000 appliance is a 2U appliance, with 2 dual-core processors, and 16 GB of memory. The MPX 15000 is a high-capacity hardware platform intended for heavy use in enterprise and service provider environments. The following figure shows the front panel of the MPX 15000 appliance.

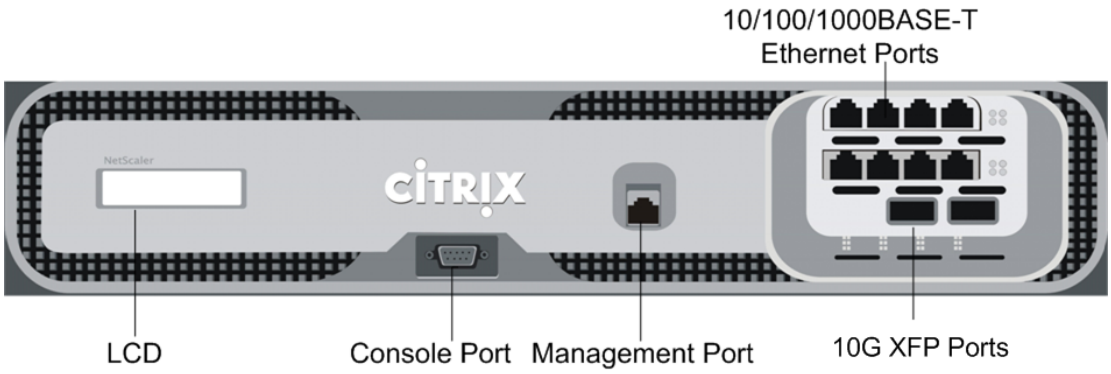


Figure 1. Citrix NetScaler MPX 15000 appliance, front panel

The appliance has the following ports:

- RS232 serial console port.
- 10/100/1000BASE-T copper Ethernet management port, numbered 0/1.
- Two XFP (10-Gigabit Small Form-Factor Pluggable) fiber optic ports, numbered from left to right 1/1 and 1/2.
- Eight 10/100/1000BASE-T copper Ethernet ports, numbered from upper left to bottom right 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 1/9, and 1/10.

When facing the bezel, the upper LEDs to the left of each port represent connectivity. They are lit and amber in color when active. The lower LEDs represent throughput. They are lit and green when active.

Note: The network port numbers on all appliances consist of two numbers separated by a forward slash. The first number is the port adapter slot number and will always be either 0 or 1. The second number is the interface port number. Ports on appliances are numbered sequentially starting with 1.

The following figure shows the back panel of the MPX 15000 appliance.

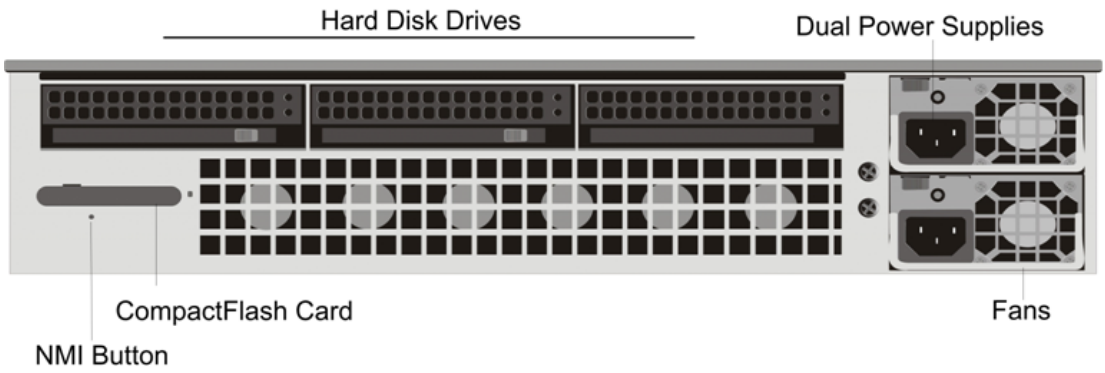


Figure 2. Citrix NetScaler MPX 15000 appliance, back panel

The following components are visible on the back panel of the MPX 15000 appliance:

- Removable hard-disk drive that is used to store user data.
- Dual power supplies, each rated at 500 watts, 110-220 volts.

  You plug separate power cords into the power supplies and connect them to separate wall sockets. The MPX 15000 functions properly with a single power supply; the extra power supply serves as a backup.
- Non-maskable interrupt (NMI) button, which signals the MPX 15000 to perform an orderly shutdown after saving all files. You must use a pen, pencil, or other pointed object to press this button, which is located inside a small hole to prevent it from being pressed accidentally.
- Removable CompactFlash card that is used to store the NetScaler software.

For information about installing the rails, rack mounting the hardware, and connecting the cables, see "Installing the Hardware."

For information about performing initial configuration of your appliance, see "Initial Configuration."

Citrix NetScaler MPX 17000

The Citrix NetScaler MPX 17000 appliance is a 2U appliance, with 2 quad-core processors, and 32 GB of memory. The MPX 17000 is a high-capacity hardware platform intended for any high traffic, intensive processing data center environment. There are two MPX 17000 models: the four network-port model and the ten network-port model.

The following figure shows the front panel of the MPX 17000, four network-port model.

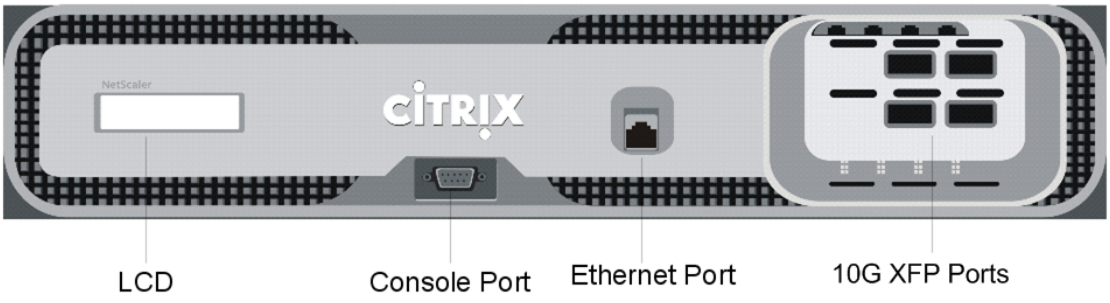


Figure 1. Citrix NetScaler MPX 17000 four network-port model, front panel

Depending on the model, the appliance has the following ports:

- RS232 serial console port.
- 10/100/1000BASE-T copper Ethernet management port, numbered 0/1.
- Network Ports
  - MPX 17000 four network-port model. Four XFP (10-Gigabit Small Form-Factor Pluggable) ports, numbered from upper left to bottom right 1/1, 1/2, 1/3, and 1/4.
  - MPX 17000 ten network-port model. Two XFP ports, numbered from left to right 1/1 and 1/2 and eight 10/100/1000BASE-T Ethernet ports, numbered from upper left to bottom right 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 1/9 and 1/10.

  Note: The network port numbers on all appliances consist of two numbers separated by a forward slash. The first number is the port adapter slot number and will always be either 0 or 1. The second number is the interface port number. Ports on appliances are numbered sequentially starting with 1.

When facing the bezel, the upper LEDs to the left of each port represent connectivity. They are lit and amber in color when active. The lower LEDs represent throughput. They are lit and green when active.

The following figure shows the back panel of the MPX 17000 appliance.

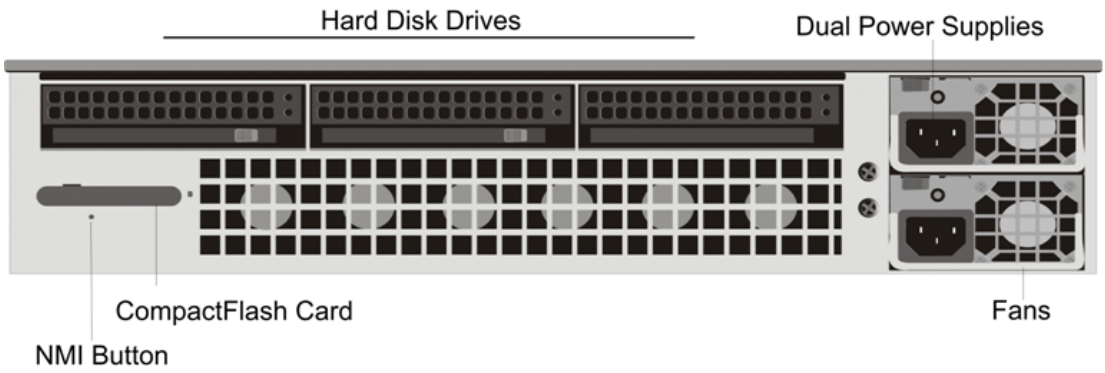


Figure 2. Citrix NetScaler MPX 17000 appliance, back panel

The following components are visible on the back of the MPX 17000 appliance:

- Removable hard-disk drive that is used to store user data.
- Dual power supplies, each rated at 500 watts, 110-220 volts.

  You plug separate power cords into the power supplies and connect them to separate wall sockets. The MPX 17000 functions properly with a single power supply; the extra power supply serves as a backup.
- Non-maskable interrupt (NMI) button, which signals the MPX 17000 to perform an orderly shutdown after saving all files. You must use a pen, pencil, or other pointed object to press this button, which is located inside a small hole to prevent it from being pressed accidentally.
- Removable CompactFlash card that is used to store the NetScaler software.

For information about installing the rails, rack mounting the hardware, and connecting the cables, see "Installing the Hardware."

For information about performing initial configuration of your appliance, see "Initial Configuration."

Citrix NetScaler MPX 17500, MPX 19500, and MPX 21500

The Citrix NetScaler models MPX 17500/19500/21500 are 2U appliances. Each model has two 6-core processors and 48 gigabytes (GB) of memory.

The following figure shows the front panel of the MPX 17500/19500/21500 appliance.

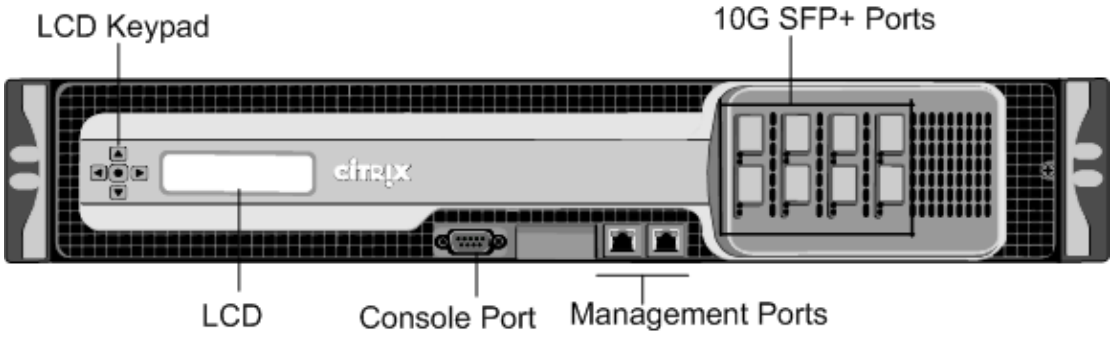


Figure 1. Citrix NetScaler MPX 17500/19500/21500 appliance, front panel

The MPX 17500/19500/21500 appliances have the following ports:

- RS232 serial console port.
- Two 10/100/1000Base-T copper Ethernet management ports (RJ45), numbered 0/1 and 0/2 from left to right. These ports are used to connect directly to the appliance for system administration functions.
- Eight 10G SFP+ ports numbered 10/1, 10/2, 10/3, and 10/4 on the top row from left to right, and 10/5, 10/6, 10/7, and 10/8 on the bottom row from left to right.

The following figure shows the back panel of the MPX 17500/19500/21500 appliance.

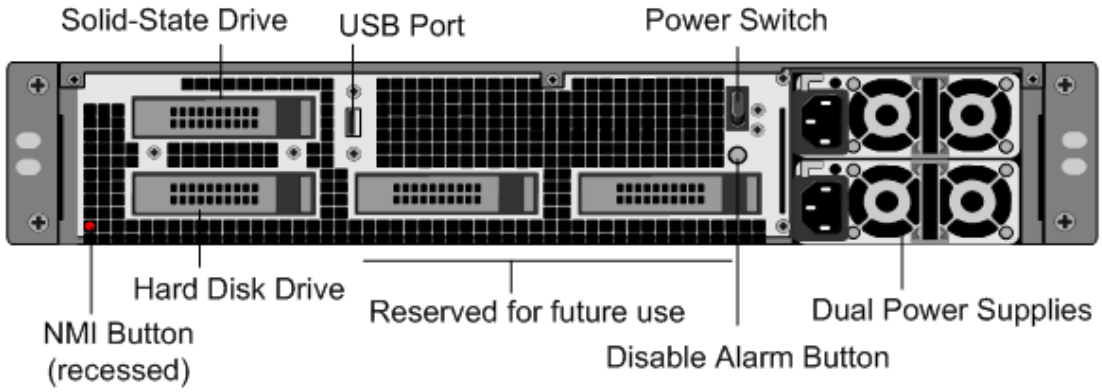


Figure 2. Citrix NetScaler MPX 17500/19500/21500 appliance, back panel

The following components are visible on the back panel of the MPX 17500/19500/21500 appliance:

- 160 GB removable solid-state drive that is used to store the NetScaler software.
- USB port (reserved for a future release).
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Non-maskable interrupt (NMI) button that is used at the request of Technical Support and produces a core dump on the NetScaler. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Removable hard-disk drive that stores user data.
- Disable alarm button. This button is functional only when the appliance has two power supplies.

  Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual power supplies, each rated at 650 watts, 110-220 volts.

For information about installing the rails, rack mounting the hardware, and connecting the cables, see "Installing the Hardware."

For information about performing initial configuration of your appliance, see "Initial Configuration."

Citrix NetScaler MPX 17550, MPX 19550, MPX 20550, and MPX 21550

The Citrix NetScaler models MPX 17550, MPX 19550, MPX 20550, and MPX 21550 are 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 96 gigabytes (GB) of memory.

The following figure shows the front panel of the MPX 17550/19550/20550/21550 appliance.

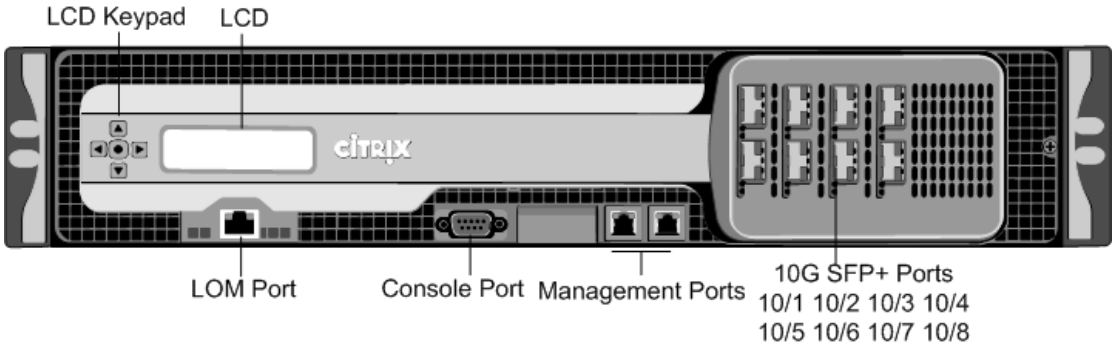


Figure 1. Citrix NetScaler MPX 17550/19550/20550/21550 appliance, front panel

The MPX 17550/19550/20550/21550 appliance has the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the NetScaler software.

  Note: The LEDs on the LOM port are not operational by design.

- RS232 serial console port.

- Two 10/100/1000Base-T copper Ethernet management ports (RJ45), numbered 0/1 and 0/2 from left to right. These ports are used to connect directly to the appliance for system administration functions.

- Eight 10G SFP+ ports numbered 10/1, 10/2, 10/3, and 10/4 on the top row from left to right, and 10/5, 10/6, 10/7, and 10/8 on the bottom row from left to right.

The following figure shows the back panel of the MPX 17550/19550/20550/21550 appliance.

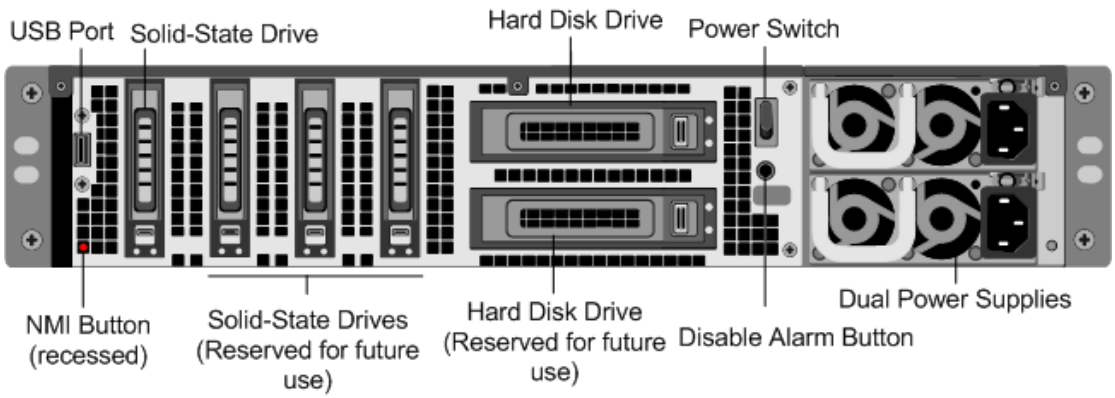


Figure 2. Citrix NetScaler MPX 17550/19550/20550/21550 appliance, back panel

The following components are visible on the back panel of the MPX 17550/19550/20550/21550 appliance:

- 160 GB removable solid-state drive that is used to store the NetScaler software.
- USB port (reserved for a future release).
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Non-maskable interrupt (NMI) button that is used at the request of Technical Support and produces a core dump on the NetScaler. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Two removable hard-disk drives that store user data.
- Disable alarm button. This button is functional only when the appliance has two power supplies.

  Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual power supplies, each rated at 850 watts, 110-220 volts.

For information about installing the rails, rack mounting the hardware, and connecting the cables, see "Installing the Hardware."

For information about performing initial configuration of your appliance, see "Initial Configuration."

Application Firewall Platforms

For information about the Application Firewall platforms, see Citrix NetScaler Application Firewall.

Summary of Hardware Specifications

The following tables summarize the specifications of the hardware platforms.

Table 1. MPX Platform Summary

	MPX 5500	MPX 5550/MPX 5650	MPX 7500/MPX 9500	MPX 15000
Processors	1 dual-core	1 quad-core	1 dual-core	2 quad-core
Memory	4 GB	8 GB	8 GB	16 GB
Ports - 1G	4x10/100/1000Base-T copper Ethernet ports	6x10/100/1000Base-T copper Ethernet ports	**8x10/100/1000Base-T copper Ethernet ports model**: 8x10/100/1000Base-T copper Ethernet ports **4x1G SFP + 4x10/100/1000Base-T copper Ethernet ports model**: 4xcopper/fiber 1G SFP ports, 4x10/100/1000Base-T copper Ethernet ports	8x10/100/1000Base-T copper Ethernet ports
Ports - 10G	NA	NA	NA	NA
Number of Power Supplies	1	1	1 with second optional	2
AC Power Supply input voltage, frequency, & current	100–240 VAC 50–60 Hz 3–1.5 A	100–240 VAC 50–60 Hz 2.5 A	100–240 VAC 50–60 Hz 3–1.5 A	100–240 VAC 47–63 Hz
Maximum Power Consumption	260 W	300 W	260 W	700 W
Heat Dissipation	887 BTU per hour	630 BTU per hour	887 BTU per hour	

Weight	22 lbs 9.98 kg	32 lbs 14.5 kg	23 lbs with one power supply 10.43 kg with one power supply	52 lbs 23.58 kg
Height	1U	1U	1U	2U
Width	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks
Depth	21.75 in or 55 cm	24.02 in or 61 cm	21.75 in or 55 cm	18.5 in or 47 cm
Operating Temperature	0–40° C 32–104° F	0–40° C 32–104° F	0–40° C 32–104° F	0–35° C 32–95° F
Humidity range (non-condensing)	5%–95%	5%–95%	5%–95%	5%–95%
Safety Certifications	CSA	CSA	CSA	UL & TUV-C
EMC & Susceptibility	FCC (Part 15 Class A), CE, C-Tick, CCC, KCC, NOM, PCT, VCCI, SASO, SABS	FCC (Part 15 Class A), CE, C-Tick, VCCI-A, CCC, KCC, NOM, SASO, SABS, PCT	FCC (Part 15 Class A), CE, C-Tick, CCC, KCC, NOM, PCT, VCCI, SASO, SABS	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES
Compliance	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE

Table 2. MPX Platform Summary (contd.)

	MPX 17000	MPX 8200/MPX 8400/MPX 8600/MPX 8800	MPX 9700/MPX 10500/MPX 12500/MPX 15500	MPX 11500/MPX 13500/MPX 14500/MPX 16500/MPX 18500/ MPX 20500
Processors	2 quad-core	1 quad-core	2 quad-core	2 six-core
Memory	32 GB	32 GB	16 GB	48 GB

Ports - 1G	**Ten network-port model:** 8x10/100/1000Base-T copper Ethernet ports	**6x1G SFP + 6x10/100/1000Base-T copper Ethernet model:** 6xcopper/fiber 1G SFP ports, 6x10/100/1000Base-T copper Ethernet ports **2x10G SFP+ 6x10/100/1000Base-T copper Ethernet model:** 6xcopper/fiber 1G SFP ports	8x10/100/1000 Base-T copper Ethernet ports, 8xcopper/fiber 1G SFP ports **10G and FIPS model:** 8xcopper/fiber 1G SFP ports	8x1G SFP ports
Ports - 10G	**Four network-port model:** 4x10G XFP ports **Ten network-port model:** 2x10G XFP ports	**2x10G SFP+ 6x10/100/1000Base-T copper Ethernet model:** 2x10G SFP+ Ports	**10G and FIPS model:** 2x10G SFP+ ports	4x10G SFP+ ports
Number of Power Supplies	2	1	2	2
AC Power Supply input voltage, frequency, & current	100–240 VAC 47–63 Hz	100–240 VAC 50–60 Hz 2.5 A	100–240 VAC 50–60 Hz 4.5–2.5 A	100–240 VAC 50–60 Hz 6.5–3.5 A
Maximum Power Consumption	700 W	450 W	450 W	650 W
Heat Dissipation		630 BTU per hour	1550 BTU per hour	2200 BTU per hour
Weight	52 lbs 23.59 kg	32 lbs 14.52 kg	31 lbs 14.06 kg	46 lbs 20.87 kg
Height	2U	1U	2U	2U
Width	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks

Depth	18.5 in or 47 cm	24.01 in or 61 cm	24.5 in or 62 cm	28 in or 71.68 cm
Operating Temperature	0–35° C 32–95° F	0–40° C 32–104° F	0–40° C 32–104° F	0–40° C 32–104° F
Humidity range (non-condensing)	5%–95%	5%–95%	5%–95%	5%–95%
Safety Certifications	UL & TUV-C	TUV	CSA	CSA
EMC & Susceptibility	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), CE, C-Tick, VCCI-A	FCC (Part 15 Class A), CE, C-Tick, KCC, NOM, PCT, VCCI, SASO, SABS	FCC (Part 15 Class A), CE, C-Tick, VCCI, CCC, KC, NOM, GOST, SABS, SASO
Compliance	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE	RoHS, SVHC, WEEE

Table 3. MPX Platform Summary (contd.)

	MPX 17500/MPX 19500/MPX 21500	MPX 17550/MPX 19550/MPX 20550/MPX 21550
Processors	2 six-core	2 six-core
Memory	48 GB	96 GB
Ports - 1G	NA	NA
Ports - 10G	8x10G SFP+ ports	8x10G SFP+ ports
Number of Power Supplies	2	2
AC Power Supply input voltage, frequency, & current	100–240 VAC 50–60 Hz 6.5–3.5 A	100–240 VAC 50–60 Hz 6.5–3.5 A
Maximum Power Consumption	650 W	850 W
Heat Dissipation	2200 BTU per hour	2900 BTU per hour
Weight	40 lbs 18.14 kg	40 lbs 18.14 kg
Height	2U	2U
Width	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks
Depth	24.75 in or 62.865 cm	24.75 in or 62.865 cm

Operating Temperature	0–40° C 32–104° F	0–40° C 32–104° F
Humidity range (non-condensing)	5%–95%	5%–95%
Safety Certifications	TUV	TUV
EMC & Susceptibility	FCC (Part 15 Class A), CE, C-Tick, VCCI-A	FCC (Part 15 Class A), CE, C-Tick, VCCI-A
Compliance	RoHS, WEEE	RoHS, WEEE

Preparing for Installation

Before you install your new appliance, carefully unpack your appliance and make sure that all parts were delivered. Once you are satisfied that your appliance has been delivered to your expectations, verify that the location where the appliance will be installed meets temperature and power requirements and that the server cabinet or floor-to-ceiling cabinet is securely bolted to the floor and has sufficient airflow.

Only trained and qualified personnel should install, maintain, or replace the appliance, and efforts should be taken to ensure that all cautions and warnings are followed.

Unpacking the Appliance

The hardware accessories for your particular appliance, such as cables, adapters, and rail kit, vary depending on the hardware platform you ordered. Unpack the box that contains your new appliance on a sturdy table with plenty of space and inspect the contents.

Use the following list to verify that you received everything that should have been included in the box.

- The appliance you ordered
- One RJ-45 to DB-9 adapter
- One 6 ft RJ-45/DB-9 cable
- The following list specifies the number of power cables included for each appliance model:
  - One power cable for the MPX 5500, MPX 5550/5650, MPX 7500/9500, and MPX 8200/8400/8600/8800 appliances
  - Two power cables for the MPX 15000, MPX 17000, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances

  Note: For Brazilian customers, Citrix does not ship a power cable. Use a cable that conforms to the **ABNT NBR 14136:2002** standard.
- One standard 4-post rail kit

  Note: If the kit that you received does not fit your rack, contact your Citrix sales representative to order the appropriate kit.

In addition to the items included in the box with your new appliance, you will need the following items to complete the installation and initial configuration process.

- Ethernet cables for each additional Ethernet port that you will connect to your network
- One available Ethernet port on your network switch or hub for each NetScaler Ethernet port you want to connect to your network

  Note: Transceiver modules are sold separately. Contact your Citrix sales representative to order transceiver modules for your appliance. Only transceivers supplied by Citrix are supported on the appliance.
- A computer to serve as a management workstation

Preparing the Site and Rack

There are specific site and rack requirements for the NetScaler appliance. You must make sure that adequate environmental control and power density are available. Racks must be bolted to the ground, have sufficient airflow, and have adequate power and network connections. Preparing the site and rack are important steps in the installation process and help ensure a smooth installation.

Site Requirements

The appliance should be installed in a server room or server cabinet with the following features:

Environment control

An air conditioner, preferably a dedicated computer room air conditioner (CRAC), capable of maintaining the cabinet or server room at a temperature of no more than 27 degrees C/80.6 degrees F at altitudes of up to 2100 m/7000 ft, or 18 degrees C/64.4 degrees F at higher altitudes, a humidity level no greater than 45 percent, and a dust-free environment.

Power density

Wiring capable of handling at least 4,000 watts per rack unit in addition to power needs for the CRAC.

Rack Requirements

The rack on which you install your appliance should meet the following criteria:

Rack characteristics

Racks should be either integrated into a purpose-designed server cabinet or be the floor-to-ceiling type, bolted down at both top and bottom to ensure stability. If you have a cabinet, it should be installed perpendicular to a load-bearing wall for stability and sufficient airflow. If you have a server room, your racks should be installed in rows spaced at least 1 meter/3 feet apart for sufficient airflow. Your rack must allow your IT personnel unfettered access to the front and back of each server and to all power and network connections.

Power connections

At minimum, two standard power outlets per unit.

Network connections

At minimum, four Ethernet connections per rack unit.

Space requirements

One empty rack unit for the Citrix NetScaler MPX 5500, MPX 5550/5650, MPX 7500/9500, and MPX 8200/8400/8600/8800, and two consecutive empty rack units for all other appliance models.

Note: You can order the following rail kits separately.

- Compact 4-post rail kit, which fits racks of 23 to 33 inches.
- 2-post rail kit, which fits 2-post racks.

Cautions and Warnings

Electrical Safety Precautions

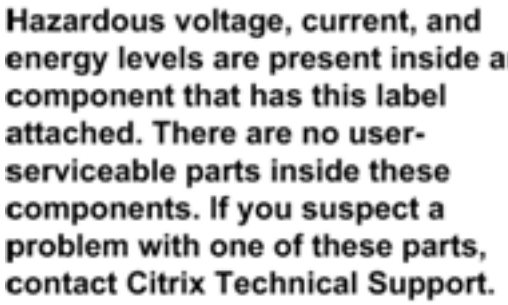
Caution: During installation or maintenance procedures, wear a grounding wrist strap to avoid ESD damage to the electronics of the appliance. Use a conductive wrist strap attached to a good earth ground or to the appliance. You can attach it to the connector beside the ESD symbol on the back.

Follow basic electrical safety precautions to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch, so that you can quickly remove power to the appliance if an electrical accident occurs.
- Remove all jewelry and other metal objects that might come into contact with power sources or wires before installing or repairing the appliance. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and may cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.
- Use a regulating, uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Never stack the appliance on top of any other server or electronic equipment.
- All appliances are designed to be installed on power systems that use TN earthing. Do not install your device on a power system that uses either TT or IT earthing.
- Make sure that the appliance has a direct physical connection to the earth during normal use. When installing or repairing an appliance, always make sure that the ground circuit is connected first and disconnected last.
- Make sure that a fuse or circuit breaker no larger than 120 VAC, 15 A U.S. (240 VAC, 16 A international) is used on all current-carrying conductors on the power system to which your appliances are connected.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, first shut down the appliance, and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages can be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload. Always unplug any appliance before

performing repairs or upgrades.

- Do not overload the wiring in your server cabinet or on your server room rack.
- During thunderstorms, or anticipated thunderstorms, avoid performing any hardware repairs or upgrades until the danger of lightning has passed.
- When you dispose of an old appliance or any components, follow any local and national laws on disposal of electronic waste.
- To prevent possible explosions, replace expired batteries with the same model or a manufacturer-recommended substitute and follow the manufacturer's instructions for battery replacement.
- Never remove a power supply cover or any sealed part that has the following label:



Appliance Precautions

- Determine the placement of each component in the rack before you install the rail.
- Install the heaviest appliance first, at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.
- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near an electrical outlet for easy access.
- Mount equipment in a rack with sufficient airflow for safe operation.
- For a closed or multiple-unit rack assembly, the ambient operating temperature of the rack environment might be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously might cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should be used only for extending the appliance out of the rack. Do not use these handles for mounting the appliance on the rack. Use the rack-rail hardware, described later, instead.

Installing the Hardware

After you have determined that the location where you will install your appliance meets the environmental standards and the server rack is in place according to the instructions, you are ready to install the hardware. After you mount the appliance, you are ready to connect it to the network, to a power source, and to the console terminal that you will use for initial configuration. To complete the installation, you turn on the appliance. Be sure to observe the cautions and warnings listed with the installation instructions.

Rack Mounting the Appliance

Most appliances can be installed in standard server racks that conform to EIA-310-D specification. The appliances ship with a set of rails, which you must install before you mount the appliance. The only tools that you need for installing an appliance are a Phillips screwdriver and a flathead screwdriver.

Caution: If you are installing the appliance as the only unit in the rack, mount it at the bottom. If the rack contains other units, make sure that the heaviest unit is at the bottom. If the rack has stabilizing devices available, install them before mounting the appliance.

The following table lists the different hardware platforms and the rack units required for each platform.

Table 1. *Height Requirements For Each Platform*

Platform	Number of rack units
MPX 5500	One rack unit
MPX 5550/5650	One rack unit
MPX 7500/9500	One rack unit
MPX 8200/8400/8600/8800	One rack unit
MPX 9700/10500/12500/15500	Two rack units
MPX 15000, MPX 17000	Two rack units
MPX 11500/13500/14500/16500/18500/20500	Two rack units
MPX 17500/19500/21500	Two rack units
MPX 17550/19550/20550/21550	Two rack units

Each appliance ships with a mounting rail kit that contains two rail assemblies, one for the left side and the other for the right side of the appliance, and screws to attach the rails. An assembly consists of an inner rail and a rack rail. The supplied rail kit is 28 inches long (38 inches extended). Contact your Citrix sales representative to order a 23-inch (33 inches extended) rail kit.

Note: The same rail kit is used for both square-hole and round-hole racks. See "Installing the Rail Assembly to the Rack" for specific instructions for threaded, round-hole racks.

To mount the appliance, you must first install the rails and then install the appliance in the rack.

Perform the following tasks to mount the appliance:

- Remove the inner rails from the rail assembly.
- Attach the inner rails to the appliance.
- Install the rack rails on the rack.

- Install the appliance in the rack.

The appliance is shipped with rack-rail hardware. This hardware consists of two inner rails that you attach to the appliance, one on each side, and a rack-rail assembly that you attach to the rack. The following figure illustrates the steps involved in mounting the Citrix NetScaler appliance to a rack.

To remove the inner rails from the rail assembly

1. Place the rail assembly on a flat surface.
2. Slide out the inner rail toward the front of the assembly.
3. Depress the latch until the inner rail comes all the way out of the rail assembly.
4. Repeat steps 1 through 3 to remove the second inner rail.

To attach the inner rails to the appliance

1. Position the right inner rail behind the handle on the right side of the appliance.
2. Align the holes on the rail with the corresponding holes on the side of the appliance.
3. Attach the rail to the appliance with the provided screws: 4 per side for a 1U appliance and 5 per side for a 2U appliance, as shown in the following figure.

Figure 1. Attaching inner rails

4. Repeat steps 1 through 3 to install the left inner rail on the other side of the appliance.

To install the rack rails on the rack

1. If you have a round-hole, threaded rack, skip to step 3.

2. Install square nut retainers into the front post and back post of the rack as shown in the following figures. Before inserting a screw, be sure to align the square nut with the correct hole for your 1U or 2U appliance. The three holes are not evenly spaced.

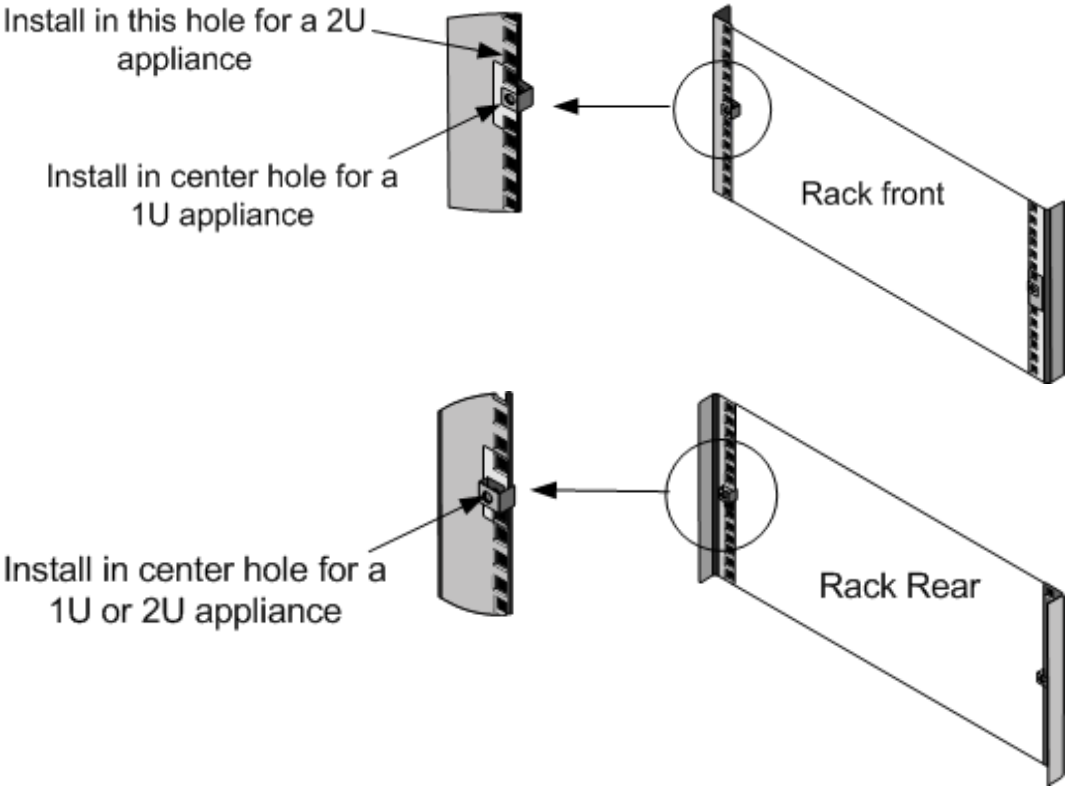


Figure 2. Installing Retainers into the Front Rack Posts Figure 3. Installing Retainers into the Rear Rack Posts

3. Install the adjustable rail assembly into the rack as shown in the following figures. Use a screw to lock the rear rail flange into the rack. With the screw securing the rail in place, you can optionally remove the latching spring.

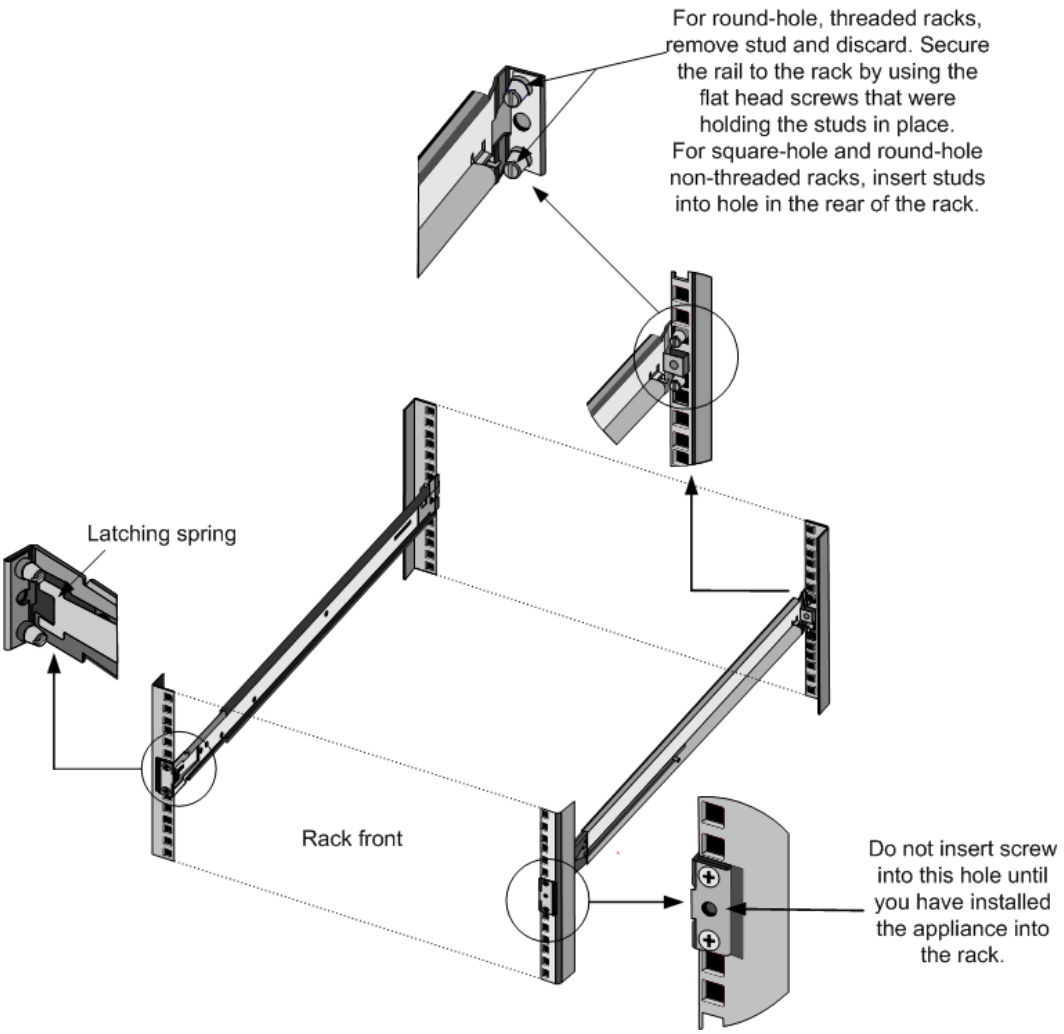


Figure 4. Installing the Rail Assembly to the Rack

To install the appliance in the rack

1. Align the inner rails, attached to the appliance, with the rack rails.
2. Slide the appliance into the rack rails, keeping the pressure even on both sides.
3. Verify that the appliance is locked in place by pulling it all the way out from the rack.

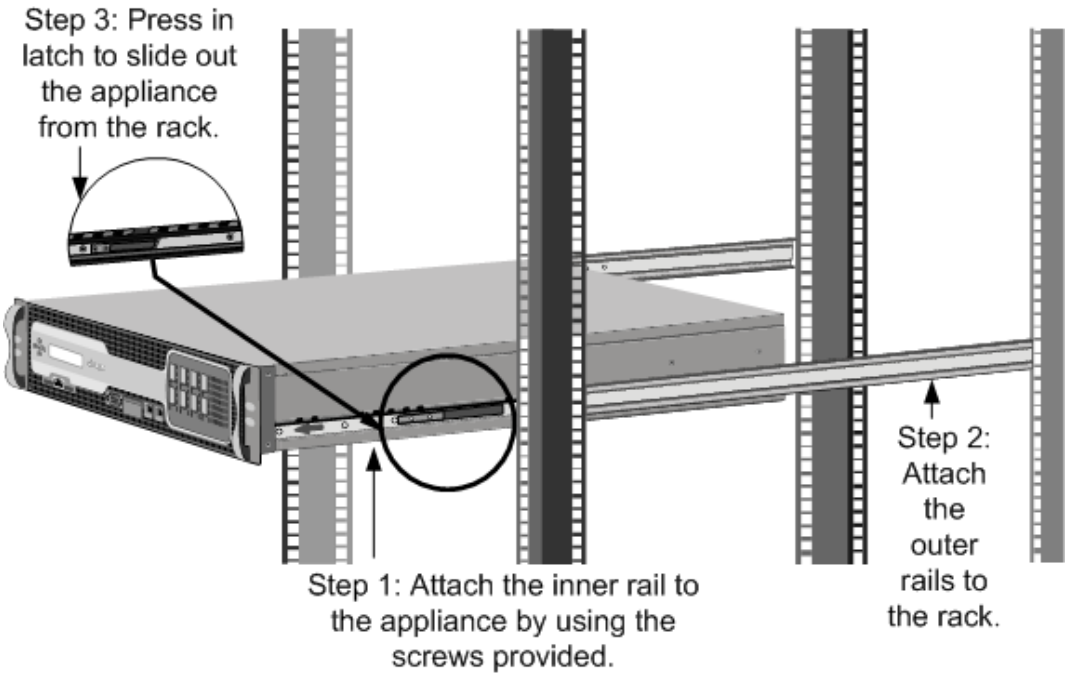


Figure 5. Rack Mounting the Appliance

Installing and Removing 1G SFP Transceivers

Note: This section applies to the MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, and MPX 11500/13500/14500/16500/18500/20500 appliances.

A Small Form-Factor Pluggable (SFP) is a compact transceiver that can operate at speeds of up to 1 gigabit per second and is available in both copper and fiber types. Inserting a 1G SFP copper transceiver converts the 1G SFP port to a 1000BASE-T port. Inserting a 1G SFP fiber transceiver converts the 1G SFP port to a 1000BASE-X port. Auto-negotiation is enabled by default on the 1G SFP port into which you insert your 1G SFP transceiver. As soon as a link between the port and the network is established, the speed and mode are matched on both ends of the cable.

Note: The 1G SFP transceiver is hot-swappable from release 9.3 build 42.2 and later on the NetScaler appliances that use the e1k interface. The following platforms support 1G SPF transceivers:

- MPX 7500/9500
- MPX 8200/8400/8600/8800
- MPX 9700/10500/12500/15500
- MPX 11500/13500/14500/16500/18500/20500

Caution: NetScaler appliances do not support 1G SFP transceivers from vendors other than Citrix Systems. Attempting to install third-party 1G SFP transceivers on your NetScaler appliance voids the warranty.

Insert 1G SFP transceivers into the 1G SFP ports on the front panel of the appliance. Frequent installation and removal of transceivers shortens their life span. Follow the removal procedure carefully to avoid damaging the 1G SFP transceiver or the appliance.

Caution: Do not install the transceivers with the cables attached. Doing so can damage the cable, the connector, or the optical interface of the transceiver.

To install a 1G SFP transceiver

1. Remove the 1G SFP transceiver carefully from its box.

   Danger: Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.

2. Align the 1G SFP transceiver to the front of the 1G SFP transceiver port on the front panel of the appliance, as shown in the following figure.

   Note: The illustration in the following figures might not represent your actual appliance.

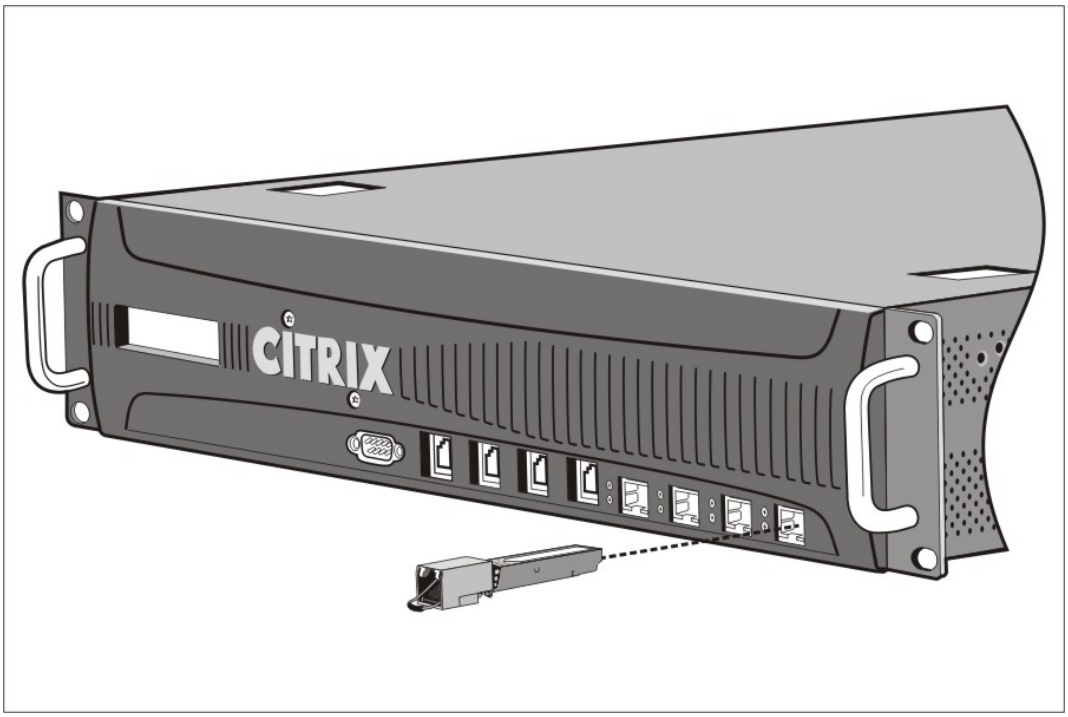


Figure 1. Installing a 1G SFP transceiver

3. Hold the 1G SFP transceiver between your thumb and index finger and insert it into the 1G SFP transceiver port, pressing it in until you hear the transceiver snap into place.

4. Lock the transceiver.

5. Verify that the LED is green and blinks twice, which indicates that the transceiver is functioning correctly.

6. If you are using a fiber 1G SFP transceiver, do not remove the dust caps attached to the transceiver and the cable until you are ready to insert the cable.

To remove a 1G SFP transceiver

1. Disconnect the cable from the 1G SFP transceiver. If you are using a fiber optic cable, replace the dust cap on the cable before putting it away.

   Danger: Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.

2. Unlock the 1G SFP transceiver.

3. Hold the 1G SFP transceiver between your thumb and index finger and slowly pull it out of the port.

4. If you are removing a fiber 1G SFP transceiver, replace the dust cap before putting it away.

5. Put the 1G SFP transceiver into its original box or another appropriate container.

Installing and Removing XFP and 10G SFP+ Transceivers

Note: This section applies to the MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, MPX 15000, MPX 17000, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances.

A 10-Gigabit Small Form-Factor Pluggable (XFP or SFP+) is a compact optical transceiver that can operate at speeds of up to 10 gigabits per second. The MPX 15000 and MPX 17000 appliances use XFP transceivers and the MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances use 10G SFP+ transceivers. Autonegotiation is enabled by default on the XFP/10G SFP+ ports into which you insert your XFP/10G SFP+ transceiver. As soon as a link between the port and the network is established, the mode is matched on both ends of the cable and for 10G SFP+ transceivers, the speed is also autonegotiated.

Note: An XFP transceiver is **not hot-swappable** on the NetScaler appliances. You must restart a NetScaler appliance after you insert an XFP transceiver.

However, the 10G SFP+ transceiver is hot-swappable from release 9.3 build 57.5 and later on the NetScaler appliances that use the ixgbe (ix) interface. The following platforms support 10G SPF+ transceivers:

- MPX 8200/8400/8600/8800
- MPX 9700/10500/12500/15500 10G and 10G FIPS
- MPX 11500/13500/14500/16500/18500/20500
- MPX 17500/19500/21500
- MPX 17550/19550/20550/21550

The following platforms support XFP transceivers:

- MPX 15000
- MPX 17000

Caution: NetScaler appliances do not support XFP/10G SFP+ transceivers provided by vendors other than Citrix Systems. Attempting to install third-party XFP/10G SFP+ transceivers on your NetScaler appliance voids the warranty.

Insert the XFP/10G SFP+ transceivers into the XFP/10G SFP+ ports on the front panel of the appliance. Frequent installation and removal of transceivers shortens their life span. Follow the removal procedure carefully to avoid damaging the transceiver or the appliance.

Caution: Do not install the transceivers with the cables attached. Doing so can damage the cable, the connector, or the optical interface of the transceiver.

To install an XFP/10G SFP+ transceiver

1. Remove the XFP/10G SFP+ transceiver carefully from its box.

   Danger: Do not look directly into fiber optic transceivers and cables. They emit laser beams that can damage your eyes.

2. Align the XFP/10G SFP+ transceiver to the front of the XFP/10G SFP+ transceiver port on the front panel of the appliance.

3. Hold the XFP/10G SFP+ transceiver between your thumb and index finger and insert it into the XFP/10G SFP+ transceiver port, pressing it in until you hear the transceiver snap into place.

4. Move the locking hinge to the DOWN position as shown in the following figure.

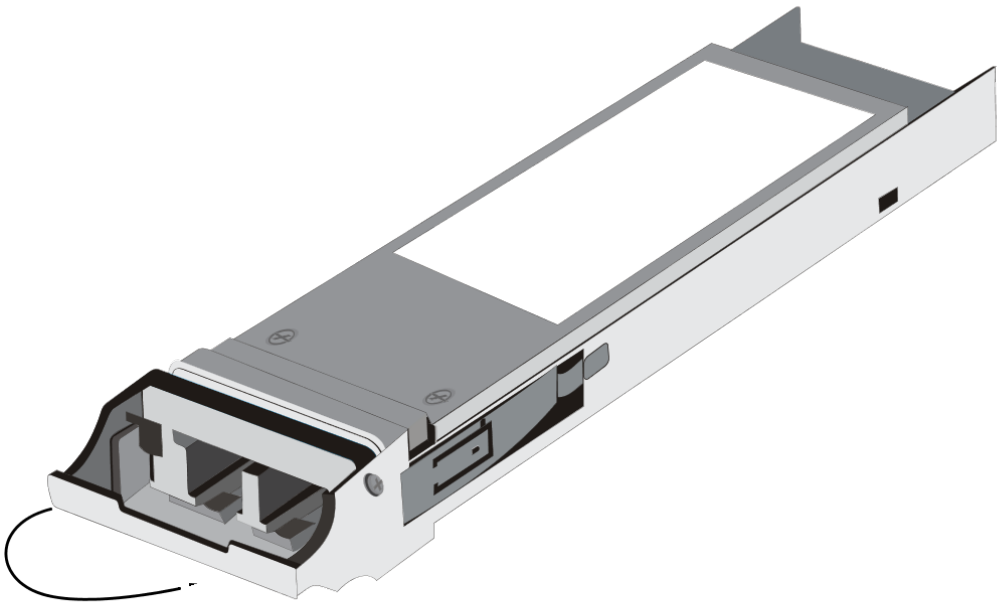


Figure 1. Locking an XFP transceiver

5. Verify that the LED is green and blinks twice, which indicates that the transceiver is functioning correctly.

6. Do not remove the dust caps attached to the transceiver and cable until you are ready to insert the cable.

To remove an XFP/10G SFP+ transceiver

1. Disconnect the cable from the XFP/10G SFP+ transceiver. Replace the dust cap on the cable before putting it away.

   Danger: Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.

2. Unlock the XFP/10G SFP+ transceiver by moving the locking hinge to the UP position.

3. Hold the XFP/10G SFP+ transceiver between your thumb and index finger and slowly pull it out of the port.

4. Replace the dust cap on the transceiver before putting it away.

5. Put the XFP/10G SFP+ transceiver into its original box or another appropriate container.

Connecting the Cables

When the appliance is securely mounted on the rack, you are ready to connect the cables. Ethernet cables and the optional console cable are connected first. Connect the power cable last.

Danger: Before installing or repairing the appliance, remove all jewelry and other metal objects that might come in contact with power sources or wires. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.

Connecting the Ethernet Cables

Ethernet cables connect your appliance to the network. The type of cable you need depends on the type of port used to connect to the network. Use a category 5e or category 6 Ethernet cable with a standard RJ-45 connector on a 10/100/1000BASE-T port or 1G SFP copper transceiver. Use a fiber optic cable with an LC duplex connector with a 1G SFP fiber transceiver, 10G SFP+, or XFP transceiver. The type of connector at the other end of the fiber optic cable depends on the port of the device that you are connecting to.

To connect an Ethernet cable to a 10/100/1000BASE-T port or 1G SFP copper transceiver

1. Insert the RJ-45 connector on one end of your Ethernet cable into an appropriate port on the front panel of the appliance, as shown in the following figure.

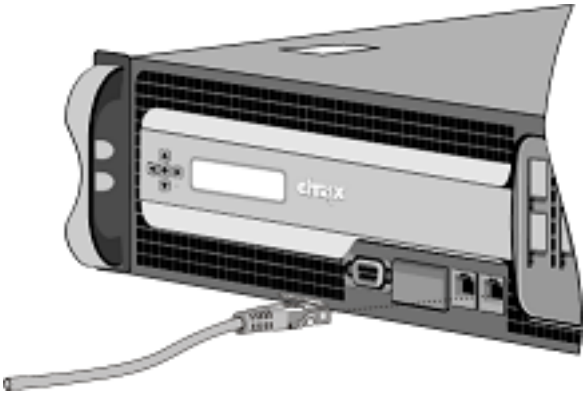


Figure 1. Inserting an Ethernet cable

2. Insert the RJ-45 connector on the other end into the target device, such as a router or switch.

3. Verify that the LED glows amber when the connection is established.

To connect the Ethernet cable to a 1G SFP fiber, 10G SFP+, or XFP transceiver

1. Remove the dust caps from the transceiver and cable.
2. Insert the LC connector on one end of the fiber optic cable into the appropriate port on the front panel of the appliance.
3. Insert the connector on the other end into the target device, such as a router or switch.
4. Verify that the LED glows amber when the connection is established.

Connecting the Console Cable

You can use the console cable to connect your appliance to a computer or terminal, from which you can configure the appliance. Alternatively, you can use a computer connected to the network. Before connecting the console cable, configure the computer or terminal to support VT100 terminal emulation, 9600 baud, 8 data bits, 1 stop bit, parity, and flow control set to NONE. Then connect one end of the console cable to the RS232 serial port on the appliance and the other end to the computer or terminal.

To connect the console cable to a computer or terminal

1. Insert the DB-9 connector at the end of the cable into the console port that is located on the front panel of the appliance, as shown in the following figure.

   Figure 2. Inserting a console cable

   Note: To use a cable with an RJ-45 converter, insert the optional converter provided into the console port and attach the cable to it.

2. Insert the RJ-45 connector at the other end of the cable into the serial port of the computer or terminal.

Connecting the Power Cable

An MPX 5500, MPX 5550/5650, MPX 7500/9500, and MPX 8200/8400/8600/8800 appliance has one power cable. All the other appliances come with two power cables, but they can also operate if only one power cable is connected. A separate ground cable is not required, because the three-prong plug provides grounding.

To connect the appliance to the power source

1. Connect one end of the power cable to the power outlet on the back panel of the appliance, next to the power supply, as shown in the following figure.

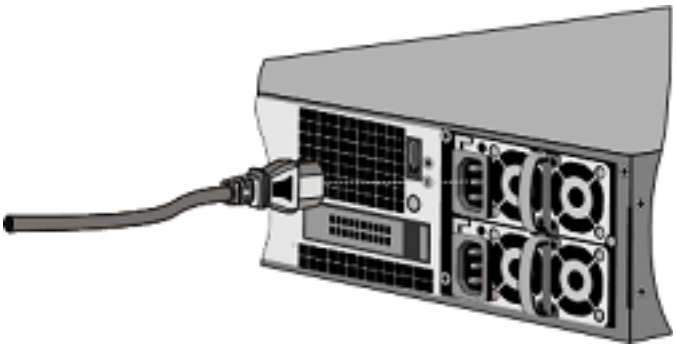


Figure 3. Inserting a power cable

2. Connect the other end of the power cable to a standard 110V/220V power outlet.

3. If a second power supply is provided, repeat steps 1 and 2 to connect the second power supply.

Note: The MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliance emit a high-pitched alert if one power supply fails or if you connect only one power cable to the appliance. To silence the alarm, you can press the small red button located on the back panel of the appliance.

Switching on the Appliance

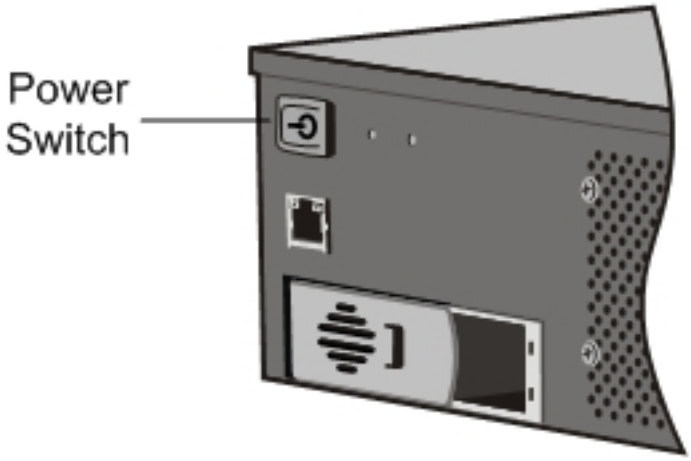
After you have installed the appliance in a rack and connected the cables, verify that the power cable is properly connected. If you have installed a second power supply, make sure the second cable is connected to an outlet for a different circuit than the first. After verifying the connections, you are ready to switch on the appliance.

To switch on the appliance

1. Verify that the appliance is connected through a console or Ethernet port. This will ensure that you can configure the appliance after it is switched on.

2. Press the ON/OFF toggle power switch on the back panel of the appliance.

Figure 1. Power switch on back panel



3. Verify that the LCD on the front panel is backlit and the start message appears, as shown in the following figure.

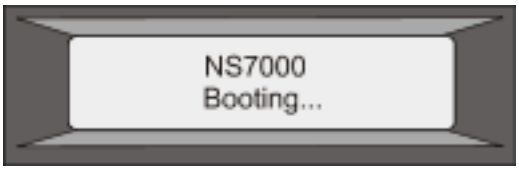


Figure 2. LCD startup screen

Caution: Be aware of the location of the emergency power off (EPO) switch, so that if an electrical accident occurs you can quickly remove power from the appliance.

Initial Configuration

After you have installed your appliance in a rack, you are ready to perform the initial configuration. Once initial configuration is complete, refer to the specific configuration guides for the features you will be using.

Initial configuration is the same for the multifunction Citrix NetScaler, the dedicated Access Gateway Enterprise Edition, and the dedicated Citrix® Application Firewall™ appliances. To perform the initial configuration on the MPX 5500, MPX 5550/5650, MPX 7500/9500, MPX 8200/8400/8600/8800, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances, you can also use the LCD keypad on the front panel of the appliance. To perform the initial configuration, you can use the serial console or the setup wizard. You can access the setup wizard from any computer that is on the same network as the new NetScaler appliance. However, because this method uses the NetScaler default IP address, you must install and configure one NetScaler appliance at a time. If you want to configure a new appliance from a remote network, or if you want to install multiple NetScaler appliances and then configure them without using the console port, you can use Dynamic Host Configuration Protocol (DHCP) to assign each new appliance an IP address at which you can access the appliance for remote configuration.

For initial configuration, use nsroot as both the administrative user name and the password. For subsequent access, use the password assigned during initial configuration.

After you complete the initial configuration of the appliance, you can configure secure access to your appliance. As a result, you are no longer prompted for a password when logging on. This is especially helpful in environments for which you would otherwise have to keep track of a large number of passwords.

Using the LCD Keypad

When you first install the appliance, you can configure the initial settings by using the LCD keypad on the front panel of the appliance. The keypad interacts with the LCD display module, which is also on the front panel of these appliances.

Note: You can use the LCD keypad for initial configuration on a new appliance with the default configuration. The configuration file (ns.conf) should contain the following command and default values.

set ns config -IPAddress 192.168.100.1 -netmask 255.255.0.0

The functions of the different keys are explained in the following table.

Table 1. LCD Key Functions

Key	Function
<	Moves the cursor one digit to the left.
>	Moves the cursor one digit to the right.
^	Increments the digit under the cursor.
v	Decrements the digit under the cursor.
.	Processes the information, or terminates the configuration, if none of the values are changed. This key is also known as the ENTER key.

To perform the initial configuration by using the LCD keypad press the "<" key.

You are prompted to enter the subnet mask, NetScaler IP address (NSIP), and gateway in that order respectively. The subnet mask is associated with both the NSIP and default gateway IP address. The NSIP is the IPv4 address of the NetScaler appliance. The default gateway is the IPv4 address for the router, which will handle external IP traffic that the NetScaler cannot otherwise route. The NSIP and the default gateway should be on the same subnet.

If you enter a valid value for the subnet mask, such as 255.255.255.224, you are prompted to enter the IP address. Similarly, if you enter a valid value for the IP address, you are prompted to enter the gateway address. If the value you entered is invalid, the following error message appears for three seconds, where xxx.xxx.xxx.xxx is the IP address you entered, followed by a request to re-enter the value.

Invalid addr!
xxx.xxx.xxx.xxx

If you press the ENTER (.) key without changing any of the digits, the software interprets this as a user exit request. The following message will be displayed for three seconds.

Exiting menu...
xxx.xxx.xxx.xxx

If all the values entered are valid, when you press the ENTER key, the following message appears.

Values accepted,
Rebooting...

The subnet mask, NSIP, and gateway values are saved in the configuration file.

Note: For information about deploying a high availability (HA) pair, see "Configuring High Availability."

Using the NetScaler Serial Console

When you first install the appliance, you can configure the initial settings by using the serial console. With the serial console, you can change the system IP address, create a subnet or mapped IP address, configure advanced network settings, and change the time zone.

Note: To locate the serial console port on your appliance, see "RS232 Serial Console Port" in "Ports."

To configure initial settings by using a serial console

1. Connect the console cable into your appliance. For more information, see "Connecting the Console Cable" in "Connecting the Cables."

2. Run the vt100 terminal emulation program of your choice on your computer to connect to the appliance and configure the following settings: 9600 baud, 8 data bits, 1 stop bit, parity, and flow control set to NONE.

3. Press ENTER. The terminal screen displays the Logon prompt.

   Note: You might have to press ENTER two or three times, depending on which terminal program you are using.

4. Log on to the appliance with the administrator credentials. Your sales representative or Citrix Customer Service can provide you with the administrator credentials.

5. At the prompt, type config ns to run the NetScaler configuration script.

6. To complete the initial configuration of your appliance, follow the prompts.

   Note: To prevent an attacker from breaching your ability to send packets to the appliance, choose a non-routable IP address on your organization's LAN as your appliance IP address.

   You can replace steps 5 and 6 with the following NetScaler commands. At the NetScaler command prompt, type:

   set ns config -ipaddress<IPAddress> -netmask<subnetMask>

   add ns ip<IPAddress> <subnetMask> -type<type>

   add route<network> <netmask> <gateway>

   set system user <userName> -password

   save ns config

   reboot

   Example

   ```
   set ns config -ipaddress 10.102.29.60 -netmask 255.255.255.0
   add ns ip 10.102.29.61 255.255.255.0 -type snip
   add route 0.0.0.0 0.0.0.0 10.102.29.1
   set system user nsroot -password
   Enter password: *****
   Confirm password: *****
   save ns config
   reboot
   ```

   You have now completed initial configuration of your appliance. To continue configuring the appliance, choose one of the following options:

Citrix NetScaler.

If you are configuring your appliance as a standard NetScaler with other licensed features, see "Load Balancing."

Citrix® Application Firewall™.

If you are configuring your appliance as a standalone application firewall, see "Application Firewall."

Access Gateway.

If you are configuring your appliance as an Access Gateway, see "Access Gateway 10."

Note: For information about deploying a high availability (HA) pair, see "Configuring High Availability."

Using the Setup Wizard

To configure the appliance by using the Setup Wizard in the configuration utility, you need an administrative computer configured on the same network as the appliance. To run the configuration utility, the Java RunTime Environment (JRE) version 1.4.2_04 or later must be installed on the workstation or laptop. You can use the Setup Wizard to configure the following initial settings on the appliance:

- System IP address and subnet mask
- Subnet or Mapped IP address and subnet mask
- Host name
- Default gateway
- Time zone
- Licenses
- Administrator password

Important: Before running the Setup Wizard, you should download your licenses from the Citrix Web site and put them in a location on your computer or another device where you can access them from your Web browser during configuration.

Note: If the appliance is configured with the default IP address, licenses are not installed on the appliance, or the mapped or subnet IP address is not configured, the configuration utility automatically opens the Setup Wizard when you log on to the appliance.

To configure initial settings by using the Setup Wizard

1. In a Web browser, type: `http://192.168.100.1`

   Note: The NetScaler software is preconfigured with a default IP address and associated netmask. The default IP address is 192.168.100.1 and the default netmask is 255.255.0.0.

2. In User Name and Password, type the administrator credentials. You can obtain the initial user name and password from your sales representative or from Citrix Customer Service.

3. In Start in, select Configuration, and then click Login.

4. In the Setup Wizard, click Next, and then follow the instructions in the wizard.

   Note: To prevent an attacker from breaching your ability to send packets to the appliance, choose a non-routable IP address on your organization's LAN as your appliance IP address.

You have now completed initial configuration of your appliance. To continue configuring the appliance, choose one of the following options:

Citrix NetScaler.

If you are configuring your appliance as a standard NetScaler with other licensed features, see "Load Balancing."

Citrix® Application Firewall™.

If you are configuring your appliance as a standalone application firewall, see "Application Firewall."

Access Gateway.

If you are configuring your appliance as an Access Gateway, see "Access Gateway 10."

Note: For information about deploying a high availability (HA) pair, see "Configuring High Availability."

Using DHCP for Initial Access

Note: The terms NetScaler, NetScaler appliance, and appliance are used interchangeably.

For initial configuration of a NetScaler appliance, Dynamic Host Configuration Protocol (DHCP) can eliminate dependency on the console by providing a subnet IP (SNIP) address at which you can access the appliance to configure it remotely. You can also use DHCP after initial configuration if, for example, you want to move a NetScaler to a different subnet.

To use DHCP, you must first specify the NetScaler vendor class identifier on a DHCP server. Optionally, you can also specify the pool of IP addresses from which your NetScaler appliance can acquire an IP address. If a pool is not specified, the address is acquired from the general pool.

A new NetScaler appliance does not have a configuration file. When you connect an appliance without a configuration file to the network, its DHCP client automatically polls the DHCP server for an IP address. If you have specified the NetScaler vendor class identifier on the DHCP server, the server returns an address. You can also enable the DHCP client on a previously configured appliance.

Prerequisites

To use DHCP, you must:

1. Note the system ID (sysid) on the serial number sticker on the back panel of the appliance. On an older appliance, the system ID may not be available. In this case, use the MAC address instead of the system ID.

2. Set up a DHCP server and configure it with the NetScaler vendor class identifier.

To configure a Linux/UNIX DHCP server for the NetScaler appliance

1. Specify "citrix-NS" as the vendor class identifier for the NetScaler appliance by adding the following configuration to the server's dhcpd.conf file. The subclass declaration must be inside the subnet declaration.

   ```
   option space auto;
    option auto.key code 1 = text;

   class "citrix-1" {
    match option vendor-class-identifier;
   }

   subclass "citrix-1" "citrix-NS"{
   vendor-option-space auto;
   option auto.key "citrix-NS";
   ```

   Note: The location of the dhcpd.conf file can be different in different versions and flavors of the Linux/UNIX-based operating system (for example, in FreeBSD 6.3 the file is present in the /etc/ folder). For the location, see the `dhcpd` man page of the DHCP server.

2. If you do not want NetScaler appliances to use IP addresses from the general pool, specify a pool of addresses for the appliance. You must include this pool declaration inside the subnet declaration. For example, adding the following configuration to the dhcpd.conf file specifies a pool of IP addresses ranging from 192.168.2.120 to 192.168.2.127.

   ```
   pool {
   allow members of "citrix-1";
   range 192.168.2.120 192.168.2.127;
   option subnet-mask 255.255.255.0;
   }
   ```

3. Terminate the DHCP process and restart it to reflect the change to the configuration file. At the shell prompt, type:

   ```
   killall dhcpd

   dhcpd&
   ```

Sample DHCP configuration (dhcpd.conf)

```
option space auto;
option auto.key code 1 = text;

class "citrix-1" {
    match option vendor-class-identifier;
}

subnet 192.168.2.0 netmask 255.255.255.0 {
```

```
option routers10.217.242.1;
option domain-name"jeffbr.local";
option domain-name-servers8.8.8.8;
default-lease-time 21600;
max-lease-time 43200;
subclass "citrix-1" "citrix-NS" {
vendor-option-space auto;
option auto.key "citrix-NS";
}
pool {
allow members of "citrix-1";
range 192.168.2.120 192.168.2.127;
option subnet-mask 255.255.255.0;
}
}
```

Implementing an Initial NetScaler Configuration from a Remote Computer

When a new NetScaler appliance (or any appliance that does not have a configuration file) starts, it automatically polls the DHCP server for an IP address and provides the DHCP server with its sysid. The DHCP server selects one IP address from its pool and assigns it as a subnet IP (SNIP) address to the appliance. The DHCP server includes the sysid of the appliance and the IP address that it assigns to the appliance in the server's dhcpd.leases file. To find the IP address currently assigned to your appliance, look in the dhcpd.leases file for the last entry with the sysid of your appliance in the uid or client-hostname field. Verify that the binding state in this entry is active. If the binding state is not active but free, the IP address is not yet associated with the appliance.

You can use this address to connect to the appliance and remotely configure the initial settings. For example, you can change the IP address, subnet mask, and gateway settings that were fetched from the DHCP server. After completing the initial configuration, you can manually return the DHCP IP address to the server pool. Alternatively, restarting the appliance automatically releases the DHCP IP address back to the server pool.

You can find out the SNIP address assigned to the appliance from the NetScaler console or from the DHCP server.

To find the SNIP address from the NetScaler console

At the console prompt, type:

```
> sh dhcpParams
DHCP Client on next reboot is ON
DHCP Client Current State: Active
DHCP Client Default route save: OFF
DHCP acquired IP:192.168.2.127
DHCP acquired Netmask:255.255.255.0
DHCP acquired Gateway:192.168.2.1
```

Done

To find the SNIP address from the DHCP server

Look in the dhcpd.leases file for the last entry with the sysid of your appliance in the uid or client-hostname field.

Example: The following entry in a DHCP server's dhcpd.leases file verifies the binding state of the appliance whose sysid is 45eae1a8157e89b9314f.

```
lease 192.168.2.127 {
  starts 3 2013/08/19 00:40:37;
  ends 3 2013/08/19 06:40:37;
  cltt 3 2013/08/19 00:40:37;
  binding state active;
  next binding state free;
  hardware ethernet 00:d0:68:11:f4:d6;
  uid "45eae1a8157e89b9314f";
  client-hostname "45eae1a8157e89b9314f";
```

In the above example, the binding state is ACTIVE and the IP address assigned to the appliance is 192.168.2.127.

The following table describes DHCP-related CLI commands that you might want to use when configuring a new NetScaler appliance.

Table 1. NetScaler CLI commands for using DHCP with a new NetScaler Appliance

Task	At the NetScaler command prompt, type:
To verify the DHCP fetched details, such as IP address, subnet mask, and gateway on the appliance	`> sh dhcpParams`
To release the DHCP IP address and return it to the IP address pool on the DHCP server when the NetScaler configuration is complete	`> release dhcpIP`

Using DHCP When a Configuration File is Present

If you need to move a NetScaler appliance to a different subnet, such as from a testing environment to a production environment, you can use DHCP to access an appliance that already has a configuration file. Before moving the appliance, enable its DHCP client and save the configuration. As a result, when the appliance restarts, it automatically polls the DHCP server for an IP address. If you did not enable the DHCP client and save the configuration before shutting down the appliance, you will need to connect to the appliance through the console and dynamically run the DHCP client on the appliance. The DHCP server will then provide an IP address, a gateway, and a subnet mask. You can use the IP address to access the appliance and configure the other settings remotely.

If the DHCP client is enabled in the configuration file, you should disable it and then save the configuration file. If the DHCP client is enabled, the appliance will poll the DHCP server again for an IP address when it restarts.

The following table lists the NetScaler CLI commands associated with each task.

Table 2. NetScaler CLI commands for using DHCP with a previously configured NetScaler Appliance

Task	At the NetScaler command prompt, type:
To dynamically run the DHCP client to fetch an IP address from the DHCP server	`> set dhcpParams dhcpClient on`

To configure the DHCP client to run when the appliance restarts	`> set dhcpParams dhcpClient on`
	
	`> save config`

To prevent the DHCP client from running when the appliance restarts	`> set dhcpParams dhcpClient off`
	
	`> save config`
	
	Note: This is required only if the ON setting was saved.

To save the DHCP acquired route so that it is available when the appliance restarts	`> set dhcpParams -dhcpclient on -saveroute on`
	
	`> save config`

To prevent saving the DHCP acquired route (default behavior)	`> set dhcpParams -dhcpclient on -saveroute off`
	
	`> save config`
	
	Note: This is required only if the ON setting was saved.

Accessing a NetScaler by Using SSH Keys and No Password

If you administer a large number of NetScaler appliances, storing and looking up passwords for logging on to individual appliances can be cumbersome. To avoid being prompted for passwords, you can set up secure shell access with public key encryption on each appliance.

NetScaler features can also use SSH key based authentication for internal communication when the internal user is disabled (by using the set ns param -internaluserlogin disabled command). In such cases, the key name must be set as "ns_comm_key".

To set up access using SSH keys, you must generate the public-private key pair on a client and copy the public key to the remote NetScaler appliance.

To generate the keys and connect to a remote NetScaler by using SSH keys

1. On a client (Linux client or a NetScaler) change directory to /root/.ssh.

   cd /root/.ssh

2. Generate the public-private key pair.

   ssh-keygen -t <key_type> -f <optional_key_file_name>

   Example: To create an RSA key with default file name.

   ssh-keygen -t rsa

3. Press ENTER when prompted for a file name for the key pair.

   Note:

   - If you update the default file name for the key pair, use the new name instead of the default name in the rest of this procedure.
   - If you want to disable internal user login, use "ns_comm_key" as the file name for the public-private key pair.

4. Press ENTER two times when prompted for a passphrase.

   Note: If the client is a NetScaler appliance, move the private key file to a persistent location such as sub-directories of the /flash and /var directories.

5. Log on to the remote NetScaler appliance from the client by using a file transfer protocol, and perform the following:

   a. Change directory to /nsconfig/ssh. At the prompt, type:

      cd /nsconfig/ssh

   b. Use the binary transfer mode to copy the public key to this directory.

      bin
      put id_rsa.pub

6. Open a connection to the remote NetScaler appliance by using an SSH client, such as PuTTY, and perform the following:

   a. Log on to the remote appliance using the administrator credentials.

   b. Go to the NetScaler shell.

      > shell

   c. At the shell prompt, change the directory to /nsconfig/ssh.

```
root@ns# cd /nsconfig/ssh
```

d. Append the public key to the authorized_keys file. At the shell prompt, type:

```
root@ns# cat id_rsa.pub >> authorized_keys
```

Note: If the authorized_keys file does not exist at the appliance, you need to first create the file and then append the contents.

e. Change the permission of the /flash, nsconfig, and ssh directories to 755.

```
root@ns# chmod 755 /flash
root@ns# chmod 755 /flash/nsconfig
root@ns# chmod 755 /flash/nsconfig/ssh
```

f. Change the permission of the authorized_keys file to 744.

```
root@ns# chmod 744 authorized_keys
```

g. Optionally, remove the public key.

```
root@ns# rm id_rsa.pub
```

7. On the client, verify that you can connect to the remote NetScaler appliance by using SSH, without entering the password.

   If using the default file name for the public-private key pair.

   ssh <user_name>@<NetScalerIPAddress>

   If using "ns_comm_key" (when internal user is disabled) for the public-private key pair.

   ssh –i /nsconfig/ssh/ns_comm_key <user_name>@<NetScalerIPAddress>

   If using any other name for the public-private key pair.

   ssh –i <path_to_client_private_key> <user_name>@<NetScalerIPAddress>

Changing the Administrative Password

The default user account is the administrative account, which provides complete access to all features of the Citrix NetScaler appliance. Therefore, to preserve security, the administrative account should be used only when necessary, and only individuals whose duties require full access should know the password for the administrative account. The default administrative username and password are nsroot and nsroot, respectively. Citrix recommends changing the administrative password frequently.

To change the administrative password by using the configuration utility

1. Log on to the appliance by using the administrative credentials.
2. On the Configuration tab, in the navigation pane, expand System, and then click Users.
3. In the Users pane, click the default user account (nsroot), and then click Change Password.
4. In the Change Password dialog box, in Password and Confirm Password, type the password of your choice.
5. Click OK.

To change the administrative password by using the command line interface

At the command prompt, type:

set system user <userName> -password

Example:

```
set system user nsroot -password
Enter password: *****
Confirm password: *****
Done
```

Lights Out Management Port of the NetScaler Appliance

The MPX 8200/8400/8600/8800, MPX 11500/13500/14500/16500/18500/20500, and MPX 17550/19550/20550/21550 appliances have an Intelligent Platform Management Interface (IPMI), also known as the Lights out Management (LOM), port on the front panel of the appliance. By using the LOM, you can remotely monitor and manage the appliance, independently of the NetScaler software. You can remotely change the IP address, perform different power operations, and obtain information of the appliance, such as health monitoring information, MAC address, serial number, and properties of the host, by connecting to the appliance through the LOM port.

By connecting the LOM port over a dedicated channel that is separate from the data channel, you can make sure that connectivity to the appliance is maintained even if the data network is down.

Caution: LOM firmware versions are platform specific. Upgrading to a LOM firmware version other than one shown for your platform in the LOM Support Matrix, below, results in the LOM becoming unusable.

The LOM Support Matrix shows the LOM firmware versions shipped with the various platforms, along with the recommended versions, and the earliest NetScaler software versions that support both the shipped and the recommended LOM firmware versions.

Hardware	Ships With Version	Recommended Version	Minimum NetScaler Version to avoid PS failure issues
MPX 8005/8015/8200/8400/8600/8800	2.04/2.07/3.02/3.10/3.11	3.11	9.3_65.x, 10.1_123.x, 10.5
MPX 11500/13500/14500/16500/18500/20500	2.52/3.02/3.33/3.34	3.34	9.3_65.x, 10.1_123.x, 10.5
MPX 11515/11520/11530/11540/11542	2.52/3.02/3.33/3.34	3.34	9.3_65.x, 10.1_123.x, 10.5
MPX 17550/19550/20550/21550	2.52/3.02/3.33/3.34	3.34	9.3_65.x, 10.1_123.x, 10.5
MPX 22040/22060/22080/22100/22120	2.63/3.22	3.22	9.3_65.x, 10.1_123.x, 10.5

MPX 24100/24150	2.63/3.22	3.22	9.3_65.x, 10.1_123.x, 10.5

Accessing the LOM Port by using a Web Browser

By using a web browser you can remotely log on to the LOM port to obtain information about the appliance and perform different operations on the appliance.

To access the LOM by using a web browser

1. In a web browser, type the IP address of the LOM port. For initial configuration, type the port's default address: `http://192.168.1.3`
2. In the User Name box, type **nsroot**.
3. In the Password box, type **nsroot**.

Configuring the LOM Port

For initial configuration of the lights-out management (LOM) port, connect to the port's default IP address and change it to the address that you want to use for remote monitoring and management. Also specify the administrator credentials and the network settings.

Note: The LEDs on the LOM port are unoperational by design.

To Configure the NetScaler LOM Port

1. Connect the NetScaler LOM port to a management workstation or network.
2. In a web browser, type: http://192.168.1.3.

   Note: The NetScaler LOM port is preconfigured with the IP address 192.168.1.3 and subnet mask 255.255.255.0.
3. In the User Name box, type **nsroot**.
4. In the Password box, type **nsroot**.
5. In the Configuration tab, click Network and type values for the following parameters:
   - IP Address—IP address of the LOM port.
   - Subnet Mask—Subnet mask used to define the subnet of the LOM port.
   - Default Gateway—IP address of the router that connects the LOM port to the network.
6. Click Save.

Power Cycling the Appliance

You can remotely turn off the appliance and turn it back on. The result is similar to pressing the power button on the back panel of the appliance for less than four seconds. The appliance's software performs a graceful shutdown. All operations on the appliance are stopped, no new connections to the client or server are accepted, and all existing connections are closed.

To power cycle the appliance

1. In a web browser, type the IP address of the LOM port.
2. In the User Name and Password boxes, type the administrator credentials.
3. In the Menu bar, click Remote Control.
4. Under Options, click Power Control, and then click Power Cycle System.
5. Click Perform Action.

Performing a Core Dump

If the appliance fails or becomes unresponsive, you can remotely perform a core dump. This procedure has the same effect as pressing the NMI button on the back panel of the appliance.

To perform a core dump

1. In a web browser, type the IP address of the LOM port.
2. In the User Name and Password boxes, type the administrator credentials.
3. In the Menu bar, click Remote Control.
4. Under Options, click NMI, and then click Initiate NMI.

Accessing the Appliance by using the Access Console

The LOM port allows you to remotely access and manage the appliance by logging on to a redirected console.

To access the appliance by using the access console

1. In a web browser, type the IP address of the LOM port.
2. In the User Name and Password boxes, type the administrator credentials.
3. In the Menu bar, click Remote Control.

4. Under Options, click Console Redirection.
5. Click Launch Console, and then click Yes.
6. Type the administrator credentials for the appliance.

Obtaining Properties of the Host

After you log on to the appliance by using the access console, you can remotely manage the appliance. At the console prompt, type sh nsip.

Obtaining Health Monitoring Information

You can log on to the LOM port to view the health information about the appliance. All system sensor information, such as system temperature, CPU temperature, status of fan and power supplies, appears on the sensor readings page.

To obtain health monitoring information

1. In a web browser, type the IP address of the LOM port.
2. In the User Name and Password boxes, type the administrator credentials.
3. In the Menu bar, click System Health.
4. Under Options, click Sensor Readings.

Obtaining the MAC Address and the Serial Number of the Appliance

A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment.

To obtain the MAC address and the serial number of the appliance

1. In a web browser, type the IP address of the LOM port.
2. In the User Name and Password boxes, type the administrator credentials.
3. In the Menu bar, click Remote Control.
4. Under Options, click Console Redirection.
5. Click Launch Console, and then click Yes.
6. Type the administrator credentials for the appliance to log on.
7. Type show interface <management_interface_id> to obtain the MAC address.
8. Type show hardware to obtain the serial number of the appliance.

Power Control Operations using the LOM Port

You can remotely perform different power control operations, such as restarting the appliance, performing a graceful shutdown, and performing a forced shutdown, by using the LOM port.

To perform power control operations

1. In a web browser, log on to the LOM port by using the administrator credentials.
2. In the Menu bar, click Remote Control.
3. Under Options, click Power Control, and then select one of the following options:
   - **Reset System**—Restart the appliance.
   - **Power Off System - Immediate**—Disconnect power to the appliance without shutting down the appliance.
   - **Power Off System - Orderly Shutdown**—Shut down the appliance, and then disconnect power to the appliance.
   - **Power On System**—Turn on the appliance.
   - **Power Cycle System**—Turn off the appliance, and then turn it back on.
4. Click Perform Action.

Migrating the Configuration of an Existing NetScaler Appliance to Another NetScaler Appliance

If you are migrating to a new appliance, you must make some changes to the configuration (ns.conf file) of the old appliance before you copy the configuration to the new appliance.

Note: The following procedure does not apply to NetScaler FIPS appliances.

To migrate a configuration

1. On the old appliance, create a backup copy of the configuration file (ns.conf).
2. Use a vi editor to edit the configuration file that you backed up. For example, you might want to change the user name, host name, and password.

   Note: You must remove all interface-related configuration, such as set interface, bind vlan, add channel, bind channel, and set channel.
3. Shut down the old appliance.
4. Perform initial configuration on the new appliance. Connect to the serial console, and at the command prompt type **config ns** to run the NetScaler configuration script. Enter parameter values, such as NetScaler IP address and subnet mask. For information about performing initial configuration by using the configuration utility (GUI) or the LCD keypad, see Initial Configuration.
5. Restart the new appliance.
6. Add a route on the new appliance. At the command prompt, type: add route <network> <netmask> <gateway>
7. Copy the edited configuration file to the new appliance.
8. Copy other relevant files, such as bookmarks, SSL certificates, and CRLs, to the new appliance. Return your feature license(s) to the Citrix licensing portal and reallocate it on the new appliance. For more info about returning your licenses, see http://support.citrix.com/article/CTX131110.

   Note: The platform license is different for a new appliance.
9. Restart the new appliance.
10. Add interface-related configuration specific to your new appliance, switch, and router, and save the configuration.

If you have a high-availability setup, you must perform the above procedure on both the nodes.

Troubleshooting

I cannot access the NetScaler appliance after it is restarted. The NetScaler IP address is not accessible and does not respond to a ping request. What should I do?

NetScaler MPX 8200/8400/8600/8800, MPX 11500/13500/14500/16500/18500/20500, MPX 17550/19550/20550/21550, and MPX 22040/22060/22080/22100/22120 appliances support LOM. Depending on the state of the LOM configuration, start with one of the steps in the following procedure. (To configure the LOM port, see Lights Out Management Port of the NetScaler Appliance).

1. If the LOM port is configured and known to have been working previously, use the LOM credentials to log on to the LOM GUI, and then do the following:

    a. Navigate to **Remote Control** > **Console Redirection**, and then click **Launch Console**.

    b. On the Java iKVM Viewer screen, check the VGA console window for boot errors, such as bad or missing boot media (boot drive/Compact Flash card), and reseat any unconnected boot media. If the appliance boots up, try to log on and run the show techsupport command from the NetScaler command line. Complete the Check Network Interfaces steps listed below to find a working interface on which to transfer the support bundle file.

    c. Navigate to System Health > Sensor Readings to check the status of the hardware components (for example, CPU temperature, system temperature, and power supply status). You might need to scroll down. Green indicates that the hardware component is functioning properly. Red indicates that it has failed. Contact Citrix Support if you observe red indicators.

    d. Navigate to Miscellaneous > Post Snooping and check for BIOS POST initialization codes. If the value of Post Snooping is "00" or "AC," and the AC power supply LED light is green, the BIOS booted up normally. If not, check the Java iKVM Viewer screen to see if the appliance stopped responding during BIOS POST initialization. Perform substeps a through f of Step 2 to recover the appliance. If these steps fail, contact Citrix Support.
2. If the LOM port is configured and the LOM GUI is not accessible, try pinging the LOM IP address. The baseboard management controller (BMC, also known as LOM) runs on standby power, so even if the appliance is powered off by pressing the power button, the BMC is still working. If you are unable to ping the LOM IP address, connect to the COM1 console port through a serial cable (the serial cable can be connected to a network serial terminal/console server for remote access), or try pinging the NetScaler IP address. On the appliance, do the following:

    a. Verify that the appliance is receiving power.

b. If the appliance is not receiving power, change the power cable and connect the cable to another socket.

c. Verify that the power supply is properly seated in power supply slot.

d. Remove all AC power supply cords for 30 seconds to completely remove power from the appliance.

e. Reinsert the AC power supply cords and check the LEDs indicating the status of the AC power supplies. If a power-supply LED is not green, troubleshoot the power supply.

f. Try pinging the LOM IP again. If successful, go to Step 1.

3. If the appliance does not support the LOM port or the LOM port is not configured, do the following:

a. Connect the serial console cable to the appliance.

b. Perform the substeps a through e of Step 2.

c. On the serial console port window, check for any boot failure errors, such as bad or missing boot media (boot drive/Compact Flash card), and reseat any unconnected boot media. If the appliance boots up, try to log on and run the show techsupport command from the NetScaler command line. Complete the Check Network Interfaces steps listed below to find a working interface on which to transfer the support bundle file.

Check Network Interfaces.

1. If management interface 0/1 is not operational, use the Java iKVM Viewer, as described in Step 1.b, to set up management interface 0/2, and connect a network cable to port 0/2. Use the serial console port for appliances that do not support the LOM port.

2. Make sure that the LED port status indicators are green for all interfaces. For more information about LED port status indicators, see "LED Port-Status Indicators" in Ports.

3. Verify that the SFP/SFP+/XFP transceivers are supported by Citrix.

Citrix® NetScaler® 10 Quick Start Guide: MPX 5500 Platform

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler appliance. If the NetScaler equipment causes interference, try to correct the interference by using one or more of the following measures:

Move the NetScaler equipment to one side or the other of your equipment.

Move the NetScaler equipment farther away from your equipment.

Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

Last Updated: March 2012

Document code: March 29 2012 10:35:41

Quick Installation and Configuration

Welcome to the Citrix NetScaler Application Delivery product line.

Please review the following information before proceeding with installation of the MPX appliance.

Before you Begin

Verify that the following components and accessories are included:

- One NetScaler MPX appliance
- One accessory kit that contains:
  - One RJ-45 to DB-9 adapter
  - One 6 ft RJ-45/DB-9 cable
  - One power cable for the MPX 5500 and MPX 7500/9500 appliances
  - Two power cables for the MPX 15000, MPX 17000, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances

    Note: Make sure that a power outlet is available for each cable.
- One mounting rail kit

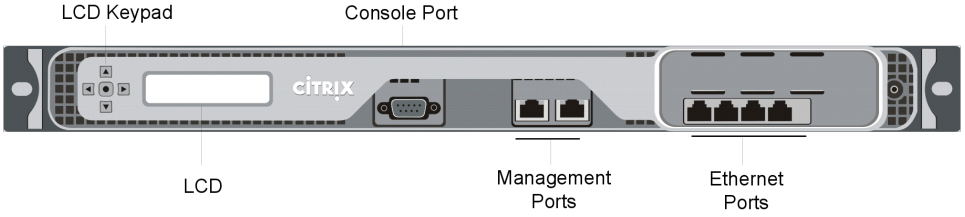
Note: SFP and SFP+ transceivers are sold separately. Contact your Citrix sales representative to order transceivers for your appliance. Only transceivers supplied by Citrix are supported on the appliance.

Citrix NetScaler MPX 5500

The Citrix NetScaler MPX 5500 is a 1U appliance, with 1 dual-core processor, and 4 gigabytes (GB) of memory.

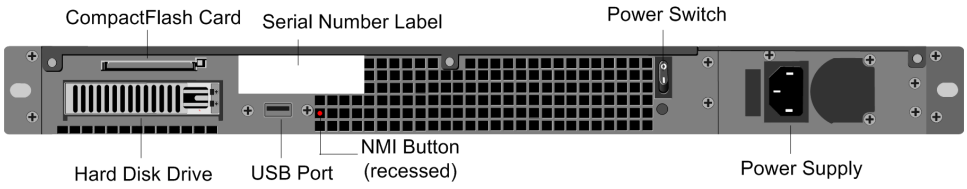
The following figure shows the front panel of the MPX 5500.

Figure 1-1. Citrix NetScaler MPX 5500, front panel



The following figure shows the back panel of the MPX 5500.

Figure 1-2. Citrix NetScaler MPX 5500, back panel



Configuration Requirements

Determine the following information for performing the initial configuration.

- NetScaler IP address: The management IP address of the appliance.
- Subnet IP address or Mapped IP address: The IP address used by the appliance to represent the client when communicating with a server.
- Default gateway: The IP address of the router that forwards traffic out of the appliance's subnet.
- Root password: The root user (nsroot) has full administrative privileges on the appliance. The root password is used to authenticate the root user.

Installation

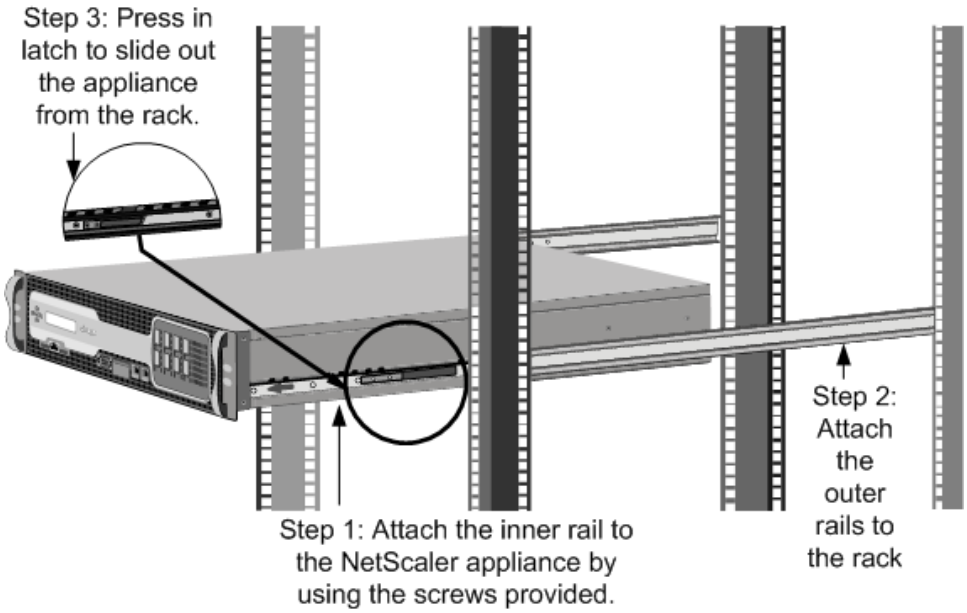
Installation involves rack-mounting the appliance, installing transceivers (if available), and connecting the appliance to the network and a power source.

Note: The appliances illustrated in the installation instructions may not represent the actual NetScaler appliance.

Rack Mounting a Citrix NetScaler Appliance

The appliance is shipped with rack-rail hardware. This hardware consists of two inner rails that you attach to the appliance, one on each side, and a rack-rail assembly that you attach to the rack. The following figure illustrates the steps involved in mounting the Citrix NetScaler appliance to a rack.

Figure 1-3. Rack Mounting the Appliance



Appliance Precautions

- Determine the placement of each component in the rack before you install the rail.
- Install the heaviest appliance first at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.
- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near a socket outlet for easy access.
- Mount equipment into a rack with sufficient airflow for safe operation.
- For a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

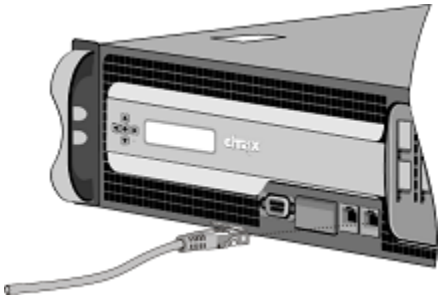
- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously may cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should only be used for extending the appliance out of the rack. These handles should not be used

for mounting the appliance on the rack. Rack-rail hardware described later should be used instead.

Connecting a NetScaler Appliance to the Network

Connect the interfaces on the appliance to the network ports on the appropriate switches by using Ethernet/fiber optic cables.

Figure 1-4. Connecting a Citrix NetScaler appliance to the network



Warning: Connecting multiple network ports to the same switch or VLAN can result in a network loop.

Note: By default, the NetScaler MPX appliance is configured to use auto-negotiation. When you install a NetScaler appliance for the first time, be sure to configure your other equipment to use auto-negotiation for the ports that are connected to the NetScaler appliance. After initial logon and configuration, you can choose to disable auto-negotiation.

Connecting a NetScaler Appliance to a Power Source

Connect the power cable to one of the inlet receptacles on the back of the appliance and connect the other end of the power cable to a power outlet. If your appliance has a second power supply, repeat this process. All models function properly with a single power supply. The extra power supply on some models serves as a backup. The Citrix logo and LCD on the front of the NetScaler illuminate after the appliance starts, and the LCD indicates the operational status of the appliance.

Figure 1-5. Connecting a Citrix NetScaler appliance to a power source

Note: If you want to upgrade to the latest release of the system software before proceeding, see the *Citrix NetScaler Migration Guide*. For a link to the guide, see the Documentation Library of this guide.

Electrical Safety Precautions

Basic electrical safety precautions should be followed to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch. If an electrical accident occurs, you can quickly remove power to the appliance.
- Use a regulating uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, you should first shut down the appliance and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages may be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Make sure that the power supply cords include grounding plugs and are plugged into grounded electrical outlets.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload.
- A reliable ground must be maintained at all times. Therefore, the rack should be grounded. Pay particular attention to power supply connections other than the direct connection to the branch circuit (for example, connections to power strips).

Setting Up Connectivity

Connect the appliance to a management workstation or the network by using the NetScaler configuration utility, the command-line interface (CLI), or the LCD keypad.

Configuration Utility Setup

To set up the appliance by using the configuration utility, you need a management workstation or laptop configured on the same network as the appliance. To run the configuration utility, the Java RunTime Environment (JRE) version 1.4.2_04 or later must be installed on the workstation or laptop.

Note: The Setup Wizard automatically opens upon log on when the appliance is configured with the default IP address, when licenses are not installed on the

appliance, and when either the mapped IP address or subnet IP address is not configured.

To configure the NetScaler by using the configuration utility

1. Connect the NetScaler to a management workstation or network.
2. Open a browser and type: `http://192.168.100.1`

   Note: The NetScaler is preconfigured with the IP address 192.168.100.1.
3. In **User Name**, type `nsroot`.
4. In **Password**, type `nsroot`.
5. In the **Setup Wizard**, click **Next** and follow the instructions in the wizard.
6. To confirm that the NetScaler is configured correctly, you can either ping the new NetScaler IP address (NSIP) or use the new NSIP to open the configuration utility in a browser.

CLI Setup

To set up the appliance by using the command-line interface (CLI), connect the serial cable to the console port. Access the command line with a terminal or terminal emulator with the following settings:

- Baud rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Log on to the NetScaler with the following credentials:

User name: `nsroot`

Password: `nsroot`

To configure the NetScaler by using the NetScaler command line

At the NetScaler command prompt, type:

- **set ns config** -ipaddress<IPAddress> -netmask<subnetMask>
- **add ns ip**<IPAddress> <subnetMask> -type<type>
- **add route Network**<subnetMask> <gateway>
- **set system user**<userName> <password>

- **save ns config**
- **reboot**

Example

```
set ns config -ipaddress 10.102.29.60 -netmask
255.255.255.0 add ns ip 10.102.29.61 255.255.255.0 -
type snip add route 0.0.0.0 0.0.0.0 10.102.29.1 set
system user nsroot administrator save ns config
reboot
```

Note: For information about deploying a high availability (HA) pair, see the *Citrix NetScaler Networking Guide* at http://support.citrix.com/article/CTX132369.

LCD Keypad Setup

To set up the appliance by using the LCD keypad on the front panel of the appliance, enter the following initial settings in the following order:

1. subnet mask
2. NSIP
3. gateway

The NSIP and the default gateway should be on the same subnet.

The subnet mask, NSIP, and gateway values are saved in the configuration file. You can then use the NSIP to connect to the appliance remotely. For more information, see the *Citrix NetScaler Hardware Installation and Setup Guide* at http://support.citrix.com/article/CTX132365.

Note: For information about deploying a high availability (HA) pair, see the *Citrix NetScaler Networking Guide* at http://support.citrix.com/article/CTX132369.

System Specifications

The following table summarizes the specifications of the NetScaler MPX 5500 appliances.

Specifications	MPX 5500
Processors	1 dual-core
Memory	4 GB
Number of power supplies	1

Specifications	MPX 5500
AC power supply input voltage, frequency, and current	100-240VAC 50-60 Hz 3-1.5A
DC power supply input voltage and current	260 W
Maximum power consumption	887 BTU per hour
Heat dissipation	22
Weight (lbs.)	1U
Height	EIA 310-D for 19-inch racks
Width	21.75 in/ 55 cm
Depth	0-40
Operating temperature (degree Celsius)	5%-95%
Humidity range (non-condensing)	CSA
Safety certifications	FCC (Part 15 Class A), CE, C-Tick, CCC, KCC, NOM, PCT, VCCI, SASO, SABS
EMC & susceptibility	RoHS, WEEE
Environmental compliance	RoHS, WEEE

Additional Information

A complete set of documentation is available on the **Documentation** tab of your NetScaler and from http://support.citrix.com/. (Most of the documents require Adobe Reader, available at http://adobe.com/.)

To view the documentation

1. From a Web browser, log on to the NetScaler.

2. Click the **Documentation** tab.
3. To view a short description of each document, hover your cursor over the title. To open a document, click the title.

If you have support questions, please contact Citrix Technical Support at 1-800-4-CITRIX (1-800-424-8749). For additional contact information, see Support Phone Numbers at http://support.citrix.com/. If you have comments or feedback on this documentation, please email to nsdocs_feedback@citrix.com.

Citrix® NetScaler® 10 Quick Start Guide: MPX 5550/5650 Platform

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler appliance. If the NetScaler equipment causes interference, try to correct the interference by using one or more of the following measures:

Move the NetScaler equipment to one side or the other of your equipment.

Move the NetScaler equipment farther away from your equipment.

Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

Last Updated: July 2012

Document code: September 28 2012 05:18:07

Quick Installation and Configuration

Welcome to the Citrix NetScaler Application Delivery product line.

Please review the following information before proceeding with installation of the MPX appliance.

Before you Begin

Verify that the following components and accessories are included:

- One NetScaler MPX appliance
- One accessory kit that contains:
  - One RJ-45 to DB-9 adapter
  - One 6 ft RJ-45/DB-9 cable
  - One power cable
- One standard 4-post rail kit

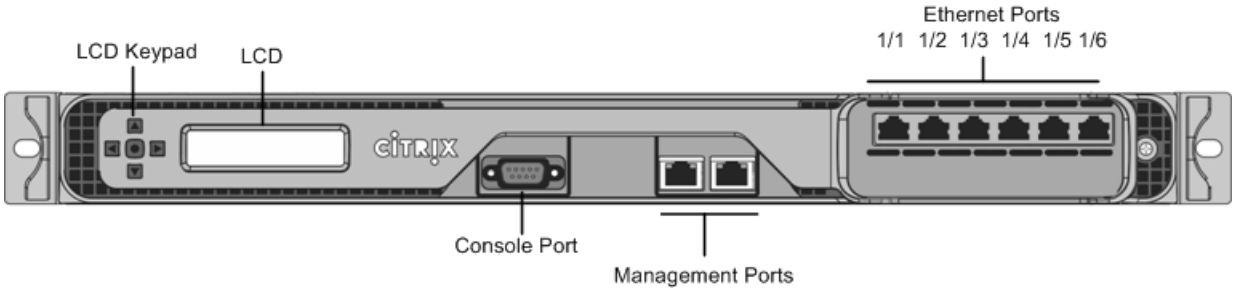
Note: If the kit that you received does not fit your rack, contact your Citrix sales representative to order the appropriate kit.

Citrix NetScaler MPX 5550 and MPX 5650

The Citrix NetScaler models MPX 5550 and MPX 5650 are 1U appliances. Each model has one quad-core processor and 8 gigabytes (GB) of memory.

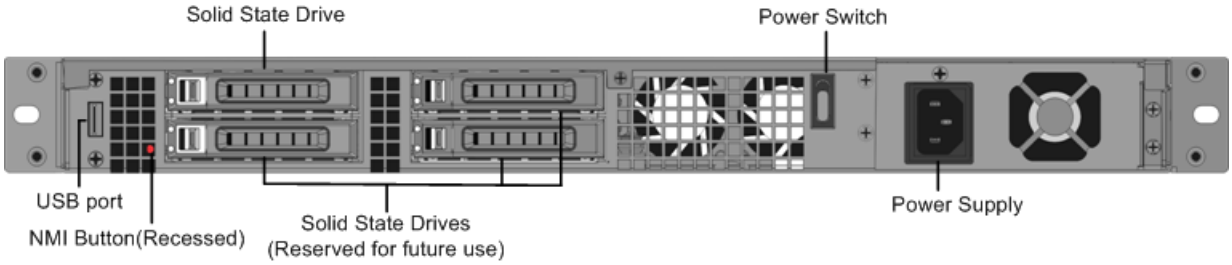
The following figure shows the front panel of the MPX 5550/5650 appliance.

Figure 1-1. Citrix NetScaler MPX 5550/5650, front panel



The following figure shows the back panel of the MPX 5550/5650 appliance.

Figure 1-2. Citrix NetScaler MPX 5550/5650 appliance, back panel



Configuration Requirements

Determine the following information for performing the initial configuration.

- NetScaler IP address (NSIP): The management IP address of the appliance. The default NSIP address is 192.168.100.1.
- Subnet IP address or Mapped IP address: The IP address used by the appliance to represent the client when communicating with a server.
- Default gateway: The IP address of the router that forwards traffic out of the appliance's subnet. The default gateway should be in the same subnet as the NSIP address.
- Root password: The root user (nsroot) has full administrative privileges on the appliance. The root password is used to authenticate the root user. The default root password is nsroot. You can change this password during initial configuration of the appliance.

Installation

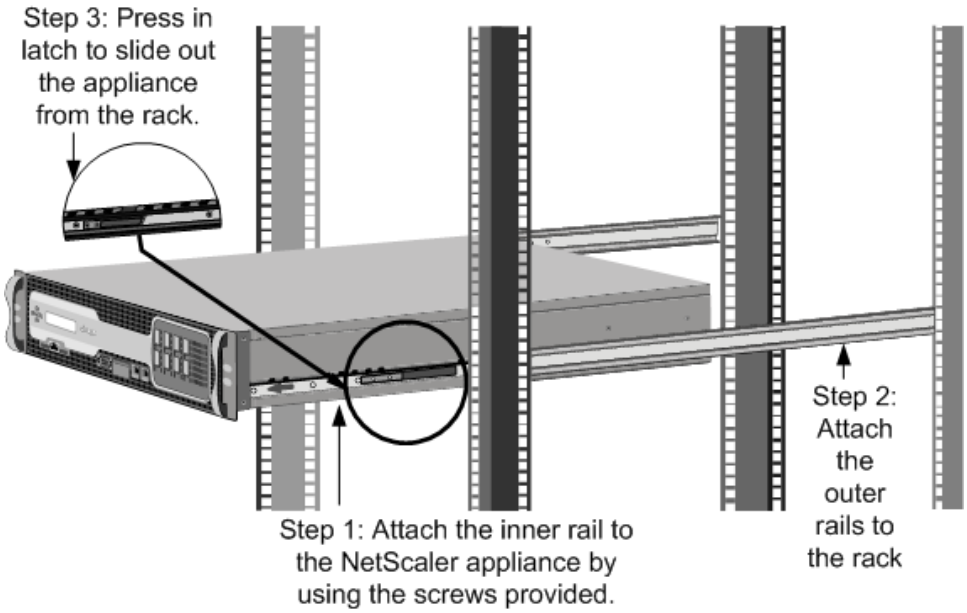
Installation involves rack-mounting the appliance, installing transceivers (if available), and connecting the appliance to the network and a power source.

Note: The appliances illustrated in the installation instructions may not represent the actual NetScaler appliance.

Rack Mounting a Citrix NetScaler Appliance

The appliance is shipped with rack-rail hardware. This hardware consists of two inner rails that you attach to the appliance, one on each side, and a rack-rail assembly that you attach to the rack. The following figure illustrates the steps involved in mounting the Citrix NetScaler appliance to a rack.

Figure 1-3. Rack Mounting the Appliance



Appliance Precautions

- Determine the placement of each component in the rack before you install the rail.
- Install the heaviest appliance first at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.
- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near an electrical outlet for easy access.
- Mount equipment into a rack with sufficient airflow for safe operation.
- For a closed or multiple-unit rack assembly, the ambient operating temperature of the rack environment might be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

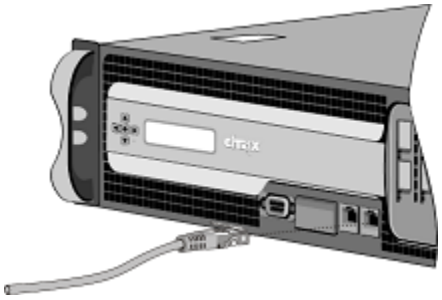
- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously might cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should be used only for extending the appliance out of the rack. These handles should not be used

for mounting the appliance on the rack. Rack-rail hardware described later should be used instead.

Connecting a NetScaler Appliance to the Network

Connect the interfaces on the appliance to the network ports on the appropriate switches by using Ethernet/fiber optic cables.

Figure 1-4. Connecting a Citrix NetScaler appliance to the network



Warning: Connecting multiple network ports to the same switch or VLAN can result in a network loop.

Note: By default, the NetScaler MPX appliance is configured to use auto-negotiation. When you install a NetScaler appliance for the first time, be sure to configure your other equipment to use auto-negotiation for the ports that are connected to the NetScaler appliance. After initial logon and configuration, you can choose to disable auto-negotiation.

Connecting a NetScaler Appliance to a Power Source

Connect the power cable to one of the inlet receptacles on the back of the appliance and connect the other end of the power cable to a power outlet. If your appliance has a second power supply, repeat this process. All models function properly with a single power supply. The extra power supply on some models serves as a backup. The Citrix logo and LCD on the front of the NetScaler illuminate after the appliance starts, and the LCD indicates the operational status of the appliance.

Figure 1-5. Connecting a Citrix NetScaler appliance to a power source

Note: If you want to upgrade to the latest release of the system software before proceeding, see Upgrading or Downgrading the System Software.

Electrical Safety Precautions

Basic electrical safety precautions should be followed to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch, so that you can quickly remove power to the appliance if an electrical accident occurs.
- Use a regulating, uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, you should first shut down the appliance and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages may be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Make sure that the power supply cords include grounding plugs and are plugged into grounded electrical outlets.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload.
- A reliable ground must be maintained at all times. Therefore, the rack should be grounded. Pay particular attention to power supply connections other than the direct connection to the branch circuit (for example, connections to power strips).

Setting Up Connectivity

Connect the appliance to a management workstation or the network by using the NetScaler configuration utility, the command-line interface (CLI), or the LCD keypad.

Log on to the appliance as nsroot. For initial configuration, use nsroot as the administrative password. For subsequent access, use the password assigned during initial configuration.

Configuration Utility Setup

To set up the appliance by using the configuration utility, you need a management workstation or laptop configured on the same network as the appliance. To run the configuration utility, the Java RunTime Environment (JRE) version 1.4.2_04 or later must be installed on the workstation or laptop.

Note: The Setup Wizard automatically opens upon logon when the appliance is configured with the default IP address, when licenses are not installed on the appliance, and when either a mapped IP address or subnet IP address is not configured.

To configure the NetScaler by using the configuration utility

1. Connect the NetScaler to a management workstation or network.
2. Open a browser and type: `http://192.168.100.1`

   Note: The NetScaler is preconfigured with the IP address 192.168.100.1.
3. In **User Name**, type `nsroot`.
4. In **Password**, type `nsroot`.
5. In the **Setup Wizard**, click **Next** and follow the instructions in the wizard to configure the basic parameters, such as IP address, netmask, and gateway.
6. To confirm that the NetScaler is configured correctly, you can either ping the new NetScaler IP address (NSIP) or use the new NSIP to open the configuration utility in a browser.

CLI Setup

To set up the appliance by using the command-line interface (CLI), connect the 6-foot RJ-45/DB-9 serial cable to the console port. Access the command line with a terminal or terminal emulator with the following settings:

- Baud rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Log on to the NetScaler with the following credentials:

User name: `nsroot`

Password: `nsroot`

To configure the NetScaler by using the NetScaler command line

At the NetScaler command prompt, type:

- **set ns config** -ipaddress<IPAddress> -netmask<subnetMask>
- **add ns ip**<IPAddress> <subnetMask> -type<type>

- **add route**<network> <netmask> <gateway>
- **set system user** <userName> -password
- **save ns config**
- **reboot**

Example

```
set ns config -ipaddress 10.102.29.60 -netmask
255.255.255.0
add ns ip 10.102.29.61 255.255.255.0 -type snip
add route 0.0.0.0 0.0.0.0 10.102.29.1
set system user nsroot -password
Enter password: *****
Confirm password: *****
save ns config
reboot
```

Note: For information about deploying a high availability (HA) pair, see Configuring High Availability.

LCD Keypad Setup

To set up the appliance by using the LCD keypad on the front panel of the appliance, press the "<" key on the keypad, and enter the following initial settings in the order shown:

1. Subnet mask
2. NSIP address
3. Gateway

The subnet mask, NSIP, and gateway values are saved in the configuration file. You can then use the NSIP to connect to the appliance remotely. For more information, see Hardware Installation.

Note: For information about deploying a high availability (HA) pair, see Configuring High Availability.

Changing the Administrative Password

The default user account is the administrative account, which provides complete access to all features of the Citrix NetScaler appliance. Therefore, to preserve security, the administrative account should be used only when necessary, and only individuals whose duties require full access should know the password for the administrative account. Citrix recommends changing the administrative password frequently.

In the configuration utility, you type the password. In the NetScaler command line, you are prompted to enter the password.

To change the administrative password by using the NetScaler configuration utility

1. On the **Configuration** tab, in the navigation pane, expand **System**, and then click **Users**.
2. In the **Users** pane, click the default user account, and then click **Change Password**.
3. In the **Change Password** dialog box, in **Password** and **Confirm Password**, type the password of your choice.
4. Click **OK**.

To change the administrative password by using the NetScaler command line

At the NetScaler command prompt, type: set system user <userName> {-password }

System Specifications

The following table summarizes the specifications of the NetScaler MPX 5550/5650 appliances.

Specifications	MPX 5550/5650
Processors	1 quad-core processor
Memory	8 GB
Number of power supplies	1
AC power supply input voltage, frequency, and current	100-240 VAC 50-60 Hz 2.5 A
Maximum power consumption	300 W
Heat dissipation	630 BTU per hour
Weight	32 lbs
Height	1U

Specifications	MPX 5550/5650
Width	EIA 310-D for 19-inch racks
Depth	61 cm
Operating temperature (degree Celsius)	0-40
Humidity range (non-condensing)	5%-95%
Safety certifications	CSA
EMC & susceptibility	FCC (Part 15 Class A), CE, C-Tick, VCCI-A, CCC, KCC, NOM, SASO, SABS, PCT
Environmental compliance	RoHS, WEEE

Additional Information

A complete set of documentation is available on the **Documentation** tab of your NetScaler appliance and from http://support.citrix.com/. (Most of the documents require Adobe Reader, available at http://adobe.com/.)

To view the documentation

1. From a web browser, log on to the NetScaler.
2. Click the **Documentation** tab.
3. To view a short description of each document, hover your cursor over the title. To open a document, click the title.

To contact Citrix Support, call 1-800-4-CITRIX (1-800-424-8749), or log on to MyCitrix at http://www.citrix.com. You will be asked for your hardware serial number as part of the support process.

Detailed instructions for contacting support can be found at: http://citrix.com/site/resources/dynamic/sup2nd/Citrix_HWS_SerialNO.pdf.

If you have comments or feedback on this documentation, please send email to nsdocs_feedback@citrix.com.

Citrix® NetScaler® 10 Quick Start Guide: MPX 7500/9500 Platform

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler appliance. If the NetScaler equipment causes interference, try to correct the interference by using one or more of the following measures:

Move the NetScaler equipment to one side or the other of your equipment.

Move the NetScaler equipment farther away from your equipment.

Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

Last Updated: March 2012

Document code: March 29 2012 10:36:04

Quick Installation and Configuration

Welcome to the Citrix NetScaler Application Delivery product line.

Please review the following information before proceeding with installation of the MPX appliance.

Before you Begin

Verify that the following components and accessories are included:

- One NetScaler MPX appliance
- One accessory kit that contains:
  - One RJ-45 to DB-9 adapter
  - One 6 ft RJ-45/DB-9 cable
  - One power cable for the MPX 5500 and MPX 7500/9500 appliances
  - Two power cables for the MPX 15000, MPX 17000, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances

    Note: Make sure that a power outlet is available for each cable.
- One mounting rail kit

Note: SFP and SFP+ transceivers are sold separately. Contact your Citrix sales representative to order transceivers for your appliance. Only transceivers supplied by Citrix are supported on the appliance.

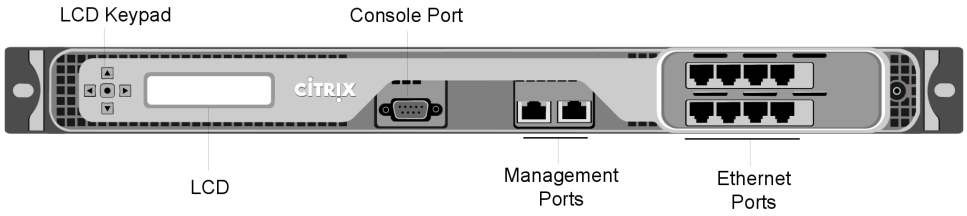
Citrix NetScaler Command Center MPX 7500 and MPX 9500

The Citrix NetScaler MPX 7500/9500 are 1U appliances, each with 1 quad-core processor, and 8 gigabytes (GB) of memory. The MPX 7500/9500 appliances are available in two port configurations: 8xCopper Ethernet (Cu) and 4xSFP+4xCu.

The Command Center hardware platform is the MPX™ 7500 appliance, which is a 1U appliance with one quad-core processor and 8 gigabytes (GB) of memory. The MPX 7500 appliance is available in an 8x Copper Ethernet (Cu) port configuration.

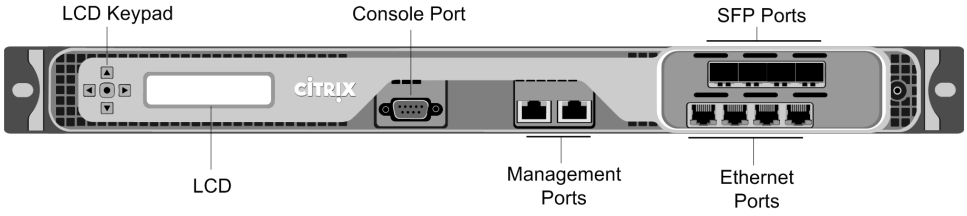
The following figure shows the front panel of the MPX 7500/9500 (8xCu) appliances.

Figure 1-1. Citrix NetScalerCommand Center MPX 7500/9500 (8xCu), front panel



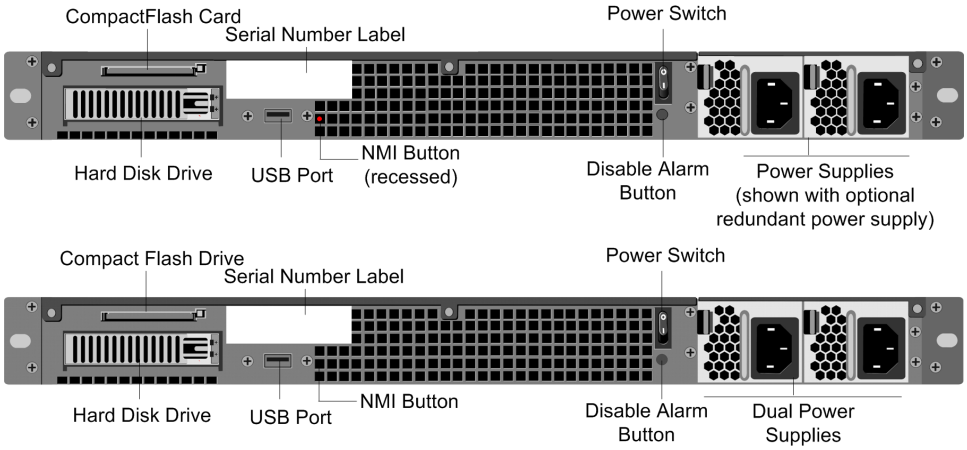
The following figure shows the front panel of the MPX 7500/9500 (4xSFP+4xCu) appliances.

Figure 1-2. Citrix NetScaler MPX 7500/9500 (4xSFP+4xCu), front panel



The following figure shows the back panel of the MPX 7500/9500appliance.

Figure 1-3. Citrix NetScalerCommand Center MPX 7500/9500, back panel



Configuration Requirements

Determine the following information for performing the initial configuration.

- NetScaler IP address: The management IP address of the appliance.
- Subnet IP address or Mapped IP address: The IP address used by the appliance to represent the client when communicating with a server.
- Default gateway: The IP address of the router that forwards traffic out of the appliance’s subnet.

- Root password: The root user (nsroot) has full administrative privileges on the appliance. The root password is used to authenticate the root user.

Installation

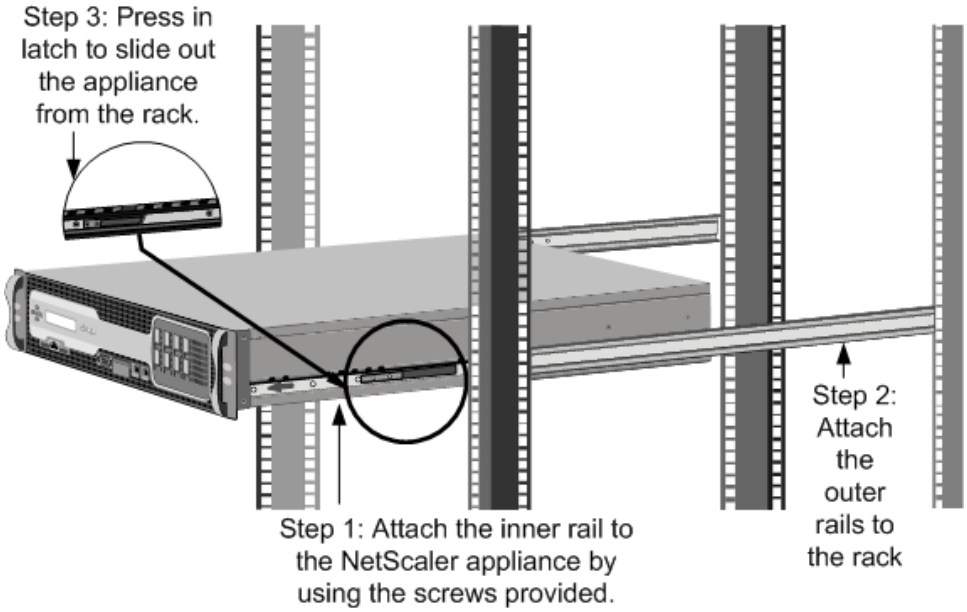
Installation involves rack-mounting the appliance, installing transceivers (if available), and connecting the appliance to the network and a power source.

Note: The appliances illustrated in the installation instructions may not represent the actual NetScaler appliance.

Rack Mounting a Citrix NetScaler Appliance

The appliance is shipped with rack-rail hardware. This hardware consists of two inner rails that you attach to the appliance, one on each side, and a rack-rail assembly that you attach to the rack. The following figure illustrates the steps involved in mounting the Citrix NetScaler appliance to a rack.

Figure 1-4. Rack Mounting the Appliance



Appliance Precautions

- Determine the placement of each component in the rack before you install the rail.
- Install the heaviest appliance first at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.
- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near a socket outlet for easy access.

- Mount equipment into a rack with sufficient airflow for safe operation.
- For a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously may cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should only be used for extending the appliance out of the rack. These handles should not be used for mounting the appliance on the rack. Rack-rail hardware described later should be used instead.

Installing Transceivers

The MPX appliances support both copper and fiber transceivers

Warning: Only those transceivers provided by Citrix Systems, Inc. are supported. You must not attempt to install third-party transceivers. Doing so voids the warranty.

To install the transceiver

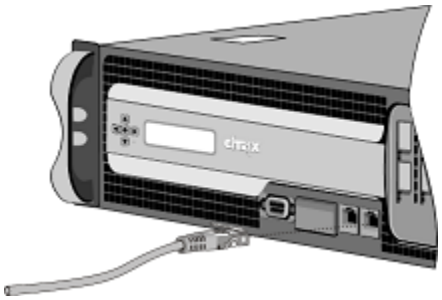
1. Carefully remove the transceiver from its box.
2. Align the transceiver to the front of the transceiver slot on the front panel of the appliance.
3. Hold the transceiver between your thumb and index finger and insert it into the transceiver slot, pressing it in until you hear the transceiver snap into place.
4. Lock the transceiver.

Note: To remove an SFP+ transceiver, you may first need to remove the SFP transceiver below it.

Connecting a NetScaler Appliance to the Network

Connect the interfaces on the appliance to the network ports on the appropriate switches by using Ethernet/fiber optic cables.

Figure 1-5. Connecting a Citrix NetScaler appliance to the network



Warning: Connecting multiple network ports to the same switch or VLAN can result in a network loop.

Note: By default, the NetScaler MPX appliance is configured to use auto-negotiation. When you install a NetScaler appliance for the first time, be sure to configure your other equipment to use auto-negotiation for the ports that are connected to the NetScaler appliance. After initial logon and configuration, you can choose to disable auto-negotiation.

Connecting a NetScaler Appliance to a Power Source

Connect the power cable to one of the inlet receptacles on the back of the appliance and connect the other end of the power cable to a power outlet. If your appliance has a second power supply, repeat this process. All models function properly with a single power supply. The extra power supply on some models serves as a backup. The Citrix logo and LCD on the front of the NetScaler illuminate after the appliance starts, and the LCD indicates the operational status of the appliance.

Figure 1-6. Connecting a Citrix NetScaler appliance to a power source

Note: If you want to upgrade to the latest release of the system software before proceeding, see the *Citrix NetScaler Migration Guide*. For a link to the guide, see the Documentation Library of this guide.

Electrical Safety Precautions

Basic electrical safety precautions should be followed to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch. If an electrical accident occurs, you can quickly remove power to the appliance.
- Use a regulating uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, you should first shut down the appliance and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages may be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Make sure that the power supply cords include grounding plugs and are plugged into grounded electrical outlets.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload.
- A reliable ground must be maintained at all times. Therefore, the rack should be grounded. Pay particular attention to power supply connections other than the direct connection to the branch circuit (for example, connections to power strips).

Setting Up Connectivity

Connect the appliance to a management workstation or the network by using the NetScaler configuration utility, the command-line interface (CLI), or the LCD keypad.

Configuration Utility Setup

To set up the appliance by using the configuration utility, you need a management workstation or laptop configured on the same network as the appliance. To run the configuration utility, the Java RunTime Environment (JRE) version 1.4.2_04 or later must be installed on the workstation or laptop.

Note: The Setup Wizard automatically opens upon log on when the appliance is configured with the default IP address, when licenses are not installed on the appliance, and when either the mapped IP address or subnet IP address is not configured.

To configure the NetScaler by using the configuration utility

1. Connect the NetScaler to a management workstation or network.
2. Open a browser and type: `http://192.168.100.1`

Note: The NetScaler is preconfigured with the IP address 192.168.100.1.

3. In **User Name**, type `nsroot`.
4. In **Password**, type `nsroot`.
5. In the **Setup Wizard**, click **Next** and follow the instructions in the wizard.
6. To confirm that the NetScaler is configured correctly, you can either ping the new NetScaler IP address (NSIP) or use the new NSIP to open the configuration utility in a browser.

CLI Setup

To set up the appliance by using the command-line interface (CLI), connect the serial cable to the console port. Access the command line with a terminal or terminal emulator with the following settings:

- Baud rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Log on to the NetScaler with the following credentials:

User name: `nsroot`

Password: `nsroot`

To configure the NetScaler by using the NetScaler command line

At the NetScaler command prompt, type:

- **set ns config** -ipaddress<IPAddress> -netmask<subnetMask>
- **add ns ip**<IPAddress> <subnetMask> -type<type>
- **add route Network**<subnetMask> <gateway>
- **set system user**<userName> <password>
- **save ns config**
- **reboot**

Example

```
set ns config -ipaddress 10.102.29.60 -netmask
255.255.255.0 add ns ip 10.102.29.61 255.255.255.0 -
type snip add route 0.0.0.0 0.0.0.0 10.102.29.1 set
```

```
system user nsroot administrator save ns config
reboot
```

Note: For information about deploying a high availability (HA) pair, see the *Citrix NetScaler Networking Guide* at http://support.citrix.com/article/CTX132369.

LCD Keypad Setup

To set up the appliance by using the LCD keypad on the front panel of the appliance, enter the following initial settings in the following order:

1. subnet mask
2. NSIP
3. gateway

The NSIP and the default gateway should be on the same subnet.

The subnet mask, NSIP, and gateway values are saved in the configuration file. You can then use the NSIP to connect to the appliance remotely. For more information, see the *Citrix NetScaler Hardware Installation and Setup Guide* at http://support.citrix.com/article/CTX132365.

Note: For information about deploying a high availability (HA) pair, see the *Citrix NetScaler Networking Guide* at http://support.citrix.com/article/CTX132369.

System Specifications

The following table summarizes the specifications of the NetScaler MPX 7500/MPX 9500 appliances.

Specifications	MPX 7500/MPX 9500
Processors	1 dual-core
Memory	8 GB
Number of power supplies	1 with second optional
AC power supply input voltage, frequency, and current	100-240VAC 50-60 Hz 3-1.5A

Specifications	MPX 7500/MPX 9500
DC power supply input voltage and current	260 W
Maximum power consumption	887 BTU per hour
Heat dissipation	23 with one power supply
Weight (lbs.)	1U
Height	EIA 310-D for 19-inch racks
Width	21.75 in/ 55 cm
Depth	0-40
Operating temperature (degree Celsius)	5%-95%
Humidity range (non-condensing)	CSA
Safety certifications	FCC (Part 15 Class A), CE, C-Tick, CCC, KCC, NOM, PCT, VCCI, SASO, SABS
EMC & susceptibility	RoHS, WEEE
Environmental compliance	RoHS, WEEE

Additional Information

A complete set of documentation is available on the **Documentation** tab of your NetScaler and from http://support.citrix.com/. (Most of the documents require Adobe Reader, available at http://adobe.com/.)

To view the documentation

1. From a Web browser, log on to the NetScaler.
2. Click the **Documentation** tab.
3. To view a short description of each document, hover your cursor over the title. To open a document, click the title.

If you have support questions, please contact Citrix Technical Support at 1-800-4-CITRIX (1-800-424-8749). For additional contact information, see Support Phone Numbers at

http://support.citrix.com/. If you have comments or feedback on this documentation, please email to nsdocs_feedback@citrix.com.

Citrix® NetScaler® 10 Quick Start Guide: MPX 9700/10500/12500/15500 Platform

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler appliance. If the NetScaler equipment causes interference, try to correct the interference by using one or more of the following measures:

Move the NetScaler equipment to one side or the other of your equipment.

Move the NetScaler equipment farther away from your equipment.

Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

Last Updated: March 2012

Document code: March 29 2012 10:36:36

Quick Installation and Configuration

Welcome to the Citrix NetScaler Application Delivery product line.

Please review the following information before proceeding with installation of the MPX appliance.

Before you Begin

Verify that the following components and accessories are included:

- One NetScaler MPX appliance
- One accessory kit that contains:
  - One RJ-45 to DB-9 adapter
  - One 6 ft RJ-45/DB-9 cable
  - One power cable for the MPX 5500 and MPX 7500/9500 appliances
  - Two power cables for the MPX 15000, MPX 17000, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances

    Note: Make sure that a power outlet is available for each cable.
- One mounting rail kit

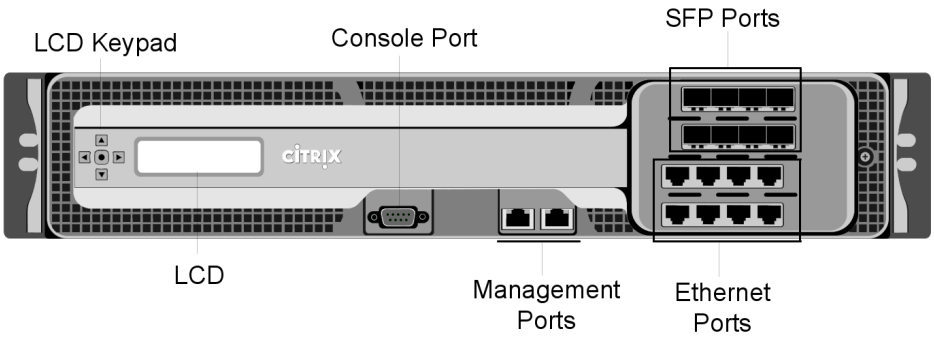
Note: SFP and SFP+ transceivers are sold separately. Contact your Citrix sales representative to order transceivers for your appliance. Only transceivers supplied by Citrix are supported on the appliance.

Citrix NetScaler MPX 9700, MPX 10500, MPX 12500, and MPX 15500

The Citrix NetScaler MPX 9700/10500/12500/15500 are 2U appliances, each with 2 quad-core processors, and 16 gigabytes (GB) of memory. All these appliances are also available in a 10G model and a FIPS model.

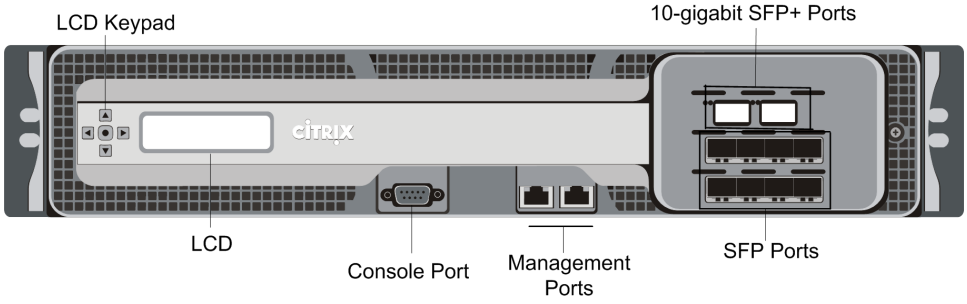
The following figure shows the front panel of the MPX 9700/10500/12500/15500.

Figure 1-1. Citrix NetScaler MPX 9700/10500/12500/15500, front panel



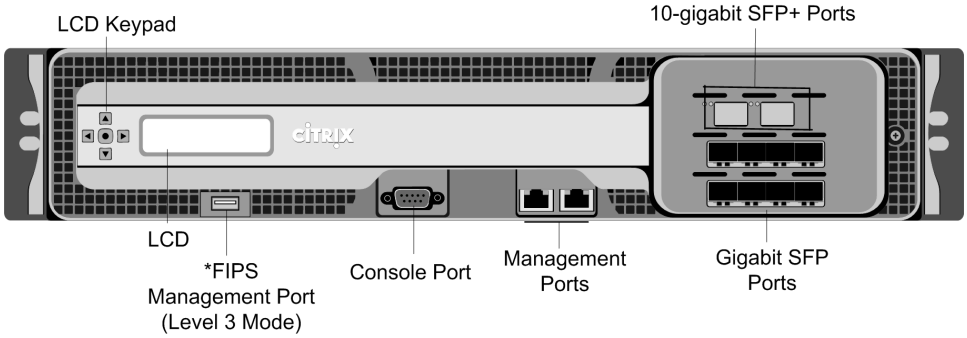
The following figure shows the front panel of the MPX 9700/10500/12500/15500 10G.

Figure 1-2. Citrix NetScaler MPX 9700/10500/12500/15500 10G, front panel



The following figure shows the front panel of the MPX 9700/10500/12500/15500 FIPS.

Figure 1-3. Citrix NetScaler MPX 9700/10500/12500/15500 FIPS, front panel

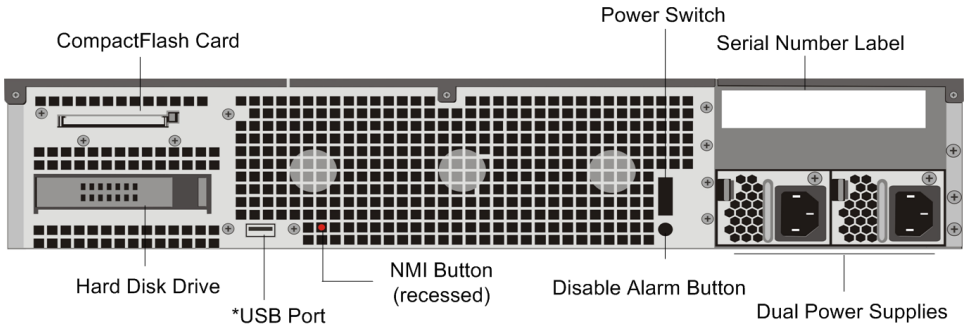


*The FIPS Management Port (Level 3 Mode) is reserved for a future release.

Caution: Do not insert a USB device into the FIPS Management Port. This will cause the FIPS card to fail.

The following figure shows the back panel of the MPX 9700/10500/12500/15500 appliances, including the 10G model and FIPS model.

Figure 1-4. Citrix NetScaler MPX 9700/10500/12500/15500, MPX 9700/10500/12500/15500 FIPS, and MPX 9700/10500/12500/15500 10G, back panel



*The USB Port is reserved for a future release.

Configuration Requirements

Determine the following information for performing the initial configuration.

- NetScaler IP address: The management IP address of the appliance.
- Subnet IP address or Mapped IP address: The IP address used by the appliance to represent the client when communicating with a server.
- Default gateway: The IP address of the router that forwards traffic out of the appliance's subnet.
- Root password: The root user (nsroot) has full administrative privileges on the appliance. The root password is used to authenticate the root user.

Installation

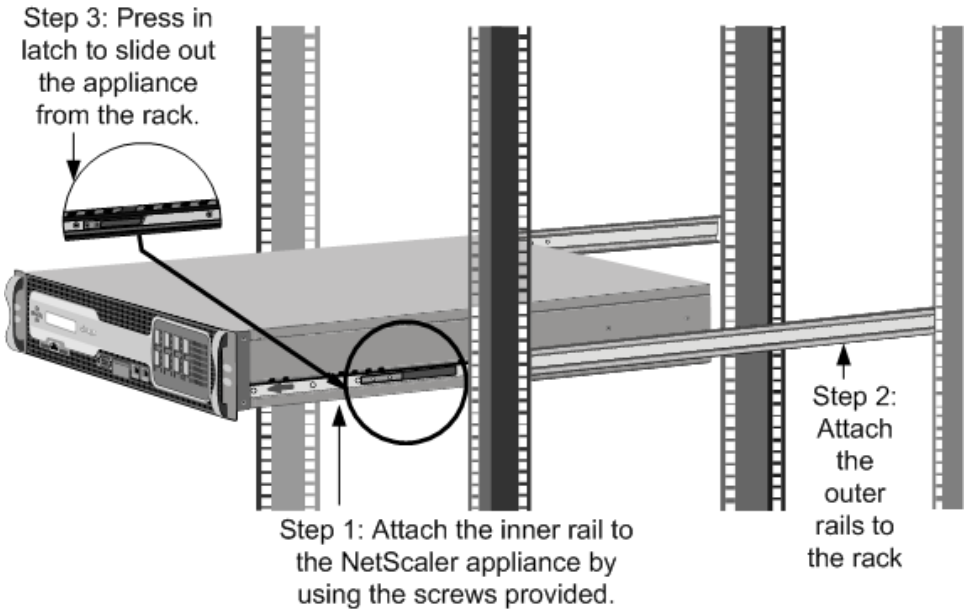
Installation involves rack-mounting the appliance, installing transceivers (if available), and connecting the appliance to the network and a power source.

Note: The appliances illustrated in the installation instructions may not represent the actual NetScaler appliance.

Rack Mounting a Citrix NetScaler Appliance

The appliance is shipped with rack-rail hardware. This hardware consists of two inner rails that you attach to the appliance, one on each side, and a rack-rail assembly that you attach to the rack. The following figure illustrates the steps involved in mounting the Citrix NetScaler appliance to a rack.

Figure 1-5. Rack Mounting the Appliance



Appliance Precautions

- Determine the placement of each component in the rack before you install the rail.
- Install the heaviest appliance first at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.
- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near a socket outlet for easy access.
- Mount equipment into a rack with sufficient airflow for safe operation.
- For a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously may cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should only be used for extending the appliance out of the rack. These handles should not be used

for mounting the appliance on the rack. Rack-rail hardware described later should be used instead.

Installing Transceivers

The MPX appliances support both copper and fiber transceivers

Warning: Only those transceivers provided by Citrix Systems, Inc. are supported. You must not attempt to install third-party transceivers. Doing so voids the warranty.

To install the transceiver

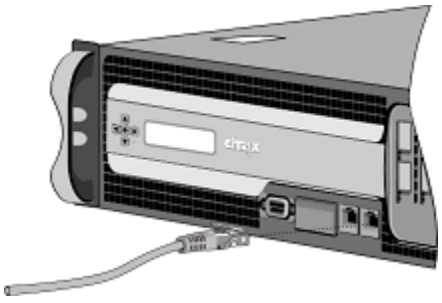
1. Carefully remove the transceiver from its box.
2. Align the transceiver to the front of the transceiver slot on the front panel of the appliance.
3. Hold the transceiver between your thumb and index finger and insert it into the transceiver slot, pressing it in until you hear the transceiver snap into place.
4. Lock the transceiver.

Note: To remove an SFP+ transceiver, you may first need to remove the SFP transceiver below it.

Connecting a NetScaler Appliance to the Network

Connect the interfaces on the appliance to the network ports on the appropriate switches by using Ethernet/fiber optic cables.

Figure 1-6. Connecting a Citrix NetScaler appliance to the network



Warning: Connecting multiple network ports to the same switch or VLAN can result in a network loop.

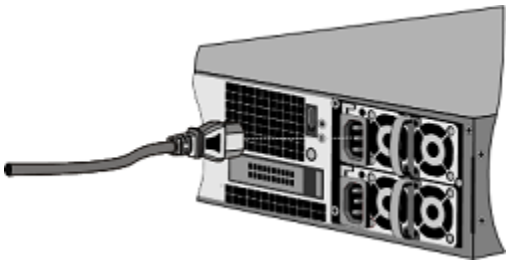
Note: By default, the NetScaler MPX appliance is configured to use auto-negotiation. When you install a NetScaler appliance for the first time, be sure to configure your other equipment to use auto-negotiation for the ports that are connected to the

NetScaler appliance. After initial logon and configuration, you can choose to disable auto-negotiation.

Connecting a NetScaler Appliance to a Power Source

Connect the power cable to one of the inlet receptacles on the back of the appliance and connect the other end of the power cable to a power outlet. If your appliance has a second power supply, repeat this process. All models function properly with a single power supply. The extra power supply on some models serves as a backup. The Citrix logo and LCD on the front of the NetScaler illuminate after the appliance starts, and the LCD indicates the operational status of the appliance.

Figure 1-7. Connecting a Citrix NetScaler appliance to a power source



Note: If you want to upgrade to the latest release of the system software before proceeding, see the *Citrix NetScaler Migration Guide*. For a link to the guide, see the Documentation Library of this guide.

Electrical Safety Precautions

Basic electrical safety precautions should be followed to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch. If an electrical accident occurs, you can quickly remove power to the appliance.
- Use a regulating uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, you should first shut down the appliance and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages may be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.

- Make sure that the power supply cords include grounding plugs and are plugged into grounded electrical outlets.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload.
- A reliable ground must be maintained at all times. Therefore, the rack should be grounded. Pay particular attention to power supply connections other than the direct connection to the branch circuit (for example, connections to power strips).

Setting Up Connectivity

Connect the appliance to a management workstation or the network by using the NetScaler configuration utility, the command-line interface (CLI), or the LCD keypad.

Configuration Utility Setup

To set up the appliance by using the configuration utility, you need a management workstation or laptop configured on the same network as the appliance. To run the configuration utility, the Java RunTime Environment (JRE) version 1.4.2_04 or later must be installed on the workstation or laptop.

Note: The Setup Wizard automatically opens upon log on when the appliance is configured with the default IP address, when licenses are not installed on the appliance, and when either the mapped IP address or subnet IP address is not configured.

To configure the NetScaler by using the configuration utility

1. Connect the NetScaler to a management workstation or network.
2. Open a browser and type: `http://192.168.100.1`

   Note: The NetScaler is preconfigured with the IP address 192.168.100.1.
3. In **User Name**, type `nsroot`.
4. In **Password**, type `nsroot`.
5. In the **Setup Wizard**, click **Next** and follow the instructions in the wizard.
6. To confirm that the NetScaler is configured correctly, you can either ping the new NetScaler IP address (NSIP) or use the new NSIP to open the configuration utility in a browser.

CLI Setup

To set up the appliance by using the command-line interface (CLI), connect the serial cable to the console port. Access the command line with a terminal or terminal emulator with the following settings:

- Baud rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Log on to the NetScaler with the following credentials:

User name: `nsroot`

Password: `nsroot`

To configure the NetScaler by using the NetScaler command line

At the NetScaler command prompt, type:

- **set ns config** -ipaddress<IPAddress> -netmask<subnetMask>
- **add ns ip**<IPAddress> <subnetMask> -type<type>
- **add route Network**<subnetMask> <gateway>
- **set system user**<userName> <password>
- **save ns config**
- **reboot**

Example

```
set ns config -ipaddress 10.102.29.60 -netmask
255.255.255.0 add ns ip 10.102.29.61 255.255.255.0 -
type snip add route 0.0.0.0 0.0.0.0 10.102.29.1 set
system user nsroot administrator save ns config
reboot
```

Note: For information about deploying a high availability (HA) pair, see the *Citrix NetScaler Networking Guide* at http://support.citrix.com/article/CTX132369.

LCD Keypad Setup

To set up the appliance by using the LCD keypad on the front panel of the appliance, enter the following initial settings in the following order:

1. subnet mask
2. NSIP
3. gateway

The NSIP and the default gateway should be on the same subnet.

The subnet mask, NSIP, and gateway values are saved in the configuration file. You can then use the NSIP to connect to the appliance remotely. For more information, see the *Citrix NetScaler Hardware Installation and Setup Guide* at http://support.citrix.com/article/CTX132365.

Note: For information about deploying a high availability (HA) pair, see the *Citrix NetScaler Networking Guide* at http://support.citrix.com/article/CTX132369.

System specifications

The following table summarizes the specifications of the NetScaler MPX 9700/10500/12500/15500 appliances.

Specifications	MPX 9700/10500/12500/15500
Processors	2 quad-core
Memory	16 GB
Number of power supplies	2
AC power supply input voltage, frequency, and current	100-240VAC 50-60 Hz 4.5-2.5A
DC power supply input voltage and current	-36 to -72VDC 14-7A
Maximum power consumption	450 W
Heat dissipation	1550 BTU per hour
Weight (lbs.)	31
Height	2U
Width	EIA 310-D for 19-inch racks
Depth	24.5 in/62 cms
Operating temperature (degree Celsius)	0-40
Humidity range (non-condensing)	5%-95%

Specifications	MPX 9700/10500/12500/15500
Safety certifications	CSA
EMC & susceptibility	FCC (Part 15 Class A), CE, C-Tick, VCCI
Environmental compliance	RoHS, WEEE

Additional Information

A complete set of documentation is available on the **Documentation** tab of your NetScaler and from http://support.citrix.com/. (Most of the documents require Adobe Reader, available at http://adobe.com/.)

To view the documentation

1. From a Web browser, log on to the NetScaler.
2. Click the **Documentation** tab.
3. To view a short description of each document, hover your cursor over the title. To open a document, click the title.

If you have support questions, please contact Citrix Technical Support at 1-800-4-CITRIX (1-800-424-8749). For additional contact information, see Support Phone Numbers at http://support.citrix.com/. If you have comments or feedback on this documentation, please email to nsdocs_feedback@citrix.com.

Citrix® NetScaler® 10 Quick Start Guide: MPX 11500/13500/14500/16500/18500/20500 Platform

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler appliance. If the NetScaler equipment causes interference, try to correct the interference by using one or more of the following measures:

Move the NetScaler equipment to one side or the other of your equipment.

Move the NetScaler equipment farther away from your equipment.

Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

Last Updated: March 2012

Document code: March 29 2012 10:36:14

Quick Installation and Configuration

Welcome to the Citrix NetScaler Application Delivery product line.

Please review the following information before proceeding with installation of the MPX appliance.

Before you Begin

Verify that the following components and accessories are included:

- One NetScaler MPX appliance
- One accessory kit that contains:
  - One RJ-45 to DB-9 adapter
  - One 6 ft RJ-45/DB-9 cable
  - One power cable for the MPX 5500 and MPX 7500/9500 appliances
  - Two power cables for the MPX 15000, MPX 17000, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances

    Note: Make sure that a power outlet is available for each cable.
- One mounting rail kit

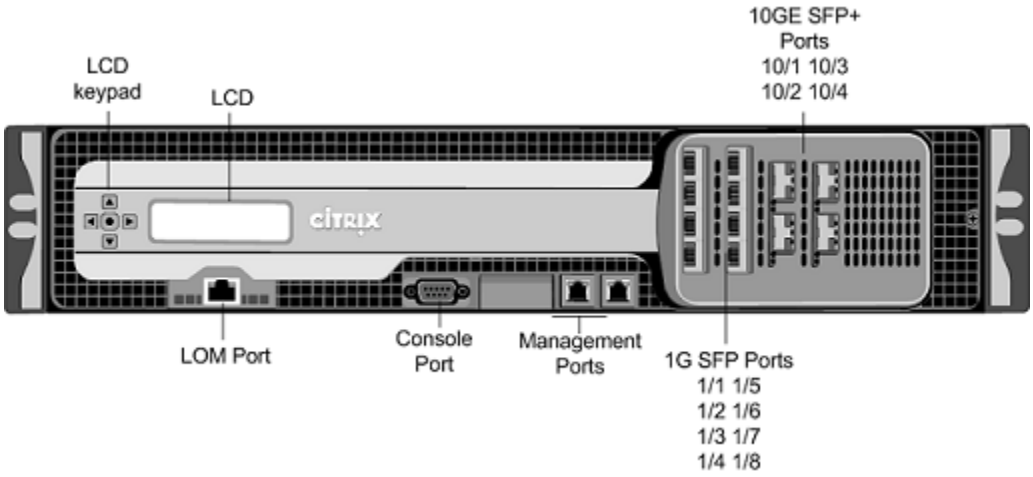
Note: SFP and SFP+ transceivers are sold separately. Contact your Citrix sales representative to order transceivers for your appliance. Only transceivers supplied by Citrix are supported on the appliance.

Citrix NetScaler MPX 11500, MPX 13500, MPX 14500, MPX 16500, MPX 18500, and MPX 20500

The Citrix NetScaler models MPX 11500/13500/14500/16500/18500/20500 are 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 48 gigabytes (GB) of memory.

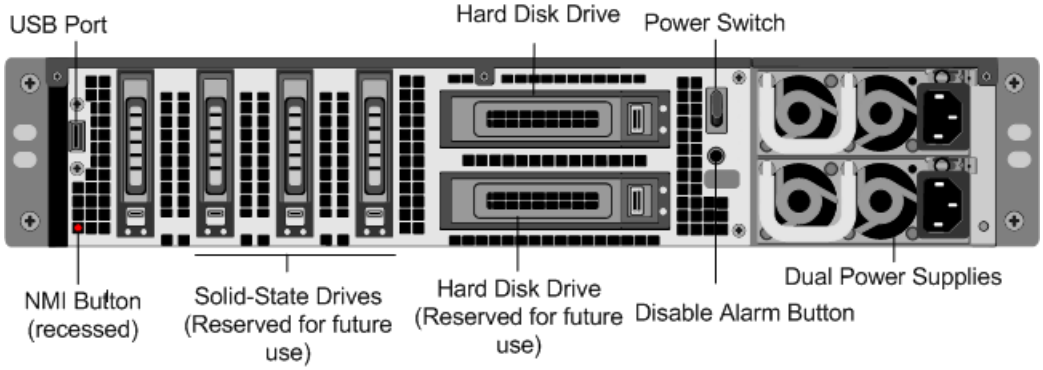
The following figure shows the front panel of the MPX 11500/13500/14500/16500/18500/20500 appliance.

Figure 1-1. Citrix NetScaler MPX 11500/13500/14500/16500/18500/20500 appliance, front panel



The following figure shows the back panel of the MPX 11500/13500/14500/16500/18500/20500 appliance.

Figure 1-2. Citrix NetScaler MPX 11500/13500/14500/16500/18500/20500 appliance, back panel



Configuration Requirements

Determine the following information for performing the initial configuration.

- NetScaler IP address: The management IP address of the appliance.
- Subnet IP address or Mapped IP address: The IP address used by the appliance to represent the client when communicating with a server.
- Default gateway: The IP address of the router that forwards traffic out of the appliance's subnet.
- Root password: The root user (nsroot) has full administrative privileges on the appliance. The root password is used to authenticate the root user.

Installation

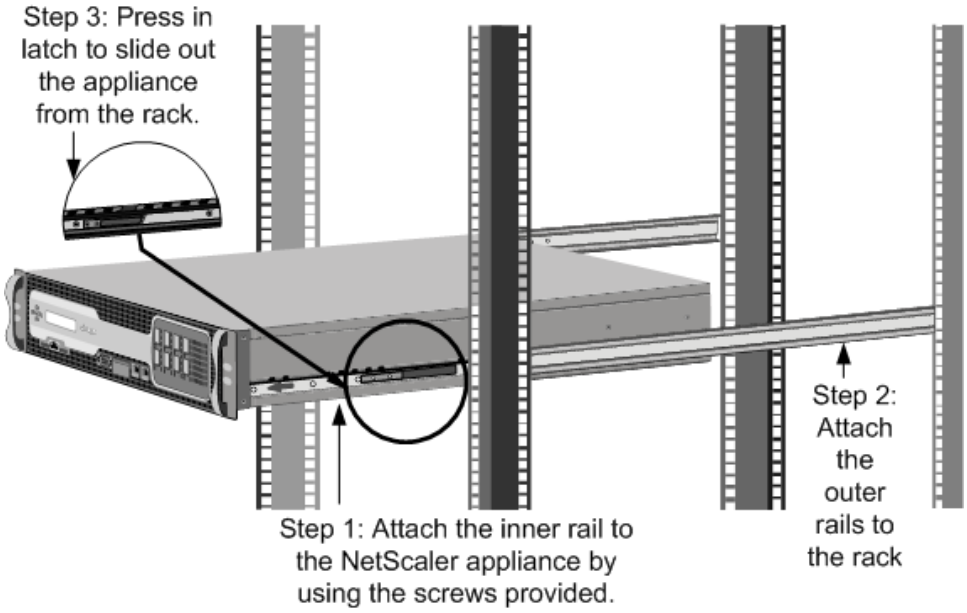
Installation involves rack-mounting the appliance, installing transceivers (if available), and connecting the appliance to the network and a power source.

Note: The appliances illustrated in the installation instructions may not represent the actual NetScaler appliance.

Rack Mounting a Citrix NetScaler Appliance

The appliance is shipped with rack-rail hardware. This hardware consists of two inner rails that you attach to the appliance, one on each side, and a rack-rail assembly that you attach to the rack. The following figure illustrates the steps involved in mounting the Citrix NetScaler appliance to a rack.

Figure 1-3. Rack Mounting the Appliance



Appliance Precautions

- Determine the placement of each component in the rack before you install the rail.
- Install the heaviest appliance first at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.
- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near a socket outlet for easy access.
- Mount equipment into a rack with sufficient airflow for safe operation.

- For a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously may cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should only be used for extending the appliance out of the rack. These handles should not be used for mounting the appliance on the rack. Rack-rail hardware described later should be used instead.

Installing Transceivers

The MPX appliances support both copper and fiber transceivers

Warning: Only those transceivers provided by Citrix Systems, Inc. are supported. You must not attempt to install third-party transceivers. Doing so voids the warranty.

To install the transceiver

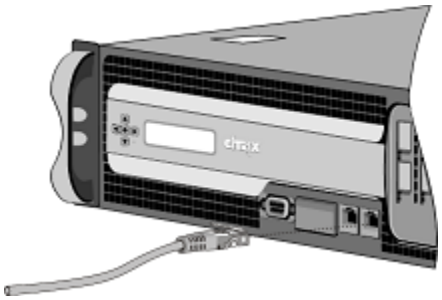
1. Carefully remove the transceiver from its box.
2. Align the transceiver to the front of the transceiver slot on the front panel of the appliance.
3. Hold the transceiver between your thumb and index finger and insert it into the transceiver slot, pressing it in until you hear the transceiver snap into place.
4. Lock the transceiver.

Note: To remove an SFP+ transceiver, you may first need to remove the SFP transceiver below it.

Connecting a NetScaler Appliance to the Network

Connect the interfaces on the appliance to the network ports on the appropriate switches by using Ethernet/fiber optic cables.

Figure 1-4. Connecting a Citrix NetScaler appliance to the network



Warning: Connecting multiple network ports to the same switch or VLAN can result in a network loop.

Note: By default, the NetScaler MPX appliance is configured to use auto-negotiation. When you install a NetScaler appliance for the first time, be sure to configure your other equipment to use auto-negotiation for the ports that are connected to the NetScaler appliance. After initial logon and configuration, you can choose to disable auto-negotiation.

Connecting a NetScaler Appliance to a Power Source

Connect the power cable to one of the inlet receptacles on the back of the appliance and connect the other end of the power cable to a power outlet. If your appliance has a second power supply, repeat this process. All models function properly with a single power supply. The extra power supply on some models serves as a backup. The Citrix logo and LCD on the front of the NetScaler illuminate after the appliance starts, and the LCD indicates the operational status of the appliance.

Figure 1-5. Connecting a Citrix NetScaler appliance to a power source

Note: If you want to upgrade to the latest release of the system software before proceeding, see the *Citrix NetScaler Migration Guide*. For a link to the guide, see the Documentation Library of this guide.

Electrical Safety Precautions

Basic electrical safety precautions should be followed to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch. If an electrical accident occurs, you can quickly remove power to the appliance.
- Use a regulating uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, you should first shut down the appliance and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages may be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Make sure that the power supply cords include grounding plugs and are plugged into grounded electrical outlets.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload.
- A reliable ground must be maintained at all times. Therefore, the rack should be grounded. Pay particular attention to power supply connections other than the direct connection to the branch circuit (for example, connections to power strips).

Setting Up Connectivity

Connect the appliance to a management workstation or the network by using the NetScaler configuration utility, the command-line interface (CLI), or the LCD keypad.

Configuration Utility Setup

To set up the appliance by using the configuration utility, you need a management workstation or laptop configured on the same network as the appliance. To run the configuration utility, the Java RunTime Environment (JRE) version 1.4.2_04 or later must be installed on the workstation or laptop.

Note: The Setup Wizard automatically opens upon log on when the appliance is configured with the default IP address, when licenses are not installed on the appliance, and when either the mapped IP address or subnet IP address is not configured.

To configure the NetScaler by using the configuration utility

1. Connect the NetScaler to a management workstation or network.
2. Open a browser and type: `http://192.168.100.1`

Note: The NetScaler is preconfigured with the IP address 192.168.100.1.

3. In **User Name**, type `nsroot`.
4. In **Password**, type `nsroot`.
5. In the **Setup Wizard**, click **Next** and follow the instructions in the wizard.
6. To confirm that the NetScaler is configured correctly, you can either ping the new NetScaler IP address (NSIP) or use the new NSIP to open the configuration utility in a browser.

CLI Setup

To set up the appliance by using the command-line interface (CLI), connect the serial cable to the console port. Access the command line with a terminal or terminal emulator with the following settings:

- Baud rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Log on to the NetScaler with the following credentials:

User name: `nsroot`

Password: `nsroot`

To configure the NetScaler by using the NetScaler command line

At the NetScaler command prompt, type:

- **set ns config** -ipaddress<IPAddress> -netmask<subnetMask>
- **add ns ip**<IPAddress> <subnetMask> -type<type>
- **add route Network**<subnetMask> <gateway>
- **set system user**<userName> <password>
- **save ns config**
- **reboot**

Example

```
set ns config -ipaddress 10.102.29.60 -netmask
255.255.255.0 add ns ip 10.102.29.61 255.255.255.0 -
type snip add route 0.0.0.0 0.0.0.0 10.102.29.1 set
```

```
system user nsroot administrator save ns config
reboot
```

Note: For information about deploying a high availability (HA) pair, see the *Citrix NetScaler Networking Guide* at http://support.citrix.com/article/CTX132369.

LCD Keypad Setup

To set up the appliance by using the LCD keypad on the front panel of the appliance, enter the following initial settings in the following order:

1. subnet mask
2. NSIP
3. gateway

The NSIP and the default gateway should be on the same subnet.

The subnet mask, NSIP, and gateway values are saved in the configuration file. You can then use the NSIP to connect to the appliance remotely. For more information, see the *Citrix NetScaler Hardware Installation and Setup Guide* at http://support.citrix.com/article/CTX132365.

Note: For information about deploying a high availability (HA) pair, see the *Citrix NetScaler Networking Guide* at http://support.citrix.com/article/CTX132369.

Configuring the LOM Port

For initial configuration of the LOM port, connect to the port's default IP address and change it to the address that you want to use for remote monitoring and management. Also specify the administrator credentials and the network settings.

Note: The LEDs on the LOM port are unoperational by design.

To configure the LOM port

1. In a Web browser, type the IP address of the LOM port. For initial configuration, type the port's default address: `http://192.168.1.3`
2. In the **User Name** and **Password** boxes, type the administrator credentials. You can obtain the initial user name and password from your sales representative or from Citrix Customer Service.
3. In the Menu bar, click **Configuration.**
4. Under **Options**, click **Network** and type values for the following parameters:

- IP Address—The IP address of the LOM port.
- Subnet Mask—The mask used to define the subnet of the LOM port.
- Default Gateway—The IP address of the router that connects the appliance to the network.

5. Click **Save.**

Power Cycling the Appliance

You can remotely turn off the appliance and turn it back on. The result is similar to pressing the power button on the back panel of the appliance for less than four seconds. The operating system performs a graceful shutdown. All operations on the appliance are stopped, no new connections to the client or server are accepted, and all the existing connections are closed.

To power cycle the appliance

1. In a Web browser, type the IP address of the LOM port.
2. In the **User Name** and **Password** boxes, type the administrator credentials.
3. In the **Menu** bar, click **Remote Control**.
4. Under **Options**, click **Power Control**, and then click **Power Cycle Server**.
5. Click **Perform Action**.

System Specifications

The following table summarizes the specifications of the NetScaler MPX 11500/13500/14500/16500/18500/20500 appliances.

Specifications	**MPX 11500/13500/14500/16500/18500/20500**
Processor	2 six-core
Memory	48 GB
Number of power supplies	2
AC power supply input voltage, frequency, and current	100-240 VAC 50-60 Hz

Specifications	MPX 11500/13500/14500/16500/18500/20500
	6.5-3.5 A
Maximum power consumption	650 W
Heat dissipation	2200 BTU per hour
Weight	46 lbs
Height	2U
Width	EIA 310-D for 19-inch racks
Depth	28 in or 71.68 cm
Operating temperature (degree Celsius)	0-40
Humidity range (non-condensing)	5%-95%
Safety certifications	CSA
EMC & susceptibility	FCC (Part 15 Class A), CE, C-Tick, VCCI, CCC, KC, NOM, GOST, SABS, SASO
Environmental compliance	RoHS, SVHC, WEEE

Additional Information

A complete set of documentation is available on the **Documentation** tab of your NetScaler and from http://support.citrix.com/. (Most of the documents require Adobe Reader, available at http://adobe.com/.)

To view the documentation

1. From a Web browser, log on to the NetScaler.
2. Click the **Documentation** tab.
3. To view a short description of each document, hover your cursor over the title. To open a document, click the title.

If you have support questions, please contact Citrix Technical Support at 1-800-4-CITRIX (1-800-424-8749). For additional contact information, see Support Phone Numbers at

http://support.citrix.com/. If you have comments or feedback on this documentation, please email to nsdocs_feedback@citrix.com.

Citrix® NetScaler® 10 Quick Start Guide: MPX 17500/19500/21500 Platform

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler appliance. If the NetScaler equipment causes interference, try to correct the interference by using one or more of the following measures:

Move the NetScaler equipment to one side or the other of your equipment.

Move the NetScaler equipment farther away from your equipment.

Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

Last Updated: March 2012

Document code: March 29 2012 10:34:39

Quick Installation and Configuration

Welcome to the Citrix NetScaler Application Delivery product line.

Please review the following information before proceeding with installation of the MPX appliance.

Before you Begin

Verify that the following components and accessories are included:

- One NetScaler MPX appliance
- One accessory kit that contains:
  - One RJ-45 to DB-9 adapter
  - One 6 ft RJ-45/DB-9 cable
  - One power cable for the MPX 5500 and MPX 7500/9500 appliances
  - Two power cables for the MPX 15000, MPX 17000, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances

  Note: Make sure that a power outlet is available for each cable.
- One mounting rail kit

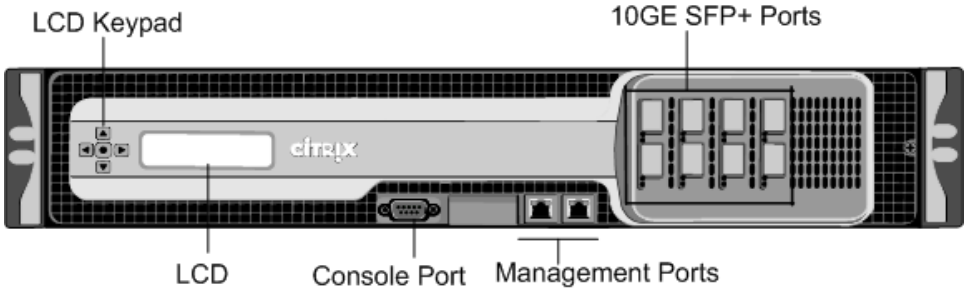
Note: SFP and SFP+ transceivers are sold separately. Contact your Citrix sales representative to order transceivers for your appliance. Only transceivers supplied by Citrix are supported on the appliance.

Citrix NetScaler MPX 17500, MPX 19500, and MPX 21500

The Citrix NetScaler models MPX 17500/19500/21500 are 2U appliances. Each model has two 6-core processors and 48 gigabytes (GB) of memory.

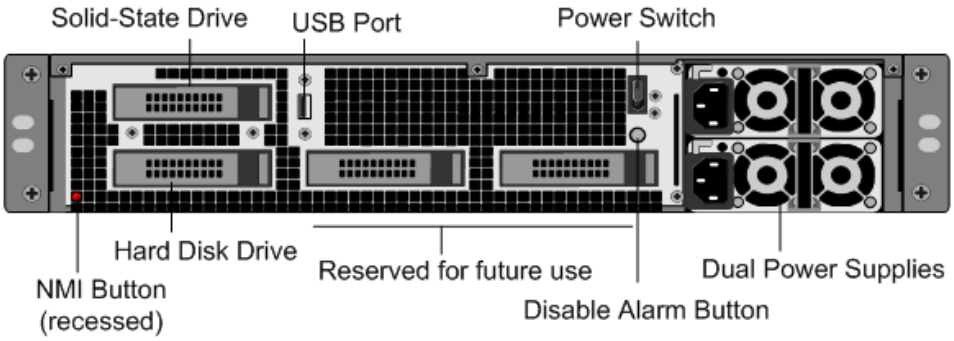
The following figure shows the front panel of the MPX 17500/19500/21500 appliance.

Figure 1-1. Citrix NetScaler MPX 17500/19500/21500 appliance, front panel



The following figure shows the back panel of the MPX 17500/19500/21500 appliance.

Figure 1-2. Citrix NetScaler MPX 17500/19500/21500 appliance, back panel



Configuration Requirements

Determine the following information for performing the initial configuration.

- NetScaler IP address: The management IP address of the appliance.
- Subnet IP address or Mapped IP address: The IP address used by the appliance to represent the client when communicating with a server.
- Default gateway: The IP address of the router that forwards traffic out of the appliance's subnet.
- Root password: The root user (nsroot) has full administrative privileges on the appliance. The root password is used to authenticate the root user.

Installation

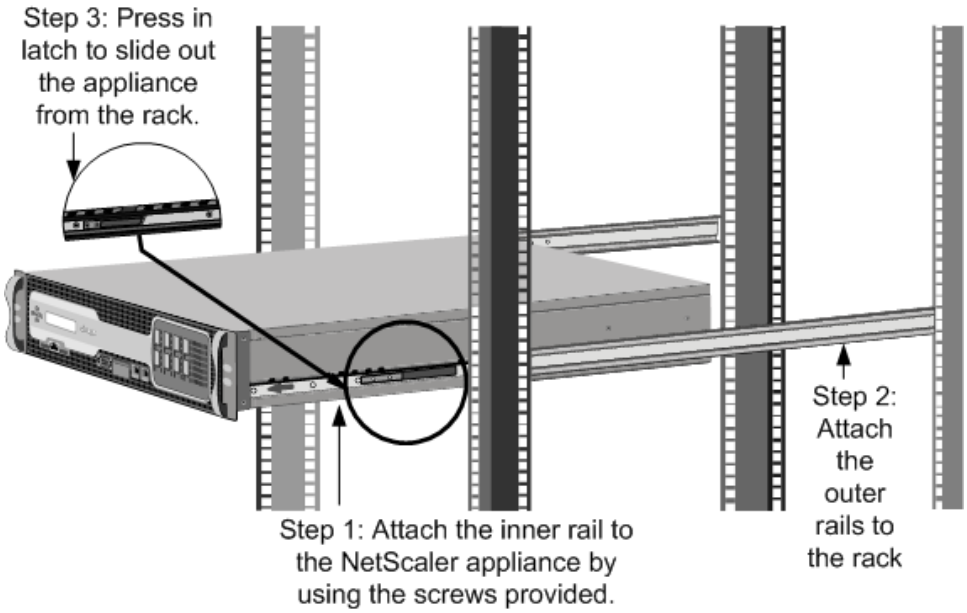
Installation involves rack-mounting the appliance, installing transceivers (if available), and connecting the appliance to the network and a power source.

Note: The appliances illustrated in the installation instructions may not represent the actual NetScaler appliance.

Rack Mounting a Citrix NetScaler Appliance

The appliance is shipped with rack-rail hardware. This hardware consists of two inner rails that you attach to the appliance, one on each side, and a rack-rail assembly that you attach to the rack. The following figure illustrates the steps involved in mounting the Citrix NetScaler appliance to a rack.

Figure 1-3. Rack Mounting the Appliance



Appliance Precautions

- Determine the placement of each component in the rack before you install the rail.
- Install the heaviest appliance first at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.
- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near a socket outlet for easy access.
- Mount equipment into a rack with sufficient airflow for safe operation.
- For a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously may cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should only be used for extending the appliance out of the rack. These handles should not be used

for mounting the appliance on the rack. Rack-rail hardware described later should be used instead.

Installing Transceivers

The MPX appliances support both copper and fiber transceivers

Warning: Only those transceivers provided by Citrix Systems, Inc. are supported. You must not attempt to install third-party transceivers. Doing so voids the warranty.

To install the transceiver

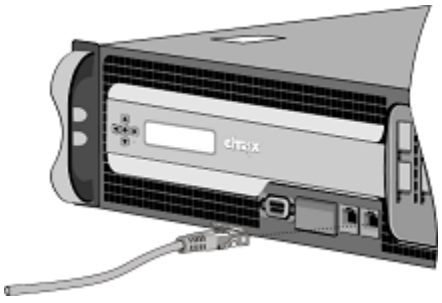
1. Carefully remove the transceiver from its box.
2. Align the transceiver to the front of the transceiver slot on the front panel of the appliance.
3. Hold the transceiver between your thumb and index finger and insert it into the transceiver slot, pressing it in until you hear the transceiver snap into place.
4. Lock the transceiver.

Note: To remove an SFP+ transceiver, you may first need to remove the SFP transceiver below it.

Connecting a NetScaler Appliance to the Network

Connect the interfaces on the appliance to the network ports on the appropriate switches by using Ethernet/fiber optic cables.

Figure 1-4. Connecting a Citrix NetScaler appliance to the network



Warning: Connecting multiple network ports to the same switch or VLAN can result in a network loop.

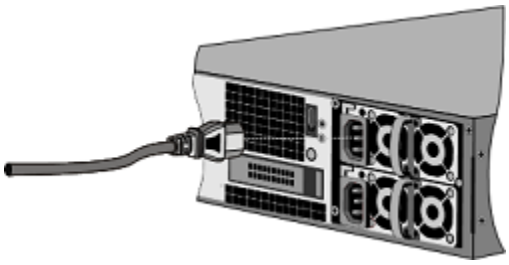
Note: By default, the NetScaler MPX appliance is configured to use auto-negotiation. When you install a NetScaler appliance for the first time, be sure to configure your other equipment to use auto-negotiation for the ports that are connected to the

NetScaler appliance. After initial logon and configuration, you can choose to disable auto-negotiation.

Connecting a NetScaler Appliance to a Power Source

Connect the power cable to one of the inlet receptacles on the back of the appliance and connect the other end of the power cable to a power outlet. If your appliance has a second power supply, repeat this process. All models function properly with a single power supply. The extra power supply on some models serves as a backup. The Citrix logo and LCD on the front of the NetScaler illuminate after the appliance starts, and the LCD indicates the operational status of the appliance.

Figure 1-5. Connecting a Citrix NetScaler appliance to a power source



Note: If you want to upgrade to the latest release of the system software before proceeding, see the *Citrix NetScaler Migration Guide*. For a link to the guide, see the Documentation Library of this guide.

Electrical Safety Precautions

Basic electrical safety precautions should be followed to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch. If an electrical accident occurs, you can quickly remove power to the appliance.
- Use a regulating uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, you should first shut down the appliance and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages may be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.

- Make sure that the power supply cords include grounding plugs and are plugged into grounded electrical outlets.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload.
- A reliable ground must be maintained at all times. Therefore, the rack should be grounded. Pay particular attention to power supply connections other than the direct connection to the branch circuit (for example, connections to power strips).

Setting Up Connectivity

Connect the appliance to a management workstation or the network by using the NetScaler configuration utility, the command-line interface (CLI), or the LCD keypad.

Configuration Utility Setup

To set up the appliance by using the configuration utility, you need a management workstation or laptop configured on the same network as the appliance. To run the configuration utility, the Java RunTime Environment (JRE) version 1.4.2_04 or later must be installed on the workstation or laptop.

Note: The Setup Wizard automatically opens upon log on when the appliance is configured with the default IP address, when licenses are not installed on the appliance, and when either the mapped IP address or subnet IP address is not configured.

To configure the NetScaler by using the configuration utility

1. Connect the NetScaler to a management workstation or network.
2. Open a browser and type: `http://192.168.100.1`

   Note: The NetScaler is preconfigured with the IP address 192.168.100.1.
3. In **User Name**, type `nsroot`.
4. In **Password**, type `nsroot`.
5. In the **Setup Wizard**, click **Next** and follow the instructions in the wizard.
6. To confirm that the NetScaler is configured correctly, you can either ping the new NetScaler IP address (NSIP) or use the new NSIP to open the configuration utility in a browser.

CLI Setup

To set up the appliance by using the command-line interface (CLI), connect the serial cable to the console port. Access the command line with a terminal or terminal emulator with the following settings:

- Baud rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Log on to the NetScaler with the following credentials:

User name: `nsroot`

Password: `nsroot`

To configure the NetScaler by using the NetScaler command line

At the NetScaler command prompt, type:

- **set ns config** -ipaddress<IPAddress> -netmask<subnetMask>
- **add ns ip**<IPAddress> <subnetMask> -type<type>
- **add route Network**<subnetMask> <gateway>
- **set system user**<userName> <password>
- **save ns config**
- **reboot**

Example

```
set ns config -ipaddress 10.102.29.60 -netmask
255.255.255.0 add ns ip 10.102.29.61 255.255.255.0 -
type snip add route 0.0.0.0 0.0.0.0 10.102.29.1 set
system user nsroot administrator save ns config
reboot
```

Note: For information about deploying a high availability (HA) pair, see the *Citrix NetScaler Networking Guide* at http://support.citrix.com/article/CTX132369.

LCD Keypad Setup

To set up the appliance by using the LCD keypad on the front panel of the appliance, enter the following initial settings in the following order:

1. subnet mask
2. NSIP
3. gateway

The NSIP and the default gateway should be on the same subnet.

The subnet mask, NSIP, and gateway values are saved in the configuration file. You can then use the NSIP to connect to the appliance remotely. For more information, see the *Citrix NetScaler Hardware Installation and Setup Guide* at http://support.citrix.com/article/CTX132365.

Note: For information about deploying a high availability (HA) pair, see the *Citrix NetScaler Networking Guide* at http://support.citrix.com/article/CTX132369.

System Specifications

The following table summarizes the specifications of the NetScaler MPX 17500/19500/21500 appliances.

Specifications	MPX 17500/19500/21500
Processors	2, each with 6 cores (24 with hyper-threading)
Memory	48 GB
Number of power supplies	2
AC power supply input voltage, frequency, and current	100-240 VAC 50-60 Hz 6.5-3.5 A
Maximum power consumption	650 W
Heat dissipation	2200 BTU per hour
Weight	40 lbs
Height	2U
Width	EIA 310-D for 19-inch racks
Depth	24.75 in or 62.865 cm
Operating temperature (degree Celsius)	0-40
Humidity range (non-condensing)	5%-95%

Specifications	MPX 17500/19500/21500
Safety certifications	TUV
EMC & susceptibility	FCC (Part 15 Class A), CE, C-Tick, VCCI-A
Environmental compliance	RoHS, WEEE

Additional Information

A complete set of documentation is available on the **Documentation** tab of your NetScaler and from http://support.citrix.com/. (Most of the documents require Adobe Reader, available at http://adobe.com/.)

To view the documentation

1. From a Web browser, log on to the NetScaler.
2. Click the **Documentation** tab.
3. To view a short description of each document, hover your cursor over the title. To open a document, click the title.

If you have support questions, please contact Citrix Technical Support at 1-800-4-CITRIX (1-800-424-8749). For additional contact information, see Support Phone Numbers at http://support.citrix.com/. If you have comments or feedback on this documentation, please email to nsdocs_feedback@citrix.com.

Citrix® NetScaler® 10 Quick Start Guide: MPX 17550/19550/20550/21550 Platform

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler appliance. If the NetScaler equipment causes interference, try to correct the interference by using one or more of the following measures:

Move the NetScaler equipment to one side or the other of your equipment.

Move the NetScaler equipment farther away from your equipment.

Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

Last Updated: March 2012

Document code: March 29 2012 10:35:11

Quick Installation and Configuration

Welcome to the Citrix NetScaler Application Delivery product line.

Please review the following information before proceeding with installation of the MPX appliance.

Before you Begin

Verify that the following components and accessories are included:

- One NetScaler MPX appliance
- One accessory kit that contains:
  - One RJ-45 to DB-9 adapter
  - One 6 ft RJ-45/DB-9 cable
  - One power cable for the MPX 5500 and MPX 7500/9500 appliances
  - Two power cables for the MPX 15000, MPX 17000, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances

    Note: Make sure that a power outlet is available for each cable.
- One mounting rail kit

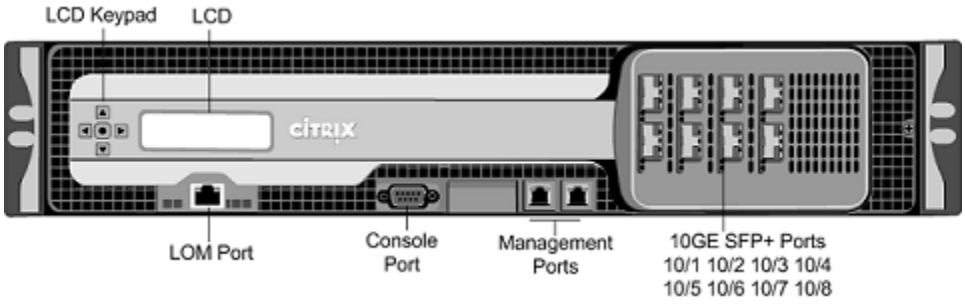
Note: SFP and SFP+ transceivers are sold separately. Contact your Citrix sales representative to order transceivers for your appliance. Only transceivers supplied by Citrix are supported on the appliance.

Citrix NetScaler MPX 17550, MPX 19550, MPX 20550, and MPX 21550

The Citrix NetScaler models MPX 17550, MPX 19550, MPX 20550, and MPX 21550 are 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 96 gigabytes (GB) of memory.

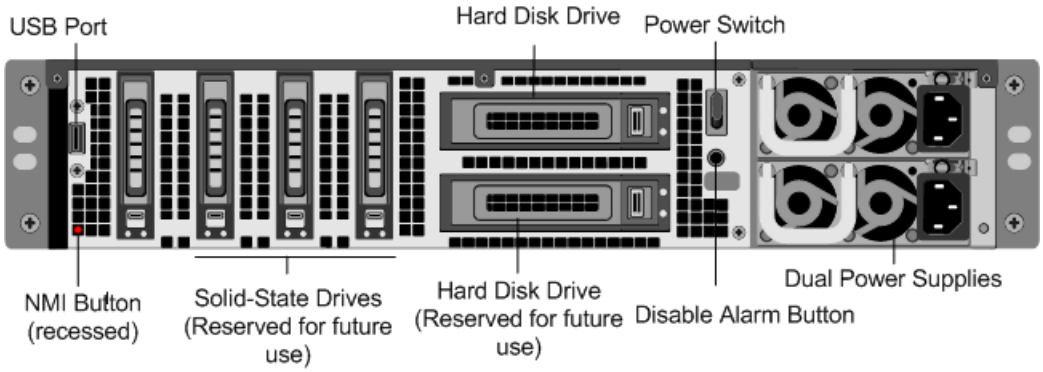
The following figure shows the front panel of the MPX 17550/19550/20550/21550 appliance.

Figure 1-1. Citrix NetScaler MPX 17550/19550/20550/21550 appliance, front panel



The following figure shows the back panel of the MPX 17550/19550/20550/21550 appliance.

Figure 1-2. Citrix NetScaler MPX 17550/19550/20550/21550 appliance, back panel



Configuration Requirements

Determine the following information for performing the initial configuration.

- NetScaler IP address: The management IP address of the appliance.
- Subnet IP address or Mapped IP address: The IP address used by the appliance to represent the client when communicating with a server.
- Default gateway: The IP address of the router that forwards traffic out of the appliance's subnet.
- Root password: The root user (nsroot) has full administrative privileges on the appliance. The root password is used to authenticate the root user.

Installation

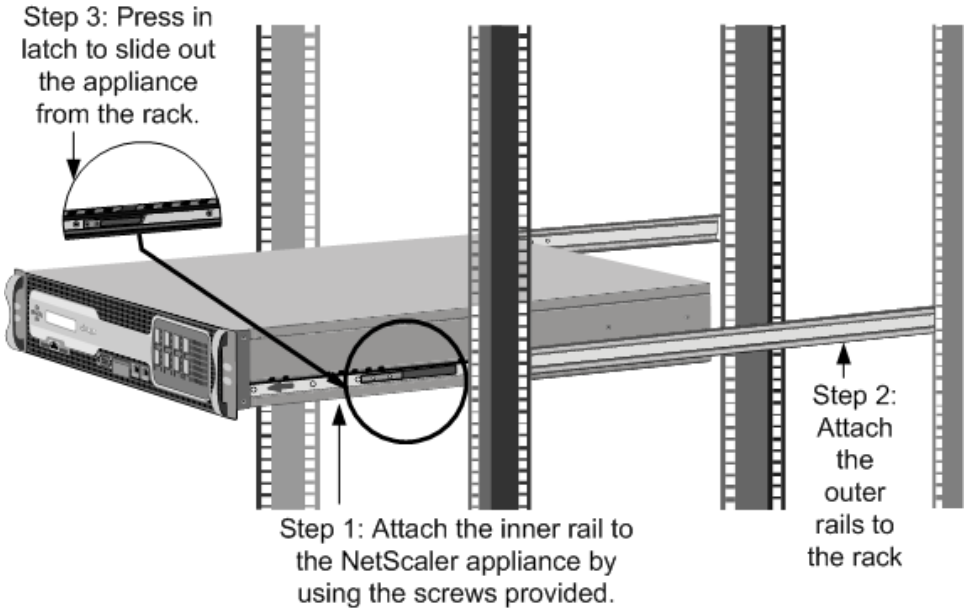
Installation involves rack-mounting the appliance, installing transceivers (if available), and connecting the appliance to the network and a power source.

Note: The appliances illustrated in the installation instructions may not represent the actual NetScaler appliance.

Rack Mounting a Citrix NetScaler Appliance

The appliance is shipped with rack-rail hardware. This hardware consists of two inner rails that you attach to the appliance, one on each side, and a rack-rail assembly that you attach to the rack. The following figure illustrates the steps involved in mounting the Citrix NetScaler appliance to a rack.

Figure 1-3. Rack Mounting the Appliance



Appliance Precautions

- Determine the placement of each component in the rack before you install the rail.
- Install the heaviest appliance first at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.
- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near a socket outlet for easy access.
- Mount equipment into a rack with sufficient airflow for safe operation.
- For a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

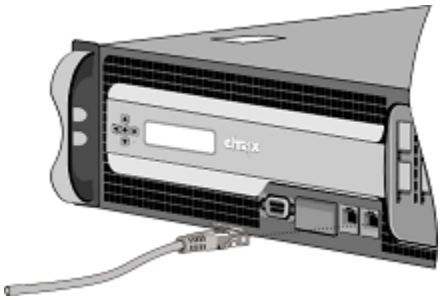
Rack Precautions

- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously may cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should only be used for extending the appliance out of the rack. These handles should not be used for mounting the appliance on the rack. Rack-rail hardware described later should be used instead.

Connecting a NetScaler Appliance to the Network

Connect the interfaces on the appliance to the network ports on the appropriate switches by using Ethernet/fiber optic cables.

Figure 1-4. Connecting a Citrix NetScaler appliance to the network



Warning: Connecting multiple network ports to the same switch or VLAN can result in a network loop.

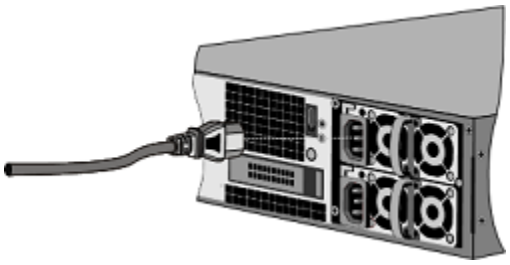
Note: By default, the NetScaler MPX appliance is configured to use auto-negotiation. When you install a NetScaler appliance for the first time, be sure to configure your other equipment to use auto-negotiation for the ports that are connected to the NetScaler appliance. After initial logon and configuration, you can choose to disable auto-negotiation.

Connecting a NetScaler Appliance to a Power Source

Connect the power cable to one of the inlet receptacles on the back of the appliance and connect the other end of the power cable to a power outlet. If your appliance has a second power supply, repeat this process. All models function properly with a single

power supply. The extra power supply on some models serves as a backup. The Citrix logo and LCD on the front of the NetScaler illuminate after the appliance starts, and the LCD indicates the operational status of the appliance.

Figure 1-5. Connecting a Citrix NetScaler appliance to a power source



Note: If you want to upgrade to the latest release of the system software before proceeding, see the *Citrix NetScaler Migration Guide*. For a link to the guide, see the Documentation Library of this guide.

Electrical Safety Precautions

Basic electrical safety precautions should be followed to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch. If an electrical accident occurs, you can quickly remove power to the appliance.
- Use a regulating uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, you should first shut down the appliance and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages may be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Make sure that the power supply cords include grounding plugs and are plugged into grounded electrical outlets.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload.
- A reliable ground must be maintained at all times. Therefore, the rack should be grounded. Pay particular attention to power supply connections other than the direct connection to the branch circuit (for example, connections to power strips).

Setting Up Connectivity

Connect the appliance to a management workstation or the network by using the NetScaler configuration utility, the command-line interface (CLI), or the LCD keypad.

Configuration Utility Setup

To set up the appliance by using the configuration utility, you need a management workstation or laptop configured on the same network as the appliance. To run the configuration utility, the Java RunTime Environment (JRE) version 1.4.2_04 or later must be installed on the workstation or laptop.

Note: The Setup Wizard automatically opens upon log on when the appliance is configured with the default IP address, when licenses are not installed on the appliance, and when either the mapped IP address or subnet IP address is not configured.

To configure the NetScaler by using the configuration utility

1. Connect the NetScaler to a management workstation or network.
2. Open a browser and type: `http://192.168.100.1`

   Note: The NetScaler is preconfigured with the IP address 192.168.100.1.
3. In **User Name**, type `nsroot`.
4. In **Password**, type `nsroot`.
5. In the **Setup Wizard**, click **Next** and follow the instructions in the wizard.
6. To confirm that the NetScaler is configured correctly, you can either ping the new NetScaler IP address (NSIP) or use the new NSIP to open the configuration utility in a browser.

CLI Setup

To set up the appliance by using the command-line interface (CLI), connect the serial cable to the console port. Access the command line with a terminal or terminal emulator with the following settings:

- Baud rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Log on to the NetScaler with the following credentials:

User name: `nsroot`

Password: `nsroot`

To configure the NetScaler by using the NetScaler command line

At the NetScaler command prompt, type:

- **set ns config** -ipaddress<IPAddress> -netmask<subnetMask>
- **add ns ip**<IPAddress> <subnetMask> -type<type>
- **add route Network**<subnetMask> <gateway>
- **set system user**<userName> <password>
- **save ns config**
- **reboot**

Example

```
set ns config -ipaddress 10.102.29.60 -netmask
255.255.255.0 add ns ip 10.102.29.61 255.255.255.0 -
type snip add route 0.0.0.0 0.0.0.0 10.102.29.1 set
system user nsroot administrator save ns config
reboot
```

Note: For information about deploying a high availability (HA) pair, see the *Citrix NetScaler Networking Guide* at http://support.citrix.com/article/CTX132369.

LCD Keypad Setup

To set up the appliance by using the LCD keypad on the front panel of the appliance, enter the following initial settings in the following order:

1. subnet mask
2. NSIP
3. gateway

The NSIP and the default gateway should be on the same subnet.

The subnet mask, NSIP, and gateway values are saved in the configuration file. You can then use the NSIP to connect to the appliance remotely. For more information, see the *Citrix NetScaler Hardware Installation and Setup Guide* at http://support.citrix.com/article/CTX132365.

Note: For information about deploying a high availability (HA) pair, see the *Citrix NetScaler Networking Guide* at http://support.citrix.com/article/CTX132369.

Configuring the LOM Port

For initial configuration of the LOM port, connect to the port's default IP address and change it to the address that you want to use for remote monitoring and management. Also specify the administrator credentials and the network settings.

Note: The LEDs on the LOM port are unoperational by design.

To configure the LOM port

1. In a Web browser, type the IP address of the LOM port. For initial configuration, type the port's default address: `http://192.168.1.3`
2. In the **User Name** and **Password** boxes, type the administrator credentials. You can obtain the initial user name and password from your sales representative or from Citrix Customer Service.
3. In the Menu bar, click **Configuration.**
4. Under **Options**, click **Network** and type values for the following parameters:
   - IP Address—The IP address of the LOM port.
   - Subnet Mask—The mask used to define the subnet of the LOM port.
   - Default Gateway—The IP address of the router that connects the appliance to the network.
5. Click **Save.**

Power Cycling the Appliance

You can remotely turn off the appliance and turn it back on. The result is similar to pressing the power button on the back panel of the appliance for less than four seconds. The operating system performs a graceful shutdown. All operations on the appliance are stopped, no new connections to the client or server are accepted, and all the existing connections are closed.

To power cycle the appliance

1. In a Web browser, type the IP address of the LOM port.
2. In the **User Name** and **Password** boxes, type the administrator credentials.
3. In the **Menu** bar, click **Remote Control**.
4. Under **Options**, click **Power Control**, and then click **Power Cycle Server**.
5. Click **Perform Action**.

System Specifications

The following table summarizes the specifications of the NetScaler MPX 17550/19550/20550/21550 appliances.

Specifications	MPX 17550/19550/20550/21550
Processors	two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading)
Memory	96 GB
Number of power supplies	2
AC power supply input voltage, frequency, and current	100-240 VAC 50-60 Hz 6.5-3.5 A
Maximum power consumption	850 W
Heat dissipation	2900 BTU per hour
Weight	40 lbs
Height	2U
Width	EIA 310-D for 19-inch racks
Depth	24.75 in or 62.865 cm
Operating temperature (degree Celsius)	0-40
Humidity range (non-condensing)	5%-95%
Safety certifications	TUV
EMC & susceptibility	FCC (Part 15 Class A), CE, C-Tick, VCCI-A
Environmental compliance	RoHS, WEEE

Additional Information

A complete set of documentation is available on the **Documentation** tab of your NetScaler and from http://support.citrix.com/. (Most of the documents require Adobe Reader, available at http://adobe.com/.)

To view the documentation

1. From a Web browser, log on to the NetScaler.
2. Click the **Documentation** tab.
3. To view a short description of each document, hover your cursor over the title. To open a document, click the title.

If you have support questions, please contact Citrix Technical Support at 1-800-4-CITRIX (1-800-424-8749). For additional contact information, see Support Phone Numbers at http://support.citrix.com/. If you have comments or feedback on this documentation, please email to nsdocs_feedback@citrix.com.

Citrix® NetScaler® 10 Quick Start Guide: MPX 15000/17000 Platform

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler appliance. If the NetScaler equipment causes interference, try to correct the interference by using one or more of the following measures:

Move the NetScaler equipment to one side or the other of your equipment.

Move the NetScaler equipment farther away from your equipment.

Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

Last Updated: March 2012

Document code: March 29 2012 10:34:08

Quick Installation and Configuration

Welcome to the Citrix NetScaler Application Delivery product line.

Please review the following information before proceeding with installation of the MPX appliance.

Before you Begin

Verify that the following components and accessories are included:

- One NetScaler MPX appliance
- One accessory kit that contains:
  - One RJ-45 to DB-9 adapter
  - One 6 ft RJ-45/DB-9 cable
  - One power cable for the MPX 5500 and MPX 7500/9500 appliances
  - Two power cables for the MPX 15000, MPX 17000, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances

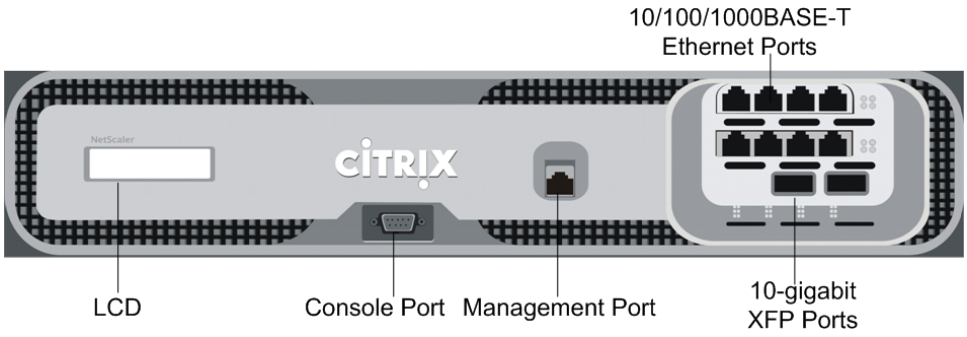
    Note: Make sure that a power outlet is available for each cable.
- One mounting rail kit

Note: SFP and SFP+ transceivers are sold separately. Contact your Citrix sales representative to order transceivers for your appliance. Only transceivers supplied by Citrix are supported on the appliance.

Citrix NetScaler MPX 15000 15000/17000

The following figure shows the front panel of the MPX 15000/17000 appliance.

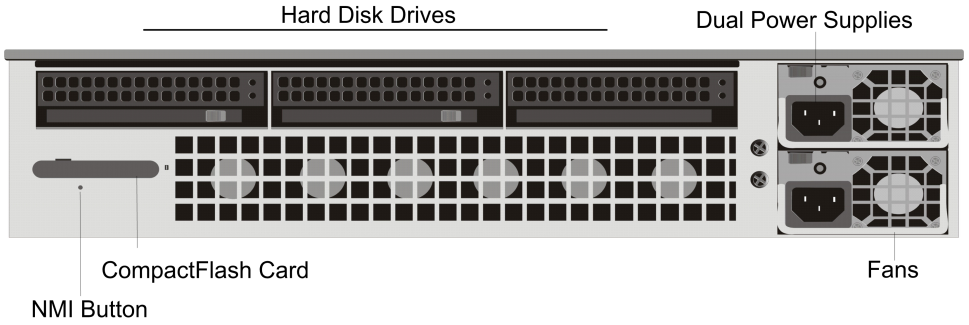
Figure 1-1. Citrix NetScaler MPX 15000/17000 appliance, front panel



Note: The MPX 17000 and MPX 15000 appliances come with other interface offerings. For more information, see the MPX Series data sheet.

The following figure shows the back panel of the MPX 15000/17000 appliance.

Figure 1-2. Citrix NetScaler MPX 15000/17000 appliance, back panel



Configuration Requirements

Determine the following information for performing the initial configuration.

- NetScaler IP address: The management IP address of the appliance.
- Subnet IP address or Mapped IP address: The IP address used by the appliance to represent the client when communicating with a server.
- Default gateway: The IP address of the router that forwards traffic out of the appliance's subnet.
- Root password: The root user (nsroot) has full administrative privileges on the appliance. The root password is used to authenticate the root user.

Installation

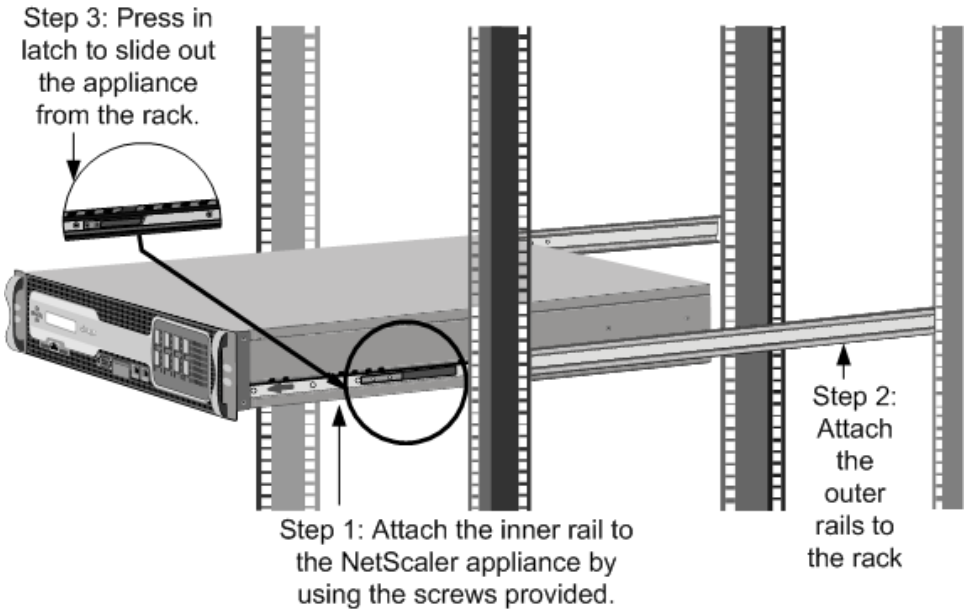
Installation involves rack-mounting the appliance, installing transceivers (if available), and connecting the appliance to the network and a power source.

Note: The appliances illustrated in the installation instructions may not represent the actual NetScaler appliance.

Rack Mounting a Citrix NetScaler Appliance

The appliance is shipped with rack-rail hardware. This hardware consists of two inner rails that you attach to the appliance, one on each side, and a rack-rail assembly that you attach to the rack. The following figure illustrates the steps involved in mounting the Citrix NetScaler appliance to a rack.

Figure 1-3. Rack Mounting the Appliance



Appliance Precautions

- Determine the placement of each component in the rack before you install the rail.
- Install the heaviest appliance first at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.
- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near a socket outlet for easy access.
- Mount equipment into a rack with sufficient airflow for safe operation.
- For a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously may cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should only be used for extending the appliance out of the rack. These handles should not be used

for mounting the appliance on the rack. Rack-rail hardware described later should be used instead.

Installing Transceivers

The MPX appliances support both copper and fiber transceivers

Warning: Only those transceivers provided by Citrix Systems, Inc. are supported. You must not attempt to install third-party transceivers. Doing so voids the warranty.

To install the transceiver

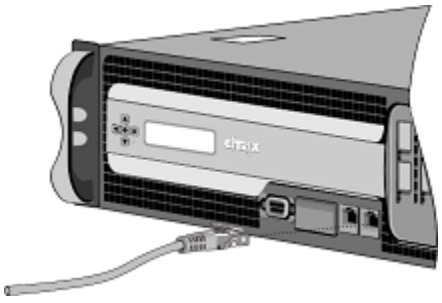
1. Carefully remove the transceiver from its box.
2. Align the transceiver to the front of the transceiver slot on the front panel of the appliance.
3. Hold the transceiver between your thumb and index finger and insert it into the transceiver slot, pressing it in until you hear the transceiver snap into place.
4. Lock the transceiver.

Note: To remove an SFP+ transceiver, you may first need to remove the SFP transceiver below it.

Connecting a NetScaler Appliance to the Network

Connect the interfaces on the appliance to the network ports on the appropriate switches by using Ethernet/fiber optic cables.

Figure 1-4. Connecting a Citrix NetScaler appliance to the network



Warning: Connecting multiple network ports to the same switch or VLAN can result in a network loop.

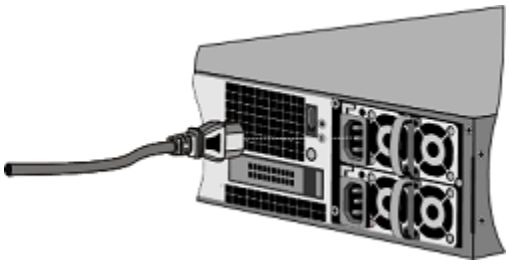
Note: By default, the NetScaler MPX appliance is configured to use auto-negotiation. When you install a NetScaler appliance for the first time, be sure to configure your other equipment to use auto-negotiation for the ports that are connected to the

NetScaler appliance. After initial logon and configuration, you can choose to disable auto-negotiation.

Connecting a NetScaler Appliance to a Power Source

Connect the power cable to one of the inlet receptacles on the back of the appliance and connect the other end of the power cable to a power outlet. If your appliance has a second power supply, repeat this process. All models function properly with a single power supply. The extra power supply on some models serves as a backup. The Citrix logo and LCD on the front of the NetScaler illuminate after the appliance starts, and the LCD indicates the operational status of the appliance.

Figure 1-5. Connecting a Citrix NetScaler appliance to a power source



Note: If you want to upgrade to the latest release of the system software before proceeding, see the *Citrix NetScaler Migration Guide*. For a link to the guide, see the Documentation Library of this guide.

Electrical Safety Precautions

Basic electrical safety precautions should be followed to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch. If an electrical accident occurs, you can quickly remove power to the appliance.
- Use a regulating uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, you should first shut down the appliance and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages may be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.

- Make sure that the power supply cords include grounding plugs and are plugged into grounded electrical outlets.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload.
- A reliable ground must be maintained at all times. Therefore, the rack should be grounded. Pay particular attention to power supply connections other than the direct connection to the branch circuit (for example, connections to power strips).

Setting Up Connectivity

Connect the appliance to a management workstation or the network by using the NetScaler configuration utility or the command-line interface (CLI).

Configuration Utility Setup

To set up the appliance by using the configuration utility, you need a management workstation or laptop configured on the same network as the appliance. To run the configuration utility, the Java RunTime Environment (JRE) version 1.4.2_04 or later must be installed on the workstation or laptop.

Note: The Setup Wizard automatically opens upon log on when the appliance is configured with the default IP address, when licenses are not installed on the appliance, and when either the mapped IP address or subnet IP address is not configured.

To configure the NetScaler by using the configuration utility

1. Connect the NetScaler to a management workstation or network.
2. Open a browser and type: `http://192.168.100.1`

   Note: The NetScaler is preconfigured with the IP address 192.168.100.1.
3. In **User Name**, type `nsroot`.
4. In **Password**, type `nsroot`.
5. In the **Setup Wizard**, click **Next** and follow the instructions in the wizard.
6. To confirm that the NetScaler is configured correctly, you can either ping the new NetScaler IP address (NSIP) or use the new NSIP to open the configuration utility in a browser.

CLI Setup

To set up the appliance by using the command-line interface (CLI), connect the serial cable to the console port. Access the command line with a terminal or terminal emulator with the following settings:

- Baud rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Log on to the NetScaler with the following credentials:

User name: `nsroot`

Password: `nsroot`

To configure the NetScaler by using the NetScaler command line

At the NetScaler command prompt, type:

- **set ns config** -ipaddress<IPAddress> -netmask<subnetMask>
- **add ns ip**<IPAddress> <subnetMask> -type<type>
- **add route Network**<subnetMask> <gateway>
- **set system user**<userName> <password>
- **save ns config**
- **reboot**

Example

```
set ns config -ipaddress 10.102.29.60 -netmask
255.255.255.0 add ns ip 10.102.29.61 255.255.255.0 -
type snip add route 0.0.0.0 0.0.0.0 10.102.29.1 set
system user nsroot administrator save ns config
reboot
```

Note: For information about deploying a high availability (HA) pair, see the *Citrix NetScaler Networking Guide* at http://support.citrix.com/article/CTX132369.

System Specifications

The following table summarizes the specifications of the NetScaler MPX 15000/17000 appliances.

Specifications	MPX 15000	MPX 17000
Processors	2 quad-core	2 quad-core

Specifications	MPX 15000	MPX 17000
Memory	16 GB	32 GB
Number of power supplies	2	2
AC power supply input voltage, frequency, and current	100-240VAC 47-63Hz	100-240VAC 47-63Hz
DC power supply input voltage and current	700W	700W
Maximum power consumption		
Heat dissipation	52	52
Weight (lbs.)	2U	2U
Height	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks
Width	18.5 in/ 47 cm	18.5 in/ 47 cm
Depth	0-35	0-35
Operating temperature (degree Celsius)	5%-95%	5%-95%
Humidity range (non-condensing)	UL & TUV-C	UL & TUV-C
Safety certifications	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES
EMC & susceptibility	RoHS, WEEE	RoHS, WEEE

Specifications	MPX 15000	MPX 17000
Environmental compliance	RoHS, WEEE	

Additional Information

A complete set of documentation is available on the **Documentation** tab of your NetScaler and from http://support.citrix.com/. (Most of the documents require Adobe Reader, available at http://adobe.com/.)

To view the documentation

1. From a Web browser, log on to the NetScaler.
2. Click the **Documentation** tab.
3. To view a short description of each document, hover your cursor over the title. To open a document, click the title.

If you have support questions, please contact Citrix Technical Support at 1-800-4-CITRIX (1-800-424-8749). For additional contact information, see Support Phone Numbers at http://support.citrix.com/. If you have comments or feedback on this documentation, please email to nsdocs_feedback@citrix.com.

Citrix NetScaler 10 Quick Start Guide: SDX 11500/13500/14500/16500/18500/20500 Platform

Citrix NetScaler 10

Last Updated: June 2013

Document code: August 27 2013 06:37:49

Quick Installation and Configuration

Welcome to the Citrix NetScaler Application Delivery product line.

Please review the following information before proceeding with installation of the SDX appliance.

Before you Begin

Verify that the following components and accessories are included:

- One NetScaler SDX appliance
- One accessory kit that contains:
  - One RJ-45 to DB-9 adapter
  - One 6 ft RJ-45/DB-9 cable
  - Two power cables

    Note: Make sure that a power outlet is available for each cable.
- One standard 4-post rail kit

  Note: If the kit that you received does not fit your rack, contact your Citrix sales representative to order the appropriate kit.

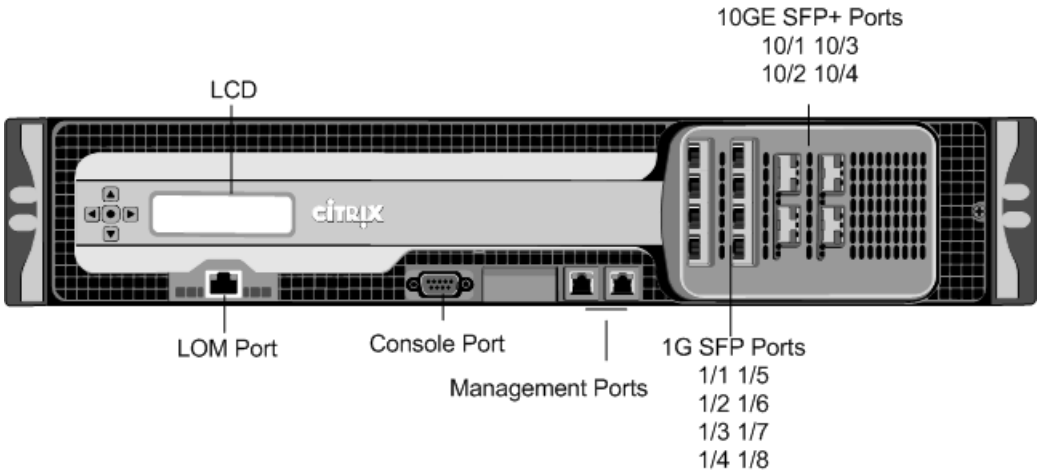
Note: 1G SFP and 10G SFP+ transceivers are sold separately. Contact your Citrix sales representative to order transceivers for your appliance. Only transceivers supplied by Citrix are supported on the appliance.

Citrix NetScaler SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500, and SDX 20500

The Citrix NetScaler models SDX 11500/13500/14500/16500/18500/20500 are 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 48 gigabytes (GB) of memory.

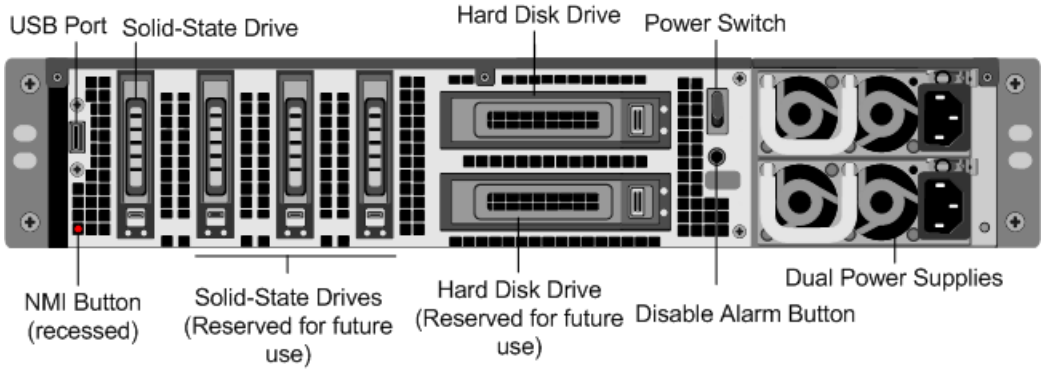
The following figure shows the front panel of the SDX 11500/13500/14500/16500/18500/20500 appliance.

Figure 1-1. Citrix NetScaler SDX 11500/13500/14500/16500/18500/20500 appliance, front panel



The following figure shows the back panel of the SDX 11500/13500/14500/16500/18500/20500 appliance.

Figure 1-2. Citrix NetScaler SDX 11500/13500/14500/16500/18500/20500 appliance, back panel



Configuration Requirements

Determine the following information for performing the initial configuration.

- NetScaler SDX IP address and subnet mask: The management IP address and the mask used to define the subnet in which the SDX appliance is located. This IP address is used to access the NetScaler SDX Management Service user interface.
- XenServer IP address: The IP address of the XenServer hypervisor.
- Default gateway: The IP address of the router that forwards traffic out of the appliance's subnet. The default gateway should be in the same subnet as the NSIP address.

- Root password: The root user (nsroot) has full administrative privileges on the appliance. The root password is used to authenticate the root user. The default root password is nsroot. You can change this password during initial configuration of the appliance.

Installation

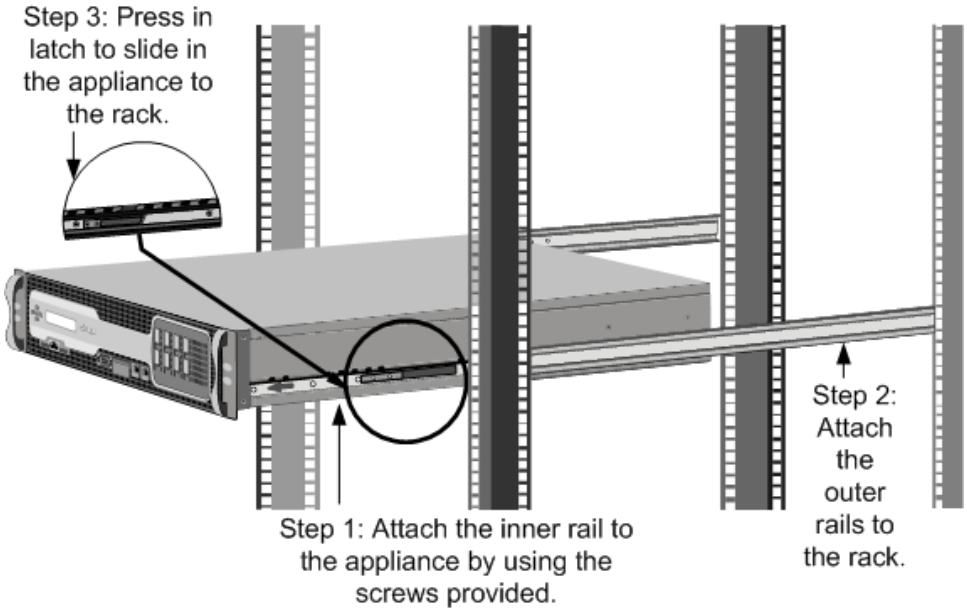
Installation involves rack-mounting the appliance, installing transceivers (if available), and connecting the appliance to the network and a power source.

Note: The appliances illustrated in the installation instructions might not represent the actual NetScaler SDX appliance.

Rack Mounting the Appliance

The appliance is shipped with rack-rail hardware. This hardware consists of two inner rails that you attach to the appliance, one on each side, and a rack-rail assembly that you attach to the rack. The following figure illustrates the steps involved in mounting the Citrix NetScaler SDX appliance to a rack.

Figure 1-3. Rack Mounting the Appliance



Appliance Precautions

- Determine the placement of each component in the rack before you install the rail.
- Install the heaviest appliance first, at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.

- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near an electrical outlet for easy access.
- Mount equipment in a rack with sufficient airflow for safe operation.
- For a closed or multiple-unit rack assembly, the ambient operating temperature of the rack environment might be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously might cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should be used only for extending the appliance out of the rack. Do not use these handles for mounting the appliance on the rack.

Installing Transceivers

The SDX appliances support only fiber transceivers in the 10GE ports.

👉 **Warning:** Only those transceivers provided by Citrix Systems, Inc. are supported. You must not attempt to install third-party transceivers. Doing so voids the warranty.

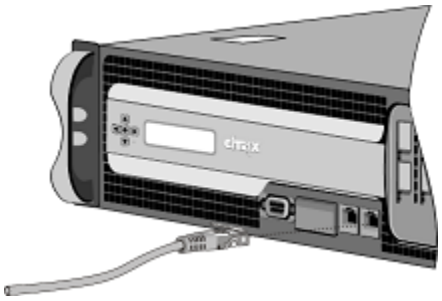
To install the transceiver

1. Carefully remove the transceiver from its box.
2. Align the transceiver to the front of the transceiver slot on the front panel of the appliance.
3. Hold the transceiver between your thumb and index finger and insert it into the transceiver slot, pressing it in until you hear the transceiver snap into place.
4. Lock the transceiver.

Connecting a NetScaler SDX Appliance to the Network

Connect the interfaces on the appliance to the network ports on the appropriate switches by using Ethernet/fiber optic cables.

Figure 1-4. Connecting a Citrix NetScaler SDX appliance to the network



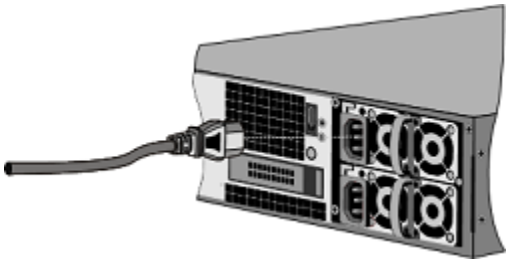
👉 **Warning:** Connecting multiple network ports to the same switch or VLAN can result in a network loop.

Note: By default, the NetScaler SDX appliance is configured to use auto-negotiation. When you install a NetScaler appliance for the first time, be sure to configure your other equipment to use auto-negotiation for the ports that are connected to the NetScaler appliance. After initial logon and configuration, you can choose to disable auto-negotiation.

Connecting an SDX Appliance to a Power Source

Connect the power cable to one of the inlet receptacles on the back of the appliance and connect the other end of the power cable to a power outlet. If your appliance has more than one power supply, repeat this process. All models function properly with a single power supply. The extra power supply on some models serves as a backup.

Figure 1-5. Connecting a Citrix NetScaler SDX appliance to a power source



Note:

Electrical Safety Precautions

⚠ **Caution:** During installation or maintenance procedures, wear a grounding wrist strap to avoid ESD damage to the electronics of the appliance. Use a conductive wrist strap attached to a good earth ground or to the appliance. You can attach it to the connector beside the ESD symbol on the back.

Basic electrical safety precautions should be followed to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch, so that you can quickly remove power to the appliance if an electrical accident occurs.
- Use a regulated, uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. First shut down the appliance, and then unplug the power cords of all the power supply units. As long as the power cord is plugged in, line voltages can be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Make sure that the power supply cords include grounding plugs and are plugged into grounded electrical outlets.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload.
- A reliable ground must be maintained at all times. Therefore, the rack should be grounded. Pay particular attention to power supply connections other than the direct connection to the branch circuit (for example, connections to power strips).

Setting Up Connectivity

After you have installed your appliance in a rack, you are ready to perform the initial configuration. To perform the initial configuration, you can use the Management Service user interface or the serial console. You can access the Management Service user interface from any computer that is on the same network as the new SDX appliance. If you do not have a computer on the same network, use the serial console to perform the initial configuration of the SDX appliance. Citrix recommends that, as soon as you complete the initial configuration, you change the root-user password. For information about changing the root-user password, see Changing the Password of the Default User Account.

Initial Configuration through the Management Service User Interface

To set up the appliance by using the Management Service user interface, connect a workstation or laptop to the same network as the appliance.

To configure the NetScaler SDX appliance by using the Management Service user interface

1. Connect the NetScaler SDX appliance to a management workstation or network by using interface 0/1.
2. Open a browser and type: `http://192.168.100.1`

   Note: The SDX Management Service is preconfigured with the IP address 192.168.100.1 and the XenServer hypervisor is preconfigured with the IP address 192.168.100.2.
3. In the **User Name** box, type `nsroot`.
4. In the **Password** box, type `nsroot`.
5. In the navigation pane, click **System**.
6. In the details pane, under **System Administration**, click **Network Configuration** and enter values for the following parameters:
   - Interface*—The management interface that connects the appliance to a management workstation or network. Possible values: 0/1, 0/2. Default: 0/1.
   - XenServer IP Address*—The IP address of the XenServer.
   - Management VM IP Address*—The IP address that is used to access the Management Service by using a Web browser.

     Note: The XenServer IP address and Management Service IP address should be in the same subnet.
   - Netmask*—The mask used to define the subnet in which the SDX appliance is located.
   - Gateway*—The IP address of the router that forwards traffic out of the appliance's subnet.
   - DNS Server—The IP address of the DNS server.

   *A required parameter
7. Click **OK**, and then click **Close.**
8. To confirm that the NetScaler SDX appliance is configured correctly, you can either ping the new Management Service IP address or use the new IP address to open the user interface in a browser.

Note: After changing the network configuration, close all browser instances and open a new browser instance to access the appliance.

Initial Configuration through the Serial Console

To perform initial configuration of the SDX appliance from outside the L2 domain, connect to the console port of the appliance and follow the instructions carefully.

Note: `networkconfig` utility is available from build 72.5 and later.

To configure the NetScaler SDX appliance by using the serial console

1. Connect the console cable into your appliance.
2. Connect the other end of the cable to your computer and run the vt100 terminal emulation program of your choice.
   - For Microsoft Windows, you can use HyperTerminal, which is installed with all current versions of Windows.
   - For Apple Macintosh OSX, you can use the GUI-based Terminal program or the shell-based telnet client.

     Note: OSX is based on the FreeBSD UNIX platform. Most standard UNIX shell programs are available from the OSX command line.
   - For UNIX-based workstations, you can use the shell-based telnet client or any supported terminal emulation program.
3. Press ENTER.
   The terminal screen displays the Logon prompt.

   Note: You might have to press ENTER two or three times, depending on which terminal program you are using.
4. Log on to the appliance with the administrator credentials. The default credentials for username and password are root and nsroot respectively.
5. At the prompt, type:
   `ssh nsroot@169.254.0.10`
   When prompted for the password, type `nsroot`.
6. At the shell prompt, type:
   `networkconfig`

You can now use the new IP address to log on to the Management Service user interface.

Changing the Password of the Default User Account

The default user account provides complete access to all features of the Citrix NetScaler SDX appliance. Therefore, to preserve security, the nsroot account should be used only when necessary, and only individuals whose duties require full access should know the password for the nsroot account. Citrix recommends changing the nsroot password frequently. If you lose the password, you can reset the password to the default by reverting the appliance settings to factory defaults , and you can then change the password.

You can change the password of the default user account in the **Users** pane. In the **Users** pane, you can view the following details:

Name
Lists the user accounts configured on the SDX appliance.

Permission
Displays the permission level assigned to the user account.

To change the password of the default user account

1. On the **Configuration** tab, in the navigation pane, expand **System**, and then click **Users**.
2. In the **Users** pane, click the default user account, and then click **Modify**.
3. In the **Modify System User** dialog box, in **Password** and **Confirm Password**, enter the password of your choice.
4. Click **OK**.

Configuring the LOM Port

For initial configuration of the lights-out management (LOM) port, connect to the port's default IP address and change it to the address that you want to use for remote monitoring and management. Also specify the administrator credentials and the network settings.

Note: The LEDs on the LOM port are unoperational by design.

To Configure the NetScaler LOM Port

1. Connect the NetScaler LOM port to a management workstation or network.
2. In a web browser, type: http://192.168.1.3.

   Note: The NetScaler LOM port is preconfigured with the IP address 192.168.1.3 and subnet mask 255.255.255.0.
3. In the **User Name** box, type **nsroot**.

4. In the **Password** box, type **nsroot**.
5. In the **Configuration** tab, click **Network** and type values for the following parameters:
   - IP Address—IP address of the LOM port.
   - Subnet Mask—Subnet mask used to define the subnet of the LOM port.
   - Default Gateway—IP address of the router that connects the LOM port to the network.
6. Click **Save**.

Power Cycling the Appliance

You can remotely turn off the appliance and turn it back on. The result is similar to pressing the power button on the back panel of the appliance for less than four seconds.

Note: Power cycling the appliance by using the LOM port is not supported in the current release.

To power cycle the appliance

1. In a web browser, type the IP address of the LOM port.
2. In the **User Name** and **Password** boxes, type the administrator credentials.
3. In the **Menu** bar, click **Remote Control**.
4. Under **Options**, click **Power Control**, and then click **Power Cycle System**.
5. Click **Perform Action**.

System Specifications

The following table summarizes the specifications of the NetScaler SDX 11500/13500/14500/16500/18500/20500 appliances.

Specifications	SDX 11500/13500/14500/16500/18500/20500
Processor	2 six-core
Memory	48 GB

Specifications	SDX 11500/13500/14500/16500/18500/20500
Number of power supplies	2
AC power supply input voltage, frequency, and current	100-240 VAC 50-60 Hz 6.5-3.5 A
Maximum power consumption	650 W
Heat dissipation	2200 BTU per hour
Weight	46 lbs
Height	2U
Width	EIA 310-D for 19-inch racks
Depth	28 in or 71.68 cm
Operating temperature (degree Celsius)	0-40
Humidity range (non-condensing)	5%-95%
Safety certifications	CSA
EMC & susceptibility	FCC (Part 15 Class A), CE, C-Tick, VCCI, CCC, KC, NOM, GOST, SABS, SASO
Environmental compliance	RoHS, SVHC, WEEE

Additional Information

A complete set of documentation is available on the **Documentation** tab of your SDX appliance and from http://support.citrix.com/. (Most of the documents require Adobe Reader, available at http://adobe.com/.)

To view the documentation

1. From a web browser, log on to the NetScaler SDX appliance.

2. Click the **Documentation** tab.
3. To view a short description of each document, hover your cursor over the title. To open a document, click the title.

To contact Citrix Support, call 1-800-4-CITRIX (1-800-424-8749), or log on to MyCitrix at http://www.citrix.com. You will be asked for your hardware serial number as part of the support process.

Detailed instructions for contacting support can be found at: http://citrix.com/site/resources/dynamic/sup2nd/Citrix_HWS_SerialNO.pdf.

If you have comments or feedback on this documentation, please send email to nsdocs_feedback@citrix.com.

Citrix® NetScaler® 10 Quick Start Guide: SDX 17500/19500/21500 Platform

Last Updated: June 2013

Document code: August 27 2013 06:38:04

Quick Installation and Configuration

Welcome to the Citrix NetScaler Application Delivery product line.

Please review the following information before proceeding with installation of the SDX appliance.

Before you Begin

Verify that the following components and accessories are included:

- One NetScaler SDX appliance
- One accessory kit that contains:
  - One RJ-45 to DB-9 adapter
  - One 6 ft RJ-45/DB-9 cable
  - Two power cables

    Note: Make sure that a power outlet is available for each cable.
- One standard 4-post rail kit

  Note: If the kit that you received does not fit your rack, contact your Citrix sales representative to order the appropriate kit.

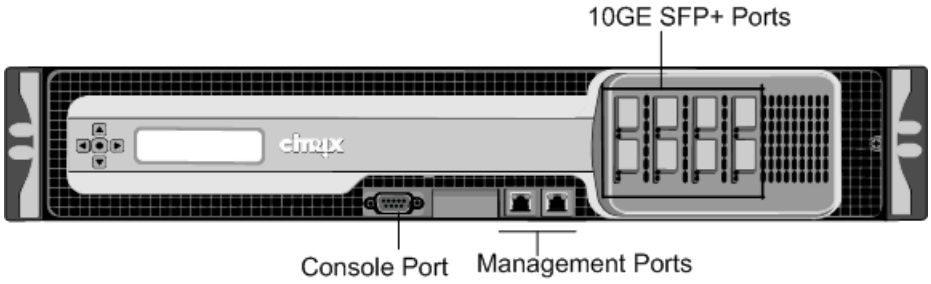
Note: 1G SFP and 10G SFP+ transceivers are sold separately. Contact your Citrix sales representative to order transceivers for your appliance. Only transceivers supplied by Citrix are supported on the appliance.

Citrix NetScaler SDX 17500, SDX 19500, and SDX 21500

The Citrix NetScaler models SDX 17500/19500/21500 are 2U appliances. Each model has two 6-core processors and 48 gigabytes (GB) of memory.

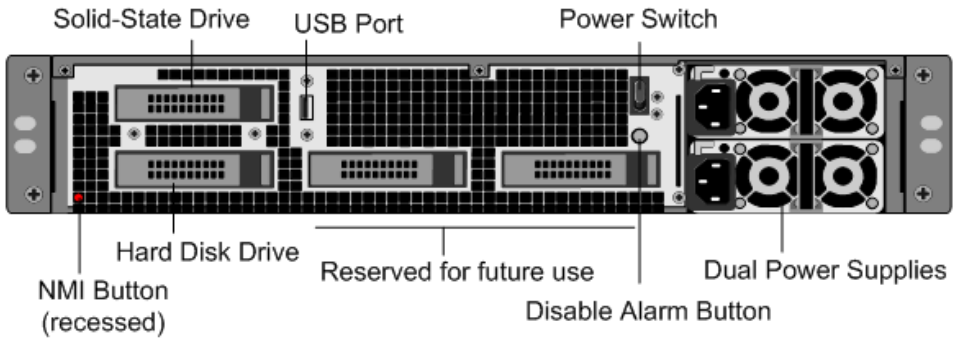
The following figure shows the front panel of the SDX 17500/19500/21500 appliance.

Figure 1-1. Citrix NetScaler SDX 17500/19500/21500 appliance, front panel



The following figure shows the back panel of the SDX 17500/19500/21500 appliance.

Figure 1-2. Citrix NetScaler SDX 17500/19500/21500 appliance, back panel



Configuration Requirements

Determine the following information for performing the initial configuration.

- NetScaler SDX IP address and subnet mask: The management IP address and the mask used to define the subnet in which the SDX appliance is located. This IP address is used to access the NetScaler SDX Management Service user interface.
- XenServer IP address: The IP address of the XenServer hypervisor.
- Default gateway: The IP address of the router that forwards traffic out of the appliance's subnet. The default gateway should be in the same subnet as the NSIP address.
- Root password: The root user (nsroot) has full administrative privileges on the appliance. The root password is used to authenticate the root user. The default root password is nsroot. You can change this password during initial configuration of the appliance.

Installation

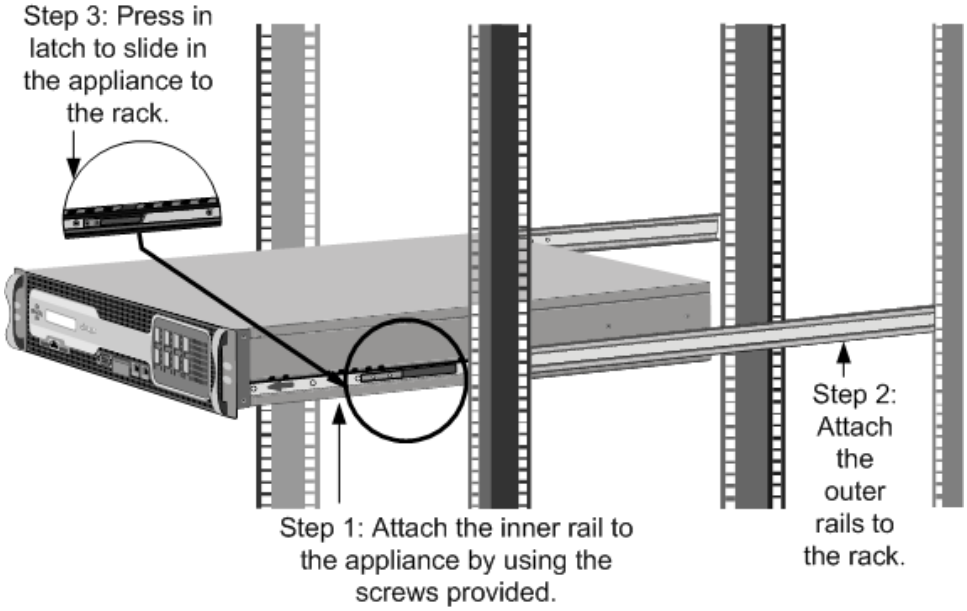
Installation involves rack-mounting the appliance, installing transceivers (if available), and connecting the appliance to the network and a power source.

Note: The appliances illustrated in the installation instructions might not represent the actual NetScaler SDX appliance.

Rack Mounting the Appliance

The appliance is shipped with rack-rail hardware. This hardware consists of two inner rails that you attach to the appliance, one on each side, and a rack-rail assembly that you attach to the rack. The following figure illustrates the steps involved in mounting the Citrix NetScaler SDX appliance to a rack.

Figure 1-3. Rack Mounting the Appliance



Appliance Precautions

- Determine the placement of each component in the rack before you install the rail.
- Install the heaviest appliance first, at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.
- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near an electrical outlet for easy access.
- Mount equipment in a rack with sufficient airflow for safe operation.
- For a closed or multiple-unit rack assembly, the ambient operating temperature of the rack environment might be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously might cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should be used only for extending the appliance out of the rack. Do not use these handles for mounting the appliance on the rack.

Installing Transceivers

The SDX appliances support only fiber transceivers in the 10GE ports.

Warning: Only those transceivers provided by Citrix Systems, Inc. are supported. You must not attempt to install third-party transceivers. Doing so voids the warranty.

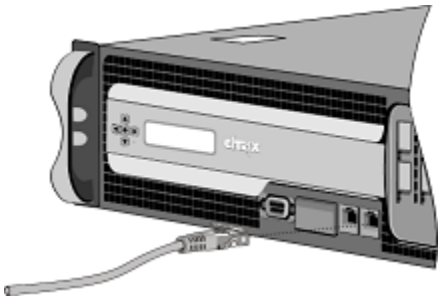
To install the transceiver

1. Carefully remove the transceiver from its box.
2. Align the transceiver to the front of the transceiver slot on the front panel of the appliance.
3. Hold the transceiver between your thumb and index finger and insert it into the transceiver slot, pressing it in until you hear the transceiver snap into place.
4. Lock the transceiver.

Connecting a NetScaler SDX Appliance to the Network

Connect the interfaces on the appliance to the network ports on the appropriate switches by using Ethernet/fiber optic cables.

Figure 1-4. Connecting a Citrix NetScaler SDX appliance to the network



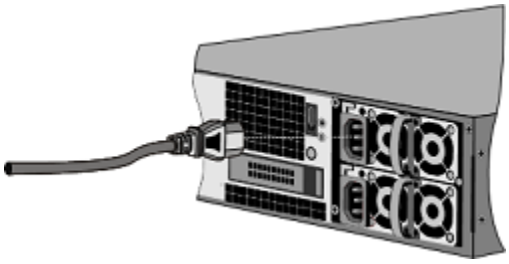
Warning: Connecting multiple network ports to the same switch or VLAN can result in a network loop.

Note: By default, the NetScaler SDX appliance is configured to use auto-negotiation. When you install a NetScaler appliance for the first time, be sure to configure your other equipment to use auto-negotiation for the ports that are connected to the NetScaler appliance. After initial logon and configuration, you can choose to disable auto-negotiation.

Connecting an SDX Appliance to a Power Source

Connect the power cable to one of the inlet receptacles on the back of the appliance and connect the other end of the power cable to a power outlet. If your appliance has more than one power supply, repeat this process. All models function properly with a single power supply. The extra power supply on some models serves as a backup.

Figure 1-5. Connecting a Citrix NetScaler SDX appliance to a power source



Note:

Electrical Safety Precautions

Caution: During installation or maintenance procedures, wear a grounding wrist strap to avoid ESD damage to the electronics of the appliance. Use a conductive wrist

strap attached to a good earth ground or to the appliance. You can attach it to the connector beside the ESD symbol on the back.

Basic electrical safety precautions should be followed to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch, so that you can quickly remove power to the appliance if an electrical accident occurs.
- Use a regulated, uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. First shut down the appliance, and then unplug the power cords of all the power supply units. As long as the power cord is plugged in, line voltages can be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Make sure that the power supply cords include grounding plugs and are plugged into grounded electrical outlets.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload.
- A reliable ground must be maintained at all times. Therefore, the rack should be grounded. Pay particular attention to power supply connections other than the direct connection to the branch circuit (for example, connections to power strips).

Setting Up Connectivity

After you have installed your appliance in a rack, you are ready to perform the initial configuration. To perform the initial configuration, you can use the Management Service user interface or the serial console. You can access the Management Service user interface from any computer that is on the same network as the new SDX appliance. If you do not have a computer on the same network, use the serial console to perform the initial configuration of the SDX appliance. Citrix recommends that, as soon as you complete the initial configuration, you change the root-user password. For information about changing the root-user password, see Changing the Password of the Default User Account.

Initial Configuration through the Management Service User Interface

To set up the appliance by using the Management Service user interface, connect a workstation or laptop to the same network as the appliance.

To configure the NetScaler SDX appliance by using the Management Service user interface

1. Connect the NetScaler SDX appliance to a management workstation or network by using interface 0/1.
2. Open a browser and type: `http://192.168.100.1`

   Note: The SDX Management Service is preconfigured with the IP address 192.168.100.1 and the XenServer hypervisor is preconfigured with the IP address 192.168.100.2.
3. In the **User Name** box, type `nsroot`.
4. In the **Password** box, type `nsroot`.
5. In the navigation pane, click **System**.
6. In the details pane, under **System Administration**, click **Network Configuration** and enter values for the following parameters:
   - Interface*—The management interface that connects the appliance to a management workstation or network. Possible values: 0/1, 0/2. Default: 0/1.
   - XenServer IP Address*—The IP address of the XenServer.
   - Management VM IP Address*—The IP address that is used to access the Management Service by using a Web browser.

     Note: The XenServer IP address and Management Service IP address should be in the same subnet.
   - Netmask*—The mask used to define the subnet in which the SDX appliance is located.
   - Gateway*—The IP address of the router that forwards traffic out of the appliance's subnet.
   - DNS Server—The IP address of the DNS server.

   *A required parameter
7. Click **OK**, and then click **Close.**
8. To confirm that the NetScaler SDX appliance is configured correctly, you can either ping the new Management Service IP address or use the new IP address to open the user interface in a browser.

   Note: After changing the network configuration, close all browser instances and open a new browser instance to access the appliance.

Initial Configuration through the Serial Console

To perform initial configuration of the SDX appliance from outside the L2 domain, connect to the console port of the appliance and follow the instructions carefully.

Note: `networkconfig` utility is available from build 72.5 and later.

To configure the NetScaler SDX appliance by using the serial console

1. Connect the console cable into your appliance.
2. Connect the other end of the cable to your computer and run the vt100 terminal emulation program of your choice.
   - For Microsoft Windows, you can use HyperTerminal, which is installed with all current versions of Windows.
   - For Apple Macintosh OSX, you can use the GUI-based Terminal program or the shell-based telnet client.

     Note: OSX is based on the FreeBSD UNIX platform. Most standard UNIX shell programs are available from the OSX command line.
   - For UNIX-based workstations, you can use the shell-based telnet client or any supported terminal emulation program.
3. Press ENTER.
   The terminal screen displays the Logon prompt.

   Note: You might have to press ENTER two or three times, depending on which terminal program you are using.
4. Log on to the appliance with the administrator credentials. The default credentials for username and password are root and nsroot respectively.
5. At the prompt, type:
   `ssh nsroot@169.254.0.10`
   When prompted for the password, type `nsroot`.
6. At the shell prompt, type:
   `networkconfig`

You can now use the new IP address to log on to the Management Service user interface.

Changing the Password of the Default User Account

The default user account provides complete access to all features of the Citrix NetScaler SDX appliance. Therefore, to preserve security, the nsroot account should be used only when necessary, and only individuals whose duties require full access should know the password for the nsroot account. Citrix recommends changing the nsroot

password frequently. If you lose the password, you can reset the password to the default by reverting the appliance settings to factory defaults , and you can then change the password.

You can change the password of the default user account in the **Users** pane. In the **Users** pane, you can view the following details:

Name
Lists the user accounts configured on the SDX appliance.

Permission
Displays the permission level assigned to the user account.

To change the password of the default user account

1. On the **Configuration** tab, in the navigation pane, expand **System**, and then click **Users**.
2. In the **Users** pane, click the default user account, and then click **Modify**.
3. In the **Modify System User** dialog box, in **Password** and **Confirm Password**, enter the password of your choice.
4. Click **OK**.

System Specifications

The following table summarizes the specifications of the NetScaler SDX 17500/19500/21500 appliances.

Specifications	SDX 17500/19500/21500
Processors	2, each with 6 cores (24 with hyper-threading)
Memory	48 GB
Number of power supplies	2
AC power supply input voltage, frequency, and current	100-240 VAC 50-60 Hz 6.5-3.5 A
Maximum power consumption	650 W
Heat dissipation	2200 BTU per hour

Specifications	SDX 17500/19500/21500
Weight	40 lbs
Height	2U
Width	EIA 310-D for 19-inch racks
Depth	24.75 in or 62.865 cm
Operating temperature (degree Celsius)	0-40
Humidity range (non-condensing)	5%-95%
Safety certifications	TUV
EMC & susceptibility	FCC (Part 15 Class A), CE, C-Tick, VCCI-A
Environmental compliance	RoHS, WEEE

Additional Information

A complete set of documentation is available on the **Documentation** tab of your SDX appliance and from http://support.citrix.com/. (Most of the documents require Adobe Reader, available at http://adobe.com/.)

To view the documentation

1. From a web browser, log on to the NetScaler SDX appliance.
2. Click the **Documentation** tab.
3. To view a short description of each document, hover your cursor over the title. To open a document, click the title.

To contact Citrix Support, call 1-800-4-CITRIX (1-800-424-8749), or log on to MyCitrix at http://www.citrix.com. You will be asked for your hardware serial number as part of the support process.

Detailed instructions for contacting support can be found at: http://citrix.com/site/resources/dynamic/sup2nd/Citrix_HWS_SerialNO.pdf.

If you have comments or feedback on this documentation, please send email to nsdocs_feedback@citrix.com.