Release Notes

2015-05-18 10:53:30 UTC

Contents

Release Notes

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

- Main Release
- Maintenance Release
- Enhancement Release

Main Release

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

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

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

Main Release

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

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

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

Enhancements

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

AAA-TM

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

127-Character User Name and Password Support

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

127-Character Support for RADIUS NAS ID

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

SAML 2.0 Consumer Support

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

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

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

Enhanced NTLMv2 Support

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

LDAP Referral Support

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

Three caveats apply:

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

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

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

Support for Password Changes on Novell NDS

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

Support for Password Changes on Microsoft RADIUS via MSCHAP

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

Logging out AAA-TM Sessions

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

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

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

AGEE

The following AGEE enhancements are available in this release.

Apply the Citrix Receiver theme to the logon page

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

Enabling Access Interface Bookmarks

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

AppExpert

The following AppExpert feature enhancements are available in this release.

Load Balancing Virtual Server Template Enhancements

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

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

Deployment Files

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

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

Variables for Non-String Parameters

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

SQL OK and SQL Error Response Types Options Added to GUI

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

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

For more information, see Configuring a Responder Action.

Responder HTML Page Imports

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

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

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

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

show responder htmlpage f<*name*>]

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

Responder Action for Timeouts

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

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

set ns httpProfile -reqTimeoutAction <responder action name>

Binding URL Transformation Policies

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

For more information, see Globally Binding URL Transformation Policies.

Expressions for Identifying the Protocol in an Incoming IP Packet

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

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

Arguments to the PROTOCOL() function

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

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

Use Case Scenarios

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

Following are some use cases for the expressions:

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

HTML5 Parsing and Expression Support

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

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

Packet Expression Support

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

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

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

SIP Expression Support

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

For more information, see SIP Expressions.

String Comparison Functions

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

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

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

APPEND() String Function

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

NE() Function for Time Values

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

Command-Line Interface Support for Importing and Exporting AppExpert Applications

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

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

To import an AppExpert application by using the NetScaler command line

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

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

To export an AppExpert application by using the NetScaler command line

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

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

Application Firewall

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

Variable Support for Application Firewall Configuration

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

For more information, see Configuration Variable Support.

Support for CEF Format Logs

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

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

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

Source Port and HTTP Method Added to Logs

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

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

Importing and Exporting Application Firewall Profiles

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

Resetting Learning Thresholds

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

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

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

Binding Application Firewall Policies

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

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

Response-Side Signatures Check

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

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

For more information, see Signatures.

Sessionless URL Closure

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

For more information, see Start URL Check.

CSRF Learning

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

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

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

The Web Interface AppExpert Template

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

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

Qualys Support

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

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

Application Firewall Support for Chunked POST Requests

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

Cache Redirection

The following Cache Redirection enhancement is available in this release.

Support for Fully Transparent Cache Redirection

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

Cloud Bridge

The following Cloud Bridge enhancements are available in this release.

Cloud Bridge Set Up for SoftLayer Enterprise Cloud

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

For more information, see CloudBridge.

IKEv2 Liveliness Check for IPSEC Tunnels

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

Statistical Counters for IPSEC Tunnels

The following statistical counters have been introduced for IPSEC tunnels:

Bytes Received.

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

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

Bytes Sent.

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

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

Packets Received.

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

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

Packets Sent.

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

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

Clustering of NetScaler Appliances

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

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

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

For more information, see Clustering.

Compression

The following compression enhancement is available in this release.

Renaming and Getting Compression Statistics

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

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

Configuration Utility

The following configuration utility enhancements are available in this release.

HTML Dashboard

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

Windows Gadget to Monitor NetScaler

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

Pagination Support in Dashboard

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

SCOM Management Pack

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

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

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

Content Switching

The following content switching enhancements are available in this release.

Priority Based Sorting of Bound Policies

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

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

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

Identifying Connections with the 4-tuple and Layer 2 Parameters

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

Enhanced Set of Counters for Virtual Servers

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

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

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

DataStream Enhancements

The following DataStream enhancements are available in this release.

Configuring Token Method of Load Balancing

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

Responder Policy Support

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

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

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

Audit Log Message Support

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

Configuring Content Switching Based on RPC for MS SQL Databases

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

MSSQL.REQ.RPC.NAME.

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

MSSQL.REQ.RPC.IS_PROCID.

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

MSSQL.REQ.RPC.PROCID.

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

AppFlow Support

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

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

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

Microsoft SQL Server Version Setting

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

SNMP Support for DataStream Rate Limiting

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

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

- DataStreamRateLimitHit

Domain Name System

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

Text (TXT) Record Support

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

Rewriting NXDOMAIN Responses

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

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

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

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

- Bind the policy to the global request bind point.

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

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

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

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

EdgeSight Monitoring

The following EdgeSight monitoring enhancement is available in this release.

Exporting EdgeSight Information to AppFlow Collector

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

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

Global Server Load Balancing

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

Overriding Static Proximity Behavior by Configuring Preferred Locations

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

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

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

Confirmation Prompt before Synchronization of Global Server Load Balancing Sites

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

Option to Save the Configuration on All Nodes after Synchronization

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

Integrated Caching

The following Integrated Caching enhancements are available in this release.

Seek Streaming of Large Content

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

Multi-part Byte Range Requests Handling from Cache

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

Viewing Cache Objects

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

Enabling Persistence based on ETag Header

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

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

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

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

Caching of SQL Protocols

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

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

Load Balancing

The following load balancing enhancements are available in this release.

Firewall Load Balancing

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

set lb parameter -vServerSpecificMac ENABLED

This parameter is DISABLED by default.

Connection Mirroring Support for Layer 2 Connection Parameters

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

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

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

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

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

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

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

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

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

Using a String as the Server ID for a Service

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

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

Example

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

For more information, see Custom Server ID Persistence.

Rule Based Persistence for a Virtual Server Group of Type ANY

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

Virtual Server-Level Slow Start

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

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

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

- Custom load

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

Automatic Domain Based Service Group Scaling

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Wizard for Setting Up Branch Repeater Load Balancing

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

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

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

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

NetScaler Online Help

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

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

NetScaler SDX Appliance

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

Assign Multiple Cores to an Instance

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

Configuring Clock Synchronization

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

For more information, see Configuring Clock Synchronization.

New Wizards for Provisioning and Modifying a NetScaler Instance

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

Installing an SSL Certificate on the SDX Appliance

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

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

Upgrading the XenServer Software

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

Polling for SSL Certificates on the NetScaler Instances

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

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

Allowing L2 Mode on a NetScaler Instance

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

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

Configuring VMACs on an Interface

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

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

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

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

Backing Up and Restoring the Configuration Data of the SDX Appliance

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

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

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

Performing a Factory Reset

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

For more information, see Performing a Factory Reset.

Generating a Certificate Signing Request

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

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

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

Monitoring CPU Core Usage on the NetScaler SDX Appliance

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

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

Initial Configuration through the Serial Console

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

Networking

The following Networking enhancements are available in this release.

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

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

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

IS-IS Dynamic Routing Protocol

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

For more information, see Configuring ISIS.

IPv6 Support for Link Load Balancing

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

For more information, see Configuring an LLB Route.

Specifying IP Addresses for Backend Communication

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

Forwarding all Fragments of an ICMP Packet

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

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

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

IPv6 Extension Header Traversing

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

For more information on ACLs, see Access Control Lists.

ARP Response Suppression for Virtual IP Addresses (VIPs)

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

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

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

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

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

SNIP Address Binding to Interfaces

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

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

Route Monitors in High Availability in Non-INC

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

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

For more information, see Configuring Route Monitors.

Command Propagation changes in High Availability

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

VLAN as Gateway in the IPv6 Routes

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

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

Policy Based Routes for IPv6 Traffic

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

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

Source IP selection based on a PBR

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

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

Load Balancing in DSR Mode for IPv6 Networks

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

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

directly to the client, bypassing the NetScaler.

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

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

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

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

Terminating Established Connections that Match Simple ACLs

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

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

Flush can be useful in the following cases:

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

For more information, see Terminating Established Connections.

Enable or Disable Established Parameter

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

Renaming Extended ACLs and ACL6s

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

Reverse Network Address Translation for IPv6 Traffic

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

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

IPv6 Prefix.

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

ACL6.

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

For more information, see Configuring RNAT for IPv6 Traffic.

Support for IPv4 Addresses with /31 Subnet Mask

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

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

NITRO API

The following NITRO API enhancements are available in this release.

Cluster APIs

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

Display Warnings in Execution of APIs

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

Display Paginated Statistics

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

Exception Handling in Bulk Operations

You can specify how exceptions are handled in bulk operations:

Exit.

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

Rollback.

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

Continue.

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

REST API Enhancements

The REST API has been enhanced for the following:

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

Support for SDX Bulk Operations

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

Policy

The following Policy enhancement is available in this release.

Non-Blocking HTTP Callout

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

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

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

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

Example:

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

Secure Sockets Layer (SSL)

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

Default Syntax Policies Support for SSL

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

Control policy.

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

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

Data policy.

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

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

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

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

For more information, see Configuring SSL Actions and Policies.

Denying Nonsecure SSL Renegotiation

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

New SNMP Alarms in SSL

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

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

SNMP

The following SNMP enhancements are available in this release.

IPv6 Based SNMP Managers

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

IPv6 address of the SNMP manager.

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

IPv6 network prefix.

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

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

For more information, see Specifying an SNMP Manager.

Logging SNMP Traps

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

For more information, see Enabling Unconditional SNMP Trap Logging.

SNMP Alarm for HA License Mismatch

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

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

- `haLicenseCheck`

New SNMP Alarms for SSL

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

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

SNMP OID for Model number

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

Stream Analytics

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

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

For more information, see Stream Analytics.

Surge Protection

The following Surge Protection enhancements are available in this release.

Flushing a Surge Queue without Having to Disable a Service

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

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

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

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

For more information, see Flushing the Surge Queue.

Virtual Server - Options of Response to PING

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

Table 2. On an IP address:

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

Table 3. On a virtual server:

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

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

CLI commands:

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

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

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

System

The following System enhancements are available in this release.

TCP Westwood

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

For more information, see Configuring TCP Profiles.

Call Home

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

For more information, see Configuring Call Home.

Idle CLI Session Timeout for a System User

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

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

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

For more information, see Configuring Users and Groups.

WebSocket Connection Support

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

For more information, see Configuring WebSocket Connections.

Web Interface

The following Web Interface enhancements are available in this release.

Customized Login Page Title for a Web Interface Site

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

For more information, see Configuring the Web Interface.

Option for Activating Web Interface in Receiver Platforms

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

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

For more information, see Configuring the Web Interface.

Web Interface Tech Support

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

Using the WebInterface.conf Dialog Box

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

You can do the following from this dialog box:

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

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

Using the config.xml Dialog Box

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

You can do the following from this dialog box:

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

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

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

New Access Modes for Configuring Web Interface

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

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

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

For more information, see Configuring the Web Interface.

Idle Session Timeout for a Web Interface Client

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

For more information, see Configuring the Web Interface.

Web Logging

The following Web Logging enhancements are available in this release.

Web Logging for an HTTP Profile

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

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

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

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

Logging Set-Cookie Headers

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

Changes

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

AppExpert

The following AppExpert feature changes are available in this release.

Entity Templates Feature Deprecated

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

Limit Selector Commands are Deprecated

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

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

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

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

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

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

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

Compression

The following compression feature change is available in this release.

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

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

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

Global Server Load Balancing

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

Backup Session Timeout Parameter is Deprecated

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

Load Balancing

The following load balancing changes are available in this release.

Work Load Manager Feature is Deprecated

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

Generic vserver Commands Deprecated

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

Policies

The following policies change is available in this release.

Order of Evaluation of Operators and Operator Associativity

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

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

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

System

The following system change is available in this release.

Changes to the set ns config command

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

Bug Fixes

The following issues have been fixed in this release.

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

AGEE Issues

Issue ID 0306678

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

System Issues

Issue ID 0290271 (nCore)

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

Known Issues and Workarounds

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

AAA Issues

Issue IDs 0303465 and 0303507

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

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

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

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

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

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

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

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

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

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

AGEE Issues

Issue ID 0251110

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

Issue ID 0251596

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

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

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

3. Configure following REG_SZ values under the Inventory key:

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

   - VPNPrompt1. Provide the value as "UserName".

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

Issue ID 0261547

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

Issue ID 0285995

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

Issue ID 0288469

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

Issue ID 0290976

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

Issue ID 0291264

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

Issue ID 0291821

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

Issue ID 0291822

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

Issue ID 0292005

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

Issue ID 0298971

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

Issue ID 0299515

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

Issue ID 0300511

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

Issue ID 0301060

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

Issue ID 0301338

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

Application Firewall Issues

Issue ID 0291389

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

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

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

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

Issue ID 0300465

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

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

Issue ID 0300827

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

Issue ID 0283780

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

Issue ID 0284009

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

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

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

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

Issue IDs 0302368 and 0302294

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

Issue ID 0303049

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

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

Issue IDs 0303057 and 0301813

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

Issue ID 0303044

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

Cluster Issues

Issue ID 0269773

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

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

Issue ID 0276162

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

Issue ID 0290504

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

Issue ID 0302924 (nCore)

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

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

Command-Line Interface Issues

Issue ID 0262838

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

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

Issue ID 0299716

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

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

Configuration Utility Issues

Issue ID 0251463

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

Issue ID 0278097

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

Issue ID 0298686 (nCore)

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

Issue ID 0300506

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

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

Issue ID 0302742

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

Issue ID 0303279

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

Issue ID 0438216

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

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

Documentation Issues

Issue ID 0277923

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

Domain Name System Issues

Issue ID 0291053

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

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

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

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

Issue ID 0301348

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

Global Server Load Balancing Issues

Issue IDs 0287825 and 0287827

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

Integrated Caching Issues

Issue ID 0278377 (nCore)

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

Issue ID 0288716

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

Load Balancing Issues

Issue ID 89129/0248646

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

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

Issue ID 90395/0249705

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

Issue ID 90875/0250110

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

Issue ID 91711/0250846

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

Issue ID 0285672

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

Issue ID 0289339

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

Issue ID 0351632

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

NetScaler SDX Appliance Issues

Issue ID 0261232

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

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

NetScaler VPX Virtual Appliance Issues

Issue ID 0302377

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

Networking Issues

Issue ID 0276933

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

System Issues

Issue ID 0290271 (nCore)

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

Web Interface Issues

Issue ID 86463/0246466

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

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

Issue ID 86538/0246528

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

- Windows Client
- Linux Client
- Macintosh Client

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

Maintenance Release

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

Build 78.6

Release version: Citrix NetScaler, version 10 build 78.6

Replaces build: None

Release date: October 2013

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Changes and Fixes
- Known Issues and Workarounds

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

Changes and Fixes

Application Firewall

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

Application Firewall Signatures

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

Command Line Interface

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

Configuration Utility

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

Content Switching

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

Global Server Load Balancing

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

High Availability

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

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

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

Load Balancing

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

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

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

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

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

Load Balancing/MSSQL

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

Monitoring

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

NetScaler SDX Appliance

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

Networking

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

Policies

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

Platform

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

Rewrite

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

SSL

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

  User requested abort.

System

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

SQL DB

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

Known Issues and Workarounds

AAA Application Traffic

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

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

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

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

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

Action Analytics/Rate Limiting

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

AppFlow

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

Application Firewall

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

Cache Redirection

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

Cluster

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

Command Line Interface

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

Configuration Utility

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Documentation

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

Domain Name System

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

Global Server Load Balancing

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

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

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

Load Balancing

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

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

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

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

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

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

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

Load Balancing/SSL

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

NetScaler SDX Appliance

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

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

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

NetScaler VPX Appliance

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

  sysctl netscaler.ns_vpx_halt_method=2

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

  sysctl netscaler.ns_vpx_halt_method=2

Networking

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

  Workaround:

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

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

Rewrite

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

SSL

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

System

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

XML API

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

Build 77.5

Release version: Citrix NetScaler, version 10 build 77.5

Replaces build: None

Release date: August 2013

Release notes version: 2.0

Language supported: English (US)

Review the following sections:

- Changes and Fixes
- Known Issues and Workarounds

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

Changes and Fixes

AppFlow

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

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

Application Firewall

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

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

  bind appfw profile <name> -inspectResContentType <type>

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

  bind appfw profile library -inspectResContentType "text/PDF"

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

  unbind appfw profile <name> -inspectResContentType <type>

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

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

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

Configuration Utility

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

Content Switching

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

Global Server Load Balancing

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

Load Balancing

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

Load Balancing/AAA-TM

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

Load Balancing/DNS

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

NetScaler SDX Appliance

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

Networking

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

Policy

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

Platform

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

SSL

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

System

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

Web Interface

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

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

XML API

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

Known Issues and Workarounds

AAA Application Traffic

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

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

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

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

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

Action Analytics/Rate Limiting

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

AppExpert

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

AppFlow

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

Application Firewall

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

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

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

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

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

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

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

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

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

Cache Redirection

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

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

Cluster

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

  Workaround: Enable MAC spoofing on the HyperV backplane interfaces.

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

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

Configuration Utility

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

  Workaround: Install Java 7, update 21.

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

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

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

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

Documentation

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

Domain Name System

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

Global Server Load Balancing

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

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

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

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

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

  - Source IP persistence is enabled,

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

High Availability

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

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

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

Load Balancing

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

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

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

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

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

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

Load Balancing/SSL

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

NetScaler SDX Appliance

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

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

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

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

  Workaround: Upgrade to XenServer 6.0

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

NetScaler VPX Appliance

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

  sysctl netscaler.ns_vpx_halt_method=2

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

  sysctl netscaler.ns_vpx_halt_method=2

Networking

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

  Workaround:

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

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

Rewrite

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

SSL

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

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

XML API

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

Build 76.7

Release version: Citrix NetScaler, version 10 build 76.7

Replaces build: None

Release date: May 2013

Release notes version: 3.0

Language supported: English (US)

Review the following sections:

- Changes and Fixes
- Known Issues and Workarounds

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

Changes and Fixes

Application Firewall

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

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

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

Configuration Utility

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

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

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

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

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

DataStream

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

Domain Name System

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

Global Server Load Balancing

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

Load Balancing

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

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

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

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

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

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

Monitoring

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

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

NetScaler SDX Appliance

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

NetScaler VPX Appliance

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

Networking

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

Platform

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

Policies

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

Rewrite

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

SSL

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

System

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

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

XML API

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

Known Issues and Workarounds

AAA Application Traffic

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

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

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

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

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

Action Analytics/Rate Limiting

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

AppExpert

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

AppFlow

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

Application Firewall

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

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

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

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

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

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

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

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

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

Cache Redirection

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

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

Cluster

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

  Workaround: Enable MAC spoofing on the HyperV backplane interfaces.

Command Line Interface

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

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

Configuration Utility

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

  Workaround: Install Java 7, update 21.

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

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

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

Documentation

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

Domain Name System

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

Global Server Load Balancing

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

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

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

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

High Availability

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

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

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

Load Balancing

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

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

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

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

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

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

Load Balancing/SSL

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

NetScaler SDX Appliance

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

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

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

  Workaround: Upgrade to XenServer 6.0

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

NetScaler VPX Appliance

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

  sysctl netscaler.ns_vpx_halt_method=2

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

  sysctl netscaler.ns_vpx_halt_method=2

Networking

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

  Workaround:

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

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

Rewrite

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

SSL

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

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

XML API

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

Build 75.7

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

Replaces build: None

Release date: April 2013

Release notes version: 2.0

Language supported: English (US)

Review the following sections:

- Changes and Fixes
- Known Issues and Workarounds

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

Changes and Fixes

AAA Application Traffic

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

AppFlow

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

Application Firewall

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

Configuration Utility

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

DataStream

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

Domain Name System

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

Global Server Load Balancing

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

Load Balancing

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

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

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

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

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

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

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

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

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

Monitoring

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

NetScaler SDX Appliance

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

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

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

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

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

Networking

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

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

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

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

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

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

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

Policy

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

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

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

SSL

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

System

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

Web Interface

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

Known Issues and Workarounds

AAA Application Traffic

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

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

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

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

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

Action Analytics/Rate Limiting

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

AppExpert

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

AppFlow

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

Application Firewall

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

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

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

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

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

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

- Issue ID 0313950: On a NetScaler appliance that has the application firewall configured and the Safe Object check configured, processing extremely large web pages can cause the NetScaler appliance to crash.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

Cluster

- Issue ID 0324865 (nCore VPX): In a cluster of VPX appliances that are deployed on HyperV, steered packets are getting dropped.

  Workaround: Enable MAC spoofing on the HyperV backplane interfaces.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click 'Application Firewall' in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0303279: In the configuration utility, in the Rewrite Policies pane, clicking Add does not display the Create Rewrite Policy dialog box but disables the main configuration utility window.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0333048: If you access the configuration utility through Internet Explorer 8, an attempt to bind 250 or more VIP addresses to a VLAN results in an error message about an unresponsive script.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

  Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the Create DNS View dialog box, the "Service(s) in this view"

and "Policy(s) in this view" lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs.

  Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0338513: When you log on to NetScaler configuration utility using Internet Explorer 8 or Internet Explorer 9, the web browser displays a blank screen as the browser is displaying the compatibility view.

  Workaround: Change to the standard view, in Tools > Compatibility View Settings dialog box, by clearing the Display all websites in Compatibility View check box.

- Issue ID 0352307: If you access the NetScaler configuration utility from a Mac machine with a client environment running JRE 1.7 or later, you cannot select the fields in the Java based configuration views.

  Workaround: Install Java 7, update 21.

- Issue ID 0353015: Load balancing virtual servers that are used by AppExpert applications are displayed in nodes other than the AppExpert node. For example, they are displayed in the Available Virtual Servers list (Load Balancing > Persistency Groups > Add > Create Persistency Group dialog box), and in the Target LB Virtual Server list (Content Switching > Actions > Add > Create Content Switching Action dialog box > Name option button).

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated. This behavior is expected.

Domain Name System

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If a GSLB virtual server's primary GSLB method is set to round trip time (RTT) and backup GSLB method is set to static proximity, or if the primary GSLB method is set to static proximity and backup GSLB method is set to RTT, and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

Load Balancing

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the "show lb persistentSessions" CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 91711/0250846: If the string (or "token") that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR("string2").AFTER_STR("string1") if the string that is enclosed by "string1" and "string2" is not larger than 64 KB.

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

- Issue ID 0261175: In a high availability or cluster setup, communication between a NetScaler appliance and a peer node fails if the IP address of the peer node matches the IP pattern configured for a virtual server on the appliance. Communication failure can also occur between the appliance and any IP address that is owned by a peer node, if that IP address matches the IP pattern configured for the virtual server.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

Load Balancing/SSL

- Issue ID 0331621: While creating SSL or load balancing virtual servers with default responder action, the NetScaler appliance throws a “No such resource” error. This issue is observed only in a cluster setup.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type: `#/etc/rc.d/svmd restart`

- Issue ID 0309711: If you create an nCore VPX instance on XenServer 5.6, the instance might not start.

  Workaround: Upgrade to XenServer 6.0

- Issue ID 0337386: When restored from a backup, a NetScaler instance is reprovisioned by using the NetScaler XVA image currently available on the appliance, even if the backup was taken from an upgraded configuration. If multiple XVA images are available, the XVA image that was used to originally provision the instance is used, if available, to reprovision the instance. If that image is not available, any XVA image is used.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.
- Issue IDs 0283035 and 0299716: In a cluster setup, the bind vlan command throws an error when interface and IP address are specified together.
- Issue ID 0288450: The show lacp command does not display the lacp configurations. This issue is observed only in a cluster setup.
- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command set ptp -state disable and configure NTP to synchronize the time across the cluster nodes.
  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator, and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed.

  Workaround: Copy the certkey under /nsconfig/ssl/ folder on all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.
- Issue ID 0343395: On the NetScaler appliance, TLS protocol version 1.2 does not support a client certificate with RSA 4096-bit key.
- Issue ID 0345883: On the NetScaler appliance, TLS protocol version 1.2 does not support ephemeral Diffie-Hellman cipher suites.

XML API

- Issue ID 0321005: The API to set the hostname for a NetScaler appliance is changed to include the owner node parameter for a cluster node. This will cause incompatibility of the API.

Build 74.4

Release version: Citrix® NetScaler®, version 10 build 74.4

Replaces build: None

Release date: February 2013

Release notes version: 3.0

Language supported: English (US)

Review the following sections:

- Changes and Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler.

Changes and Fixes

AAA Application Traffic

- Issue ID 0349418: The NetScaler appliance now supports the exclusive normalization method with SAML. For that reason, assertions posted by any SAML 2.0 compliant IDP (such as the Pingone IDP server or Oracle ID server) are now handled correctly.

AppExpert

- Issue ID 0243716: You can now configure a persistency group for the application units in an AppExpert application. In the context of an AppExpert application, a persistency group is a group of application units that you can treat as a single entity for the purpose of applying common persistence settings. When the application is exported to an application template file, the persistency group settings are included, and they are automatically applied to the application units when you import the AppExpert application.

Application Firewall

- Issue ID 0338443: The application firewall cannot use negated (!) literal strings in a fastmatch signature pattern. If you include a negated literal string in a fastmatch-designated pattern in a signatures file, the application firewall displays an error message and does not bind the signatures file to the specified profile.

- Issue ID 0360302: On a NetScaler appliance with the application firewall enabled, the cookies generated by the cookie consistency check to verify the integrity of server cookies do not have the secure flag set, as it should be for HTTPS connections.

- Issue ID 0361617: On a NetScaler appliance that has Edgesite configured, if the application firewall learning feature is enabled, it might crash intermittently. To work around this problem, disable the learning feature or reboot the NetScaler appliance.

Cluster

- Issue ID 0360131: In a cluster setup, some TCP sessions initiated by the Flow Processor are failing as Bridge Access Control Lists are applied on the Flow Receiver.

Configuration Utility

- Issue ID 0334042: The configuration utility does not display a details panel for all the entities.
- Issue ID 0349813: If you use the configuration utility to unbind all the cipher suites from a user-defined SSL cipher group, the user-defined cipher group is deleted from the appliance.
- Issue ID 0361670: If multiple domain based services are bound to a service group, and the domain name of a member cannot be resolved (its IP address is displayed as 0.0.0.0), you cannot unbind that member from the service group.
- Issue ID 0363408: When using the Load Balancing Wizard for Citrix XenDesktop to configure load balancing for Citrix XenDesktop, if you specify a wildcard port (*) for a load balancing virtual server, the wizard inserts an asterisk in the name of the virtual server, in the name of the associated service group, and in the name of the monitor. Because the asterisk is an invalid character for an entity name, you cannot perform any operation (such as rename, set, or remove) on those entities.

DataStream

- Issue ID 0357185: The MYSQL-ECV monitor closes the TCP connection with a FIN without first issuing the quit command to close the MySQL session. As a result, the `aborted_clients` counter for MYSQL servers is incremented.

High Availability

- Issue ID 0287765: In a high availability setup, SNMP traps netScalerConfigChange and netScalerConfigSave are getting generated on the secondary appliance. High Cpu usage in stats sync on 7 seconds boundary were causing latency in some transactions.

Integrated Caching

- Issue ID 0322506 (nCore): When users upgrade from 9.1 to 9.3, the number of objects being cached is reduced because of architectural changes.

Load Balancing

- Issue ID 0348302: Stateful connection failover is now supported on Layer 3 Direct Server Return (DSR) configuration that uses IP tunneling.

  Connection failover helps prevent disruption of access to applications deployed in a distributed environment. In a NetScaler High Availability (HA) setup, connection failover (or connection mirroring-CM) refers to keeping active an established TCP or UDP connection when a failover occurs.

  In stateful failover, to maintain current information about the mirrored connections, the primary appliance sends messages to the secondary appliance. The secondary appliance maintains the data related to the packets but uses it only in the event of a failover. If a failover occurs, the new primary (old secondary) appliance starts using the stored data about the mirrored connections and accepting traffic.

Monitoring

- Issue ID 0354059: The `Last response` field in the output of the show service command should indicate that a probe timed out if the following sequence of events occurs:

  1. The monitor bound to the service fails due to an internal error (for example, an unavailable ARP table entry).

  2. The error condition is corrected.

  3. Probes are successfully sent to the service, but they time out.

  Instead of text indicating that the most recent probe timed out, the content of the Last response field is `Internal error: resource unavailable to send probe`.

Networking

- Issue ID 0283793: If the NetScaler appliance receives an ICMPv6 `Packet Too Big` error for a UDP packet, it does not fragment the remaining packets to be sent to the client.

- Issue ID 0288356: With MAC-Based Forwarding (MBF) enabled, new connections to a server fail through a Virtual IP (VIP) address, if the server is configured to reach over the newly added Subnet IP (SNIP) addresses that are bound to a Layer 3 (L3) VLAN.

- Issue ID 0347842: When the NetScaler appliance reestablishes OSPF adjacency with a peer router, latency might delay the Link State (LS) updates sent by the appliance. The delay might cause the peer router to install invalid Link State Advertisements (LSAs) for a short period of time. As a result, traffic arriving during this period encounters a black-hole.

Platform

- Issue ID 0333400 The Citrix NetScaler SDX 8400/8600 platform supports NetScaler release 10 build 74.x and later.
- Issue ID 0344262: 1G copper SFP transceivers are now supported on the ixgbe (ix) interfaces. These transceivers are hot-swappable on this interface. However, fiber SFP transceivers are not supported.

  The following SFP+ and SFP transceivers, and direct access cables, are supported:

  - Intel fiber SFP+: "FTLX8571D3BCV-IT"
  - Intel fiber SFP+: "FTLX8571D3BCV-I3"
  - Finisar fiber SFP+: "FTLX8571D3BCV"
  - Intel fiber SFP+ (LR): "FTLX1471D3BCV-IT"
  - Finisar fiber SFP+ (LR): "FTLX1471D3BCV "
  - Finisar copper SFP: "FCLF-8521-3"
  - Avago copper SFP: "ABCU-5710RZ"
  - Methode DAC cable: "DM-255-100 "
  - Methode DAC cable: "DM-255-300 "
  - Methode DAC cable: "DM-255-500 "

  Note:

  - Only 10G ports support DAC cables.
  - Fiber SFPs are not supported.
- Issue ID 0357030: NetScaler release 10 build 74.x is supported on the SDX 11500/13500/14500/16500/18500/20500 NEBS platform.

Policies

- Issue ID 0334472: In some deployments you cannot remove string patterns from string maps.
- Issue ID 0342589: Existing compression policies cannot be disabled without changing the priority value.

SSL

- Issue ID 0352611: If you log on to a NetScaler account other than the administrative account and enter the show ssl service command or show running config command, the command output appears repeatedly.

System

- Issue ID 0288067: By default, the Precision Time Protocol daemon (PTPd) is disabled on a NetScaler appliance. However, if you add the node to a cluster, PTPd is automatically enabled on that node.
- Issue ID 0350189: Latency in some transactions because of high CPU usage on the 7 seconds boundary while synchronizing statistics.
- Issue ID 0353546: When you try to add a second name-based SNMP manager, you get an error message that says an SNMP manger with that name already exists.
- Issue ID 0356420: A large number of routine system health check messages are continually added to the system log.
- Issue ID 0356430: SNMP traps are not being sent.
- Issue ID 0358197: SNMP cannot complete in the 5 minutes window between polling period because it sends the request to aggregator and waits for response.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0283556: Currently the SAML implementation supports only RSA digital signatures. DSA digital signatures are not supported.
- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberoes authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, and then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.
- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

Action Analytics/Rate Limiting

- Issue ID 91353/0250526: If multiple stream identifiers and/or rate limiting identifiers evaluate a connection, the NetScaler appliance updates the counters for bandwidth, response time, and number of concurrent connections for only the identifier that evaluates the connection first. Those statistical counters are not updated for the other identifiers. However, the counter for number of requests is updated for all the identifiers that evaluate the connection.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

AppFlow

- Issue ID 0327439: AppFlow records generated by the NetScaler appliances cannot be seen on SPLUNK.
- Issue ID 0333560 (nCore): AppFlow records generated by the NetScaler appliance might contain junk characters.

Application Firewall

- Issue ID 0272715: If you use the Google Chrome browser with the default Chrome PDF plugin to view the PCI-DSS report, certain links and pages do not render correctly.

  Workaround: Disable Chrome PDF and install the Adobe Acrobat Reader plugin for Chrome.

- Issue ID 0282932: If you use the Signature Editor to add a signature rule for a response-side check (such as the Credit Card or Safe Object check), in addition to one or more response patterns you must also add at least one request pattern. If you do not, then when you try to save the new signature rule, the configuration utility displays an error message and does not save the rule.

- Issue ID 0283780: When you enable the sessionless URL closure feature, you must also enable the URL closure feature. If you do not enable URL closure, the sessionless URL closure feature does not work.

- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked. To work around this issue, if you configure Sessionless URL Closure, set Validate Referer Header to Off.

- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported for importing as application firewall signature rules. WAS 2.0 scan reports are not supported.

- Issue ID 0303060: Application firewall statistics are not supported for NetScaler classic policies. If you need to see numbers of policy hits and other statistics, you must use NetScaler default syntax policies.

- Issue ID 0313950: On a NetScaler appliance that has the application firewall configured and the Safe Object check configured, processing extremely large web pages can cause the NetScaler appliance to crash.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

Cluster

- Issue ID 0324865 (nCore VPX): In a cluster of VPX appliances that are deployed on HyperV, steered packets are getting dropped.

  Workaround: Enable MAC spoofing on the HyperV backplane interfaces.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click 'application firewall' in the navigation pane, the scroll bar moves up and the subnodes of the application firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0303279: In the configuration utility, in the Rewrite Policies pane, clicking Add does not display the Create Rewrite Policy dialog box but disables the main configuration utility window.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0333048: If you access the configuration utility through Internet Explorer 8, an attempt to bind 250 or more VIP addresses to a VLAN results in an error message about an unresponsive script.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

  Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the Create DNS View dialog box, the "Service(s) in this view"

and "Policy(s) in this view" lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs.

  Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0338513: When you log on to NetScaler configuration utility using Internet Explorer 8 or Internet Explorer 9, the web browser displays a blank screen as the browser is displaying the compatibility view.

  Workaround: Change to the standard view, in the Compatibility View Settings dialog box, by clearing the Display all websites in Compatibility View check box.

- Issue ID 0352307: If you access the NetScaler configuration utility from a Mac machine with a client environment running JRE 1.7 or later, you cannot select the fields in the Java based configuration views.

  Workaround: If you click outside and return to the browser window, you will be able to select the fields in the configuration views.

- Issue ID 0353015: Load balancing virtual servers that are used by AppExpert applications are displayed in nodes other than the AppExpert node. For example, they are displayed in the Available Virtual Servers list (Load Balancing > Persistency Groups > Add > Create Persistency Group dialog box), and in the Target LB Virtual Server list (Content Switching > Actions > Add > Create Content Switching Action dialog box > Name option button).

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated.

Domain Name System

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If a GSLB virtual server's primary GSLB method is set to round trip time (RTT) and backup GSLB method is set to static proximity, or if the primary GSLB method is set to static proximity and backup GSLB method is set to RTT, and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

Load Balancing

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the show lb persistentSessions CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 91711/0250846: If the string (or "token") that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR("string2").AFTER_STR("string1") if the string that is enclosed by "string1" and "string2" is not larger than 64 KB.

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

- Issue ID 0261175: In a high availability or cluster setup, communication between a NetScaler appliance and a peer node fails if the IP address of the peer node matches the IP pattern configured for a virtual server on the appliance. Communication failure can also occur between the appliance and any IP address that is owned by a peer node, if that IP address matches the IP pattern configured for the virtual server.

- Issue ID 0317281: The bind serviceGroup command, which can be used to specify either a member of or a monitor for a service group, includes two identically named parameters called state. One parameter specifies the state of a service group member’s binding with the service group, and the other parameter specifies the state of a monitor’s binding with the service group. When you use the command with a state parameter, the command-line interface (CLI) sometimes interprets the parameter as being associated with a member of the service group and at other times as being associated with a monitor bound to the service group. Consequently, if you use the command to specify a member, the CLI might interpret the state parameter as being associated with a monitor, and it might display an error message saying that the name of a monitor is required.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout

values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

Load Balancing/SSL

- Issue ID 0331621: While creating SSL or load balancing virtual servers with default responder action, the NetScaler appliance throws a “No such resource” error. This issue is observed only in a cluster setup.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type: `#/etc/rc.d/svmd restart`

- Issue ID 0337386: When restored from a backup, a NetScaler instance is reprovisioned by using the NetScaler XVA image currently available on the appliance, even if the backup was taken from an upgraded configuration. If multiple XVA images are available, the XVA image that was used to originally provision the instance is used, if available, to reprovision the instance. If that image is not available, any XVA image is used.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.
- Issue IDs 0283035 and 0299716: In a cluster setup, the bind vlan command throws an error when interface and IP address are specified together.
- Issue ID 0288450: The show lacp command does not display the lacp configurations. This issue is observed only in a cluster setup.
- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command set ptp -state disable and configure NTP to synchronize the time across the cluster nodes.
  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator, and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed.

  Workaround: Copy the certkey under /nsconfig/ssl/ folder on all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.
- Issue ID 0343395: On the NetScaler appliance, TLS protocol version 1.2 does not support a client certificate with RSA 4096-bit key.
- Issue ID 0345883: On the NetScaler appliance, TLS protocol version 1.2 does not support ephemeral Diffie-Hellman cipher suites.
- Issue ID 0352334: TLS protocol, version 1.2, handshake fails if all the following conditions are met:
  - The Client browser is Internet Explorer.
  - Client authentication is set to mandatory on the virtual server.
  - The configured client certificate on IE browser is not signed by SHA256 hash algorithm.

XML API

- Issue ID 0321005: The API to set the hostname for a NetScaler appliance is changed to include the owner node parameter for a cluster node.

Build 73.5

Release version: Citrix® NetScaler®, version 10 build 73.5

Replaces build: None

Release date: January 2013

Release notes version: 2.0

Language supported: English (US)

Review the following sections:

- Changes and Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler and Citrix Access Gateway.

Changes and Fixes

Access Gateway

- **Documentation:** Starting with this maintenance release, for Access Gateway issues, see http://support.citrix.com/article/CTX133966.

Application Firewall

- Issue ID 0348647: On a NetScaler appliance that has the application firewall configured, if the client sends a web form with data that contains a plus sign (+), that form field triggers a form field consistency violation. This applies for data that the user types into the form, and for data in hidden fields that was generated by a javascript or sent to the user from the server. To work around this issue, ensure that no field contains a plus sign, or temporarily disable blocking for the form field consistency check.

- Issue ID 0354289: On a NetScaler appliance that has the application firewall configured, chunked requests sent by mobile devices to XML services might receive 400-level HTTP responses. This occurs only for requests that do not contain web forms.

Cluster

- Issue ID 0343137: The configuration utility does not display the Add button while configuring linksets.

Configuration Utility

- Issue ID 0324797: The NetScaler configuration utility does not display the queue depth value for the configured priority queuing policies. This issue is observed only in a cluster setup.
- Issue ID 0334292: If you navigate to HTTP Compression > Policies or HTTP Compression > Actions, the Remove button is disabled in the task pane.
- Issue ID 0346094: The Configured table on the Monitors tab of the Configure Service dialog box does not display the correct states for monitors that are bound to a service. Any check boxes that you selected earlier, in the State column, are shown as unselected the next time you open the Configure Service dialog box for that service. However, the monitors remain active and continue to check the health of the service.
- Issue ID 0345888: If you log off and then log back on to the NetScaler configuration utility, an “Invalid username or password" error is logged in the ns.log file.
- Issue ID 0351805: The Monitor Name column of the Monitor details for service group member dialog box displays the name of the server instead of the name of the monitor.
- Issue ID 0355097: If you use the configuration utility to modify the security settings of profiles for the application firewall feature, the changes are not saved.

DataStream

- Issue ID 0354182: The flush cache contentGroup command does not flush objects that are cached in a content group of type MYSQL.

Global Server Load Balancing

- Issue ID 0344759: If you attempt to create a CNAME based GSLB service with a CNAME that is already associated with another service, the NetScaler appliance not only disallows creation of the new service, but also removes the CNAME record for that CNAME. A subsequent attempt to create a GSLB service with that CNAME is successful, and creates a new CNAME record. Therefore, two GSLB services (the previously existing service and the new one) are associated with the same CNAME.

Integrated Caching

- Issue ID 0337778: If both the rewrite feature and the Integrated caching feature are configured, the integrated caching feature might not function normally, and as a result the NetScaler appliance might fail. The problem can occur if objects are stored in selector based content groups and heavy traffic causes a server to respond slowly.
- Issue ID 0347120: For HTTP callout caching, if a response gets cached in a content group that has the minimum number of hits set to a non-zero value, the show cache object command fails.

Load Balancing/AAA Application Traffic

- Issue ID 0346093: The traffic management policy hit count shows no hits ("0") even when traffic management policies are functioning and matching traffic.

Load Balancing

- Issue ID 0278377 (nCore): Cache policy labels cannot be bound to MYSQL or MSSQL virtual servers.
- Issue ID 0330173: If a domain based service is configured with a wildcard port, its domain name does not get resolved to an IP address. Therefore, the service does not come up.
- Issue ID 0331414: The states and port numbers of load balancing virtual servers and services are not included in log entries in the newnslog file.
- Issue ID 0338196: The NetScaler appliance might fail during active-mode FTP transactions.
- Issue ID 0350458: The servicegroupbindings NITRO request (URL: `http://<NS_IP>/nitro/v1/config/servicegroupbindings/<servicegroupname>`) does not retrieve the names of t group is bound.

NetScaler SDX Appliance

- Issue ID 0318968: If you log on to a NetScaler VPX instance and change the password for access to the instance, instead of changing the password from the Management Service, connectivity from the Management Service to the instance is lost. With this release, you can restore connectivity by creating a new profile from the Management Service, assigning it the same password that you specified on the NetScaler VPX instance, and then binding the new profile to the NetScaler VPX instance.

  To create a new administrator profile, log on to the Management Service and, on the Configuration tab, navigate to NetScaler > Admin Profiles. In the details pane, click Add. In the Create NetScaler Admin Profile dialog box, type the new profile name and password. Then navigate to NetScaler > Instances and select the instance to which you want to bind the new profile. Click Modify to open the Modify NetScaler wizard and, from the Admin Profile list, select the new profile. You do not need to restart the instance for this change to take effect.

  You can also lose connectivity to XenServer by changing the password on XenServer instead of from the Management Service. To restore connectivity, you can now change the password for XenServer from the Management Service.

  To change the password, log on to the Management Service and, on the Configuration tab, navigate to System > Users. Select the nsroot user, and then click Modify. In the Modify System User dialog box, type the same password that you specified when you were logged directly on to XenServer.

- Issue ID 0329597: In certain cases, the status of a storage disk present in the SDX appliance might appear as "Missing" in the Management Service User interface under Monitoring > System Health > Storage > Disk node.

- Issue ID 0336831: If you bind a new interface to a NetScaler instance, the physical to virtual interface mapping does not change. However, if you modify a NetScaler instance that involves disabling a virtual interface, the physical interface to virtual interface mapping on the instance might change.

Networking

- Issue ID 0342151: The set l4 parameter command has a new parameter,l2connMethod, for specifying the MAC address, channel number, and VLAN ID attributes for the L2 Conn option behavior in a virtual server.

  For a load balancing virtual server with L2 Conn enabled and l2connMethod parameter of the set l4 parameter command is set to Channel or Vlan or VlanChannel, a client MAC address change no longer causes the NetScaler appliance to create a new session entry. Instead, the appliance updates the existing session entry with the new MAC address. This update resolves issues (especially with MBF) that were caused by the appliance using the old session entry instead of the new one.

- Issue IDs 0343485 and 0358382: The NetScaler appliance becomes unresponsive when highly demanding traffic (~5000 HTTP threads at a request rate of 100 KB/s) is sent through GRE and IPsec tunnels.

- Issue ID 0343789: In an High Availability configuration, BGP peer of the secondary node stays in open sent state.

- Issue ID 0346654: The NetScaler appliance does not ignore some unsupported capabilities. It might reset BGP connections even when strict-capability-match is not configured on the appliance.

NITRO API

- Issue ID 93372/0257279: You can now view the virtual servers to which a specified service is bound. The REST URL for this is `http//<nsip>/nitro/v1/config/svcbindings/svcname`.

- Issue ID 0318912: On the NetScaler appliance versions 9.2, 9.3, and 10, incorrect values are returned for cpuusagepcnt and rescpuusagepcnt on the following query: /nitro/v1/stat/system.

SSL

- Issue ID 0342706: If you bind a cipher or cipher group to a virtual server, service group, or service, and then save the configuration, the cipher group binding is missing from the configuration after you restart the appliance.

- Issue ID 0344323: An attempt to add a CA certificate fails if the modulus value of the public key is not a multiple of 512 bits.

- Issue IDs 0352611, 0357697, and 0358026: If you log on to a NetScaler account other than the administrative account and enter the show ssl service command or show running config command, the command output appears repeatedly.

- Issue ID 0353680: The add ssl certkey command fails if the private key file does not have a newline at the end of the file.

- Issue ID 0357528: On a FIPS platform, if an SSL renegotiation request is received on an SSL virtual server, the appliance fails.

System

- Issue ID 0301065: When using the HTTP monitor, the NetScaler appliance might send SYN packets from a port on which an earlier session was not closed by the server. The server then responds with a bad syn ack response, which causes the NetScaler appliance to send a RST to the server.
- Issue ID 0334500: High disk usage as the newnslog log files of NetScaler appliance version 9.2 are not automatically cleaned up on upgrade to NetScaler appliance version 9.3.
- Issue ID 0335155: When USIP is enabled, the Netscaler appliance sends a probe to the server using the client IP address as the source IP address. If the server responds to the probe with a packet having incorrect acknowledgement number, the appliance tries to probe the server again using MIP address instead of client IP address.
- Issue IDs 0355812 and 0357937: If you log on to a NetScaler appliance using an account other than the administrative account, when you execute the show monitor command, not all monitors are displayed.

Web Interface

- Issue ID 0353708: If you modify a web interface services site (for access via Citrix receiver) using the configuration utility, on a NetScaler version 10 appliance running a build older than 72.6, the services site might stop working.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0283556: Currently the SAML implementation supports only RSA digital signatures. DSA digital signatures are not supported.
- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberoes authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, and then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.
- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

Action Analytics/Rate Limiting

- Issue ID 91353/0250526: If multiple stream identifiers and/or rate limiting identifiers evaluate a connection, the NetScaler appliance updates the counters for bandwidth, response time, and number of concurrent connections for only the identifier that evaluates the connection first. Those statistical counters are not updated for the other identifiers. However, the counter for number of requests is updated for all the identifiers that evaluate the connection.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

AppFlow

- Issue ID 0327439: AppFlow records generated by the NetScaler appliances cannot be seen on SPLUNK.
- Issue ID 0333560 (nCore): AppFlow records generated by the NetScaler appliance might contain junk characters.

Application Firewall

- Issue ID 0272715: If you use the Google Chrome browser with the default Chrome PDF plugin to view the PCI-DSS report, certain links and pages do not render correctly. To work around this issue, disable Chrome PDF and install the Adobe Acrobat Reader plugin for Chrome.

- Issue ID 0282932: If you use the Signature Editor to add a signature rule for a response-side check (such as the Credit Card or Safe Object check), in addition to one or more response patterns you must also add at least one request pattern. If you do not, then when you try to save the new signature rule, the configuration utility displays an error message and does not save the rule.

- Issue ID 0283780: When you enable the sessionless URL closure feature, you must also enable the URL closure feature. If you do not enable URL closure, the sessionless URL closure feature does not work.

- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked. To work around this issue, if you configure Sessionless URL Closure, set Validate Referer Header to Off.

- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported for importing as application firewall signature rules. WAS 2.0 scan reports are not supported.

- Issue ID 0303060: Application firewall statistics are not supported for NetScaler classic policies. If you need to see numbers of policy hits and other statistics, you must use NetScaler default syntax policies.

- Issue ID 0313950: On a NetScaler appliance that has the application firewall configured and the Safe Object check configured, processing extremely large web pages can cause the NetScaler appliance to crash.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click 'Application Firewall' in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0303279: In the configuration utility, in the Rewrite Policies pane, clicking Add does not display the Create Rewrite Policy dialog box but disables the main configuration utility window.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0333048: If you access the configuration utility through Internet Explorer 8, an attempt to bind 250 or more VIP addresses to a VLAN results in an error message about an unresponsive script.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

  Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0334042: The configuration utility does not display a details panel for all the entities.

Workaround: Click 'Edit' to display the details.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the Create DNS View dialog box, the "Service(s) in this view" and "Policy(s) in this view" lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs.

  Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0338513: When you log on to NetScaler configuration utility using Internet Explorer 8 or Internet Explorer 9, the web browser displays a blank screen as the browser is displaying the compatibility view.

  Workaround: Change to the standard view, in the Compatibility View Settings dialog box, by clearing the Display all websites in Compatibility View check box.

- Issue ID 0349813: If you use the configuration utility to unbind all the cipher suites from a user-defined SSL cipher group, the user-defined cipher group is deleted from the appliance.

- Issue ID 0352307: If you access the NetScaler configuration utility from a Mac machine with a client environment running JRE 1.7 or later, you cannot select the fields in the Java based configuration views.

  Workaround: If you click outside and return to the browser window, you will be able to select the fields in the configuration views.

- Issue ID 0353015: Load balancing virtual servers that are used by AppExpert applications are displayed in nodes other than the AppExpert node. For example, they are displayed in the Available Virtual Servers list (Load Balancing > Persistency Groups > Add > Create Persistency Group dialog box), and in the Target LB Virtual Server list (Content Switching > Actions > Add > Create Content Switching Action dialog box > Name option button).

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated.

Domain Name System

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If a GSLB virtual server's primary GSLB method is set to round trip time (RTT) and backup GSLB method is set to static proximity, or if the primary GSLB method is set to static proximity and backup GSLB method is set to RTT, and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

Load Balancing

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the "show lb persistentSessions" CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 91711/0250846: If the string (or "token") that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR("string2").AFTER_STR("string1") if the string that is enclosed by "string1" and "string2" is not larger than 64 KB.

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

Load Balancing/SSL

- Issue ID 0331621: While creating SSL or load balancing virtual servers with default responder action, the NetScaler appliance throws a “No such resource” error. This issue is observed only in a cluster setup.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type: `#/etc/rc.d/svmd restart`

- Issue ID 0337386: When restored from a backup, a NetScaler instance is reprovisioned by using the NetScaler XVA image currently available on the appliance, even if the backup was taken from an upgraded configuration. If multiple XVA images are available, the XVA image that was used to originally provision the instance is used, if available, to reprovision the instance. If that image is not available, any XVA image is used.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.
- Issue IDs 0283035 and 0299716: In a cluster setup, the bind vlan command throws an error when interface and IP address are specified together.
- Issue ID 0288450: The show lacp command does not display the lacp configurations. This issue is observed only in a cluster setup.
- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command set ptp -state disable and configure NTP to synchronize the time across the cluster nodes.
  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator, and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed.

  Workaround: Copy the certkey under /nsconfig/ssl/ folder on all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.
- Issue ID 0343395: On the NetScaler appliance, TLS protocol version 1.2 does not support a client certificate with RSA 4096-bit key.
- Issue ID 0345883: On the NetScaler appliance, TLS protocol version 1.2 does not support ephemeral Diffie-Hellman cipher suites.
- Issue ID 0352334: TLS protocol, version 1.2, handshake fails if all the following conditions are met:
  - The Client browser is Internet Explorer.
  - Client authentication is set to mandatory on the virtual server.
  - The configured client certificate on IE browser is not signed by SHA256 hash algorithm.

XML API

- Issue ID 0321005: The API to set the hostname for a NetScaler appliance is changed to include the owner node parameter for a cluster node.

Build 72.5

Release version: Citrix® NetScaler®, version 10 build 72.5

Replaces build: None

Release date: November 2012

Release notes version: 5.0

Language supported: English (US)

Review the following sections:

- Changes
- Bug Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler and Citrix Access Gateway.

Changes

Configuration Utility

- Issue ID 0317403: On the Monitoring tab, when you disable a virtual server or a service, a confirmation window is displayed to confirm the disable operation.

Content Switching

- Issue ID 0248750: In this release, for a content switching policy that uses a default syntax rule, you can specify the target load balancing virtual server in a content switching action. In the content switching action, you can specify the name of the target load balancing virtual server, or you can configure a request-based expression that, at run time, computes the name of the load balancing virtual server to which to send the request. The expression option can drastically reduce the size of your content switching configuration, because you need only one policy per content switching virtual server. Content switching policies that use an action can also be bound to multiple content switching virtual servers, because the target load balancing virtual server is no longer specified in the content switching policy. The ability to bind a single policy to multiple content switching virtual servers helps to further reduce the size of your content switching configuration.

  You can also, for a content switching policy that uses a default syntax rule, specify the target load balancing virtual server when binding the policy to a content switching virtual server, as you would in earlier releases, without the need for a separate action. For domain-based and URL-based policies, an action is not available, and you continue to specify the name of the target load balancing virtual server when binding the policy to a content switching virtual server.

  For more information, see http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-map/ns-cs-basicconfig-config-cs-action-con.html.

Load Balancing

- Issue ID 0345300: If a UDP connection that is being managed by a load balancing virtual server of type UDP, SIP_UDP , DNS, RADIUS , or ANY is blocked pending a decision on persistence, and the associated protocol control block is freed before all the NetScaler buffers that reference the protocol control block are processed, the appliance might fail.

SSL

- Issue ID 0236585: You can now load a certificate bundle containing one server certificate, up to nine intermediate certificates, and optionally, a server key. Separate steps for loading and linking the certificates are no longer required.

- Issue ID 0338862: If you unbind all the cipher suites from a user-defined cipher group by using the command line, the user-defined cipher group is not deleted from the appliance.

Bug Fixes

AAA Application Traffic

- Issue IDs 0272417 and 0344661: SSO using 401-based authentication fails when an initial user request is redirected to another URL.
- Issue ID 0345220: If a AAA virtual server is configured for two-factor authentication with RADIUS challenge/response in a single-signon (SSO) environment, with the SSO name extracted from the primary authentication service and the second factor from RADIUS challenge/response, the wrong user name might be extracted. This can result in intermittent authentication failures.

Access Gateway

- Issue ID 0330636: When users log on with the Access Gateway Plug-in to an nCore Access Gateway appliance, occasionally when server-initiated connections occur, depending on the core through which the traffic is passed, the user device may fail.
- Issue IDs 0332483 and 0336091: If you have a VLAN configuration on the NetScaler appliance, when users log on with the Access Gateway Plug-in, occasionally server-initiated connections to the user device fail.
- Issue ID 0337609: When you integrate Access Gateway with a SharePoint site, after users log on successfully, when they open a Microsoft Office document, the session ends and the logon page appears.
- Issue IDs 0340122 and 0337613: After users upgrade to Access Gateway 10, Build 70.7, if you have a high availability configuration that includes an FTP server, when users log on with the Access Gateway Plug-in and initiate an FTP session, occasionally Access Gateway fails on both primary and secondary appliances while the FTP connection is active.
- Issue ID 0348694: If a published application is configured to require a user name with both capital and lower-case letters and is configured for single sign-on, after users log on with the Access Gateway Plug-in with the same user name, when they open a published desktop from the Web Interface and try to open the published application, they are prompted to enter their credentials again.
- Issue ID 0349178: After users log on to the StoreFront-based store remotely over Access Gateway from a browser and then select Log out under the users' name on the page, a page appears with message "Logoff is successful" and includes a Log on button. If users click Log on, the Storefront store-based web page is available again and authentication is not required.

AppFlow

- Issue ID 0344666: When the appflow policy evaluation fails, the NetScaler appliance sometimes continues to attempt “Appflow Logging” because of which it fails.

Application Firewall

- Issue ID 0346118: If sessionless form field consistency is enabled, a memory leak can cause fill up on the NetScaler appliance’s memory.
- Issue ID 0346384: If the Start URL feature is configured to use an uploaded HTML error object instead of an error URL, the start URL feature cannot block access to "/" even if you exclude "/" from the start URLs list.

CloudBridge

- Issue ID 0325718 (nCore): The amount of memory allocated to a packet engine can be retrieved by using show ns stat command (value of InUseMemory) or by SNMP polling (value of resMemUsage). There was a mismatch in InUseMemory and resMemUsage value for the same packet engine due to difference method used to calculate the allocated memory. This mismatch problem is now resolved and both the methods return the correct value.

Cluster

- Issue ID 0343514: The cluster instance view in the configuration utility does not display which node is the configuration coordinator.

Configuration Utility

- Issue ID 0329547 (nCore): In some cases, the value to which you set the prefetchPeriodMilliSec parameter for a cache content group might not be saved in the nsconfig file.
- Issue ID 0332839: If you access the configuration utility through Internet Explorer 8, the System > Settings > Configure TCP Parameters, dialog box has no spaces between field names and fields.
- Issue ID 0334292: If you navigate to HTTP Compression > Policies or HTTP Compression > Actions, the 'Remove' button is disabled in the task pane.

  Note: You can access the command line interface from the configuration utility. Navigate to System > Diagnostics > Command Line interface.
- Issue ID 0335701: You cannot add an SSL service with the Clear Text Port option in the configuration utility, because the option is disabled.
- Issue ID 0336854: When you open a log file in Syslog messages viewer, all the logs are not displayed when the uncompressed log file size is more than 10MB.
- Issue ID 0342735: Users might not be able to enable or disable NTP synchronization by using the configuration utility.
- Issue ID 0345828: When you log on to the NetScaler configuration utility by using certain versions of Internet Explorer 8, the web browser does not load the configuration utility.
- Issue ID 0346060: When you access the NetScaler configuration utility from a client environment using JRE 7, in certain configurations, the NetScaler configuration utility displays "Operation in Progress" message when you open a load balancing virtual server configuration.

Content Switching

- Issue ID 0315161: A NetScaler appliance fails under the following sequence of events:

  1. You associate an HTTP load balancing virtual server with an HTTP profile and a backup load balancing virtual server of type TCP.
  2. You configure a content switching virtual server to switch requests on the basis of content switching policies, and you set the load balancing virtual server as a target for the content switching virtual server.
  3. The HTTP load balancing virtual server goes down.
  4. When the content switching virtual server receives a request, it happens to select the load balancing virtual server.
  5. Because the HTTP virtual server is down, the content switching virtual server selects the backup load balancing virtual server, which is of type TCP.
  6. The appliance attempts to access the HTTP profile, which cannot be associated with a load balancing virtual server of type TCP.
- Issue ID 0344944: When you remove a content switching virtual server, the NetScaler appliance fails to remove some or all of the configuration information that binds load balancing virtual servers to the content switching virtual server. Consequently, if the state of a load balancing virtual server changes, the appliance attempts to update the state of the content switching virtual server, which no longer exists. When attempting such a state update, the appliance fails.

Domain Name System

- Issue IDs 0330529 and 0322151: The following message might be displayed if you disable a virtual server-based DNS name server: 'ERROR: Name server does not exist. [nsnet_recvrpcioctl]'

Global Server Load Balancing

- Issue ID 0308555: In certain scenarios, if the primary and backup GSLB methods are static proximity and dynamic RTT, respectively, requests for domain name resolution are not processed correctly. As a result, the appliance can fail.

Integrated Caching

- Issue ID 0331520: After an upgrade to 10.0, the NetScaler appliance might occasionally fail because of internal memory handling issues.

Load Balancing

- Issue ID 0333200: If rule based persistence is configured for a load balancing virtual server, and the virtual server receives traffic from a content switching virtual server, the load balancing virtual server's persistence sessions expire at the end of the configured timeout period, even if new requests arrive before session expiry.

Load Balancing/AAA Application Traffic

- Issue ID 0346093: The traffic management policy hit count shows no hits ("0"), even when traffic management policies are functioning and matching traffic.

Monitoring

- Issue ID 0339736: The NetScaler appliance might fail when generating the SNMP trap described in the following scenario:
  - You set the response timeout threshold parameter for a monitor that is bound to a domain based service.
  - You configure the MONITOR-RTO-THRESHOLD SNMP alarm on the NetScaler appliance.
  - The response timeout threshold is exceeded by a domain based service, and the appliance attempts to generate the monRespTimeoutAboveThresh trap.

Networking

- Issue ID 0334312: During a warm restart of the NetScaler appliance, a daemon might fail to start. After not receiving heartbeats from the daemon, the Pitboss process restarts the appliance.
- Issue ID 0336136: If a NetScaler appliance acting as a DHCP relay agent receives DHCP Discover traffic that is not from a Layer 3 VLAN, the appliance might disconnect from the default gateway and remain disconnected for some time.
- Issue ID 0336886: When a VIP with OSPF LSA TYPE-1 exists on the NetScaler appliance, any new VIPs configured with TYPE-5 are saved as TYPE-1.
- Issue ID 0341895: The state of the IPSEC tunnel becomes DOWN and SA reformation/rekeying does not happen after the IKE lifetime expires.
- Issue ID 0343578: The NetScaler appliance drops an ARP request if it arrives on a VLAN to which two different subnets are bound and the source IP address and the destination IP address in the ARP request packet belongs to these different subnets bound to the VLAN.

Policies

- Issue ID 0291487: NetScaler appliances running version 9.2 build 52.1 or later and have a large number (in the hundreds) of policy bindings can experience performance issues on 'save ns config' and 'show config' operations. This can lead to interruption in services.
- Issue IDs 0332600 and 0335877: The running configuration does not show the command used to bind a policy to a load balancing virtual server, in the following scenarios:
  - When a policy is globally bound.
  - When a service is bound to same load balancing virtual server.

SSL

- Issue ID 0302532: The NetScaler appliance fails if all of the following conditions are met:
  - A certificate revocation list (CRL) is present and linked with a CA certificate, and the CA certificate is continuously updated.
  - The CRL is uploaded by using HTTP, and auto refresh is enabled on the CRL.
  - Client authentication is enabled. Therefore, the client is verified for every GET request.

System

- Issue ID 0241964: The SNMP engine ID does not get saved to the ns.conf file after the configurations are saved. Hence the engine ID is not retained across reboots. Also, the default SNMP engine ID is not displayed on issuing the 'show snmp engineid' command.
- Issue ID 0306237: If the number of dynamic services running on the NetScaler appliance exceeds 64k, any service created could not be accessed even after when the number of services is less than 64k.
- Issue ID 0334585: The NetScaler appliance runs out of memory when processing the traffic management logout URL.

Web Interface

- Issue ID 0341459: An invalid argument error is thrown when you try to create a web interface site with default access method selected as 'GatewayDirect' and authentication point selected as 'Web Interface'.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0283556: Currently, the SAML implementation supports only RSA digital signatures. DSA digital signatures are not supported.
- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberoes authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, and then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.
- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

Access Gateway

- Issue ID 92543/0251596: After you configure Access Gateway to provide user connections through Citrix Receiver, when users right-click the Receiver icon in the notification area, the Log on option does not appear. Users must connect by using the Web browser or they must right-click the Receiver icon and then, depending on the version of Receiver they are using, click About or Preferences from the Receiver menu and Plug-in Status or Advanced from the Receiver panel. You can also enable the log on option to appear when users right-click the Receiver icon by adding the following settings in the registry:
  - Add the Receiver key (if the key does not already exist) under the following registry locations:
    - `HKEY_CURRENT_USER\Software\Citrix\`
    - `HKEY_LOCAL_MACHINE\Software\Citrix\`
  - Add the Inventory key in the following registry locations:
    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`
    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`
  - In the Inventory key, configure the following **REG_SZ** values:
    - **VPNAddress**. Provide the value as the Web address for the Access Gateway appliance; for example, https://<AccessGatewayFQDN>.
    - **VPNPrompt1**. Provide the value as 'UserName'.
    - **VPNPrompt2**. Provide the value as '*Password'.

      Note: To mask the password, enter an asterisk (*) before the word.

      In addition, if you configure double-source authentication that requires authentication with LDAP plus RSA authentication, you need to also add the following as **REG_SZ**:
    - **VPNPrompt3**. Provide the value as '*Passcode'.
- Issue ID 0261547: When you enable Access Gateway as a reverse proxy and you enable basic preauthentication and post- authentication scans, as well as encryption and client choices, when users log on with the Access Gateway Plug-in, the preauthentication scan passes, but the post-authentication scan fails.
- Issue ID 0275079: When users access applications published on XenApp, each user consumes multiple Access Gateway licenses per application. Instead, one session ID should be shared across the applications the user accesses. As a result, users exceed their allocated license count and an SSL error occurs.
- Issue ID 0278218: If you configure an endpoint policy, the preauthentication policy runs as expected. When users try to log on with the Access Gateway Plug-in, however, occasionally the post-authentication policy does not work as expected and authentication fails.
- Issue ID 0285995: If you configure Access Gateway to assign an intranet IP address to user devices that connect to Access Gateway, when users log on with the Access

Gateway Plug-in, the secure DNS dynamic update does not occur and the intranet IP address is not registered with the DNS Server.

- Issue ID 0288469: After you configure a virtual server to use the Access Gateway Plug-in for Java, when users log on with the Access Gateway Plug-in by using a browser that has a 64-bit Java Runtime Environment (JRE) installed, the plug-in fails to establish a connection.

- Issue ID 0291264: If you create a Web Interface 5.4 site and enable authentication through Access Gateway, and you enable single sign-on with a smart card to the Web Interface that enables smart card pass-through, when users log on with the Access Gateway Plug-in, the users' desktops are not listed on the Web Interface.

- Issue ID 0291821: If you create a Web Interface 5.4 site and enable authentication with a smart card through Access Gateway, and you configure the 'Single Sign-on Domain' on the 'Published Applications' tab using the format domainname.com instead of domainname, when users start a published application or desktop, authentication fails.

- Issue ID 0292005: When users connect with clientless access and try to download a file larger than 1 gigabyte (GB) from the file share on the home page, as the file is downloading, if an upload is attempted, the download process fails but the upload continues.

- Issue ID 0298971: When users log on with the Access Gateway Plug-in for Java and the Web Interface opens in Internet Explorer 9, if users do not turn on Compatibility View in Internet Explorer, when they click a published application, the following error appears: Resource shortcuts are not available.

- Issue ID 0299515: If you configure an intranet IP address on Access Gateway, when users connect with the Access Gateway Plug-in on a computer running Windows XP Service Pack 3 and try to access a CIFS share hosted on a computer in the secure network, users receive an error that the share is inaccessible.

- Issue ID 0300511: When users log on using clientless access and click a bookmark from the home page to open a Distributed File Share (DFS), if the target folder resides on a different computer than the computer where the domain DFS server resides, the share does not open.

- Issue ID 0309017: When you configure a preauthentication and post-authentication policy with an expression to scan a user device for a file, Access Gateway does not check for expression syntax. As a result, Access Gateway accepts inappropriate syntax configuration and the scan fails.

- Issue ID 0327433: If you configure a virtual server by using the Remote Access wizard and configure a Secure Ticket Authority (STA), the status of the server appears as UP. However, in the configuration utility, on the Home tab, under Alerts, a message states that the STA server is not configured. You must bind the server globally in order to clear the message.

- Issue ID 0337886: If users select Automatically detect settings in Internet Explorer on a computer running Windows XP, when users log on with the Access Gateway Plug-in and then log off from Access Gateway, the Automatically detect settings check box is not restored to the previously configured setting.

- Issue ID 0338451: If hundreds of concurrent sessions occur, the generation of a support file takes several hours.

- Issue ID 0340346: If you configure a session time-out setting, after users connect to Access Gateway, even though the session expires according to the value you enter, the actual process of closing the session takes longer.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

AppFlow

- Issue ID 0327439: AppFlow records generated by the NetScaler appliances cannot be seen on SPLUNK.
- Issue ID 0333560 (nCore): AppFlow records generated by the NetScaler appliance might contain junk characters.

Application Firewall

- Issue ID 0272715: If you use the Google Chrome browser with the default Chrome PDF plugin to view the PCI-DSS report, certain links and pages do not render correctly.

  Workaround: Disable Chrome PDF and install the Adobe Acrobat Reader plugin for Chrome.
- Issue ID 0282932: If you use the Signature Editor to add a signature rule for a response-side check (such as the Credit Card or Safe Object check), in addition to one or more response patterns you must also add at least one request pattern. If you do not, then when you try to save the new signature rule, the configuration utility displays an error message and does not save the rule.
- Issue ID 0283780: If you enable the sessionless URL closure feature, you must also enable the URL closure feature. If you do not, the sessionless URL closure feature does not work.
- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked. To work around this issue, if you configure Sessionless URL Closure, set Validate Referer Header to Off.
- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported for importing as application firewall signature rules. WAS 2.0 scan reports are not supported.
- Issue ID 0303060: Application firewall statistics are not supported for NetScaler classic policies. If you need to see numbers of policy hits and other statistics, you must use NetScaler default syntax policies.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

Cluster

- Issue ID 0343137: The configuration utility does not display the "Add" button while configuring linksets.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click 'Application Firewall' in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0303279: In the configuration utility, in the Rewrite Policies pane, clicking Add does not display the Create Rewrite Policy dialog box but disables the main configuration utility window.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0324797: The NetScaler configuration utility does not display the queue depth value for the configured priority queuing policies. This issue is observed only in a cluster setup.

  Workaround: You can view the queue depth of the policy by using the 'show pq policy' command on the command line interface.

- Issue ID 0333048: Using the Configuration Utility in Internet Explorer version 8, when you attempt to bind 250 or more VIP addresses to a VLAN, the Configuration Utility displays an unresponsive script error.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

  Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0334042: The configuration utility does not display a details panel for all the entities.

  Workaround: Click 'Edit' to display the details.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the 'Create DNS View' dialog box, the 'Service(s) in this view' and 'Policy(s) in this view' lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs.

  Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0338513: When you log on to NetScaler configuration utility using Internet Explorer 8 or Internet Explorer 9, the web browser displays a blank screen as the browser is displaying the compatibility view.

  Workaround: Change to the standard view, in the Compatibility View Settings dialog box, by clearing the Display all websites in Compatibility View check box.

- Issue ID 0349813: If you use the configuration utility to unbind all the cipher suites from a user-defined SSL cipher group, the user-defined cipher group is deleted from the appliance.

- Issue ID 0352307: If you access the NetScaler configuration utility from a Mac machine with a client environment running JRE 1.7 or later, you cannot select the fields in the Java based configuration views.

  Workaround: If you click outside and return to the browser window, you will be able to select the fields in the configuration views.

- Issue ID 0353015: Load balancing virtual servers that are used by AppExpert applications are displayed in nodes other than the AppExpert node. For example, they are displayed in the Available Virtual Servers list (Load Balancing > Persistency Groups > Add > Create Persistency Group dialog box), and in the Target LB Virtual Server list (Content Switching > Actions > Add > Create Content Switching Action dialog box > Name option button).

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated.

Domain Name System

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If a GSLB virtual server’s primary GSLB method is set to round trip time (RTT) and backup GSLB method is set to static proximity, or if the primary GSLB method is set to static proximity and backup GSLB method is set to RTT, and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

Load Balancing

- Issue ID 0278377 (nCore): Cache policy labels cannot be bound to MYSQL or MSSQL virtual servers.
- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the 'show lb persistentSessions' CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.
- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).
- Issue ID 91711/0250846: If the string (or 'token') that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR('string2').AFTER_STR('string1') if the string that is enclosed by 'string1' and 'string2' is not larger than 64 KB.
- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.
- Issue ID 0278377 (nCore): Cache policy labels cannot be bound to MYSQL or MSSQL virtual servers.
- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

Load Balancing/SSL

- Issue ID 0331621: While creating SSL or load balancing virtual servers with default responder action, the NetScaler appliance throws a 'No such resource' error. This issue is observed only in a cluster setup.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type : #/etc/rc.d/svmd restart

- Issue ID 0337386: When restored from a backup, a NetScaler instance reverts to the release and build in which it was originally provisioned, even if the backup was taken from an upgraded configuration.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.

- Issue IDs 0283035 and 0299716: In a cluster setup, the 'bind vlan' command throws an error when interface and IP address are specified together.

- Issue ID 0288450: The 'show lacp' command does not display the lacp configurations. This issue is observed only in a cluster setup.

- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command 'set ptp -state disable' and configure NTP to synchronize the time across the cluster nodes.

  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator, and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed.

  Workaround: Copy the certkey under /nsconfig/ssl/ folder on all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.
- Issue ID 0343395: On the NetScaler appliance, TLS protocol version 1.2 does not support a client certificate with RSA 4096-bit key.
- Issue ID 0345883: On the NetScaler appliance, TLS protocol version 1.2 does not support ephemeral Diffie-Hellman cipher suites.
- Issue ID 0352334: TLS protocol, version 1.2, handshake fails if all the following conditions are met:
  - The Client browser is Internet Explorer.
  - Client authentication is set to mandatory on the virtual server.
  - The configured client certificate on IE browser is not signed by SHA256 hash algorithm.

XML API

- Issue ID 0321005: The API to set the hostname for a NetScaler appliance is changed to include the owner node parameter for a cluster node.

Build 71.6

Release version: Citrix® NetScaler® release 10 build 71.6

Replaces build: None

Release date: October 2012

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Changes
- Bug Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler and Citrix Access Gateway.

Changes

Configuration Utility

- Issue ID 0319070: The Setup wizard is not launched automatically if a mapped IP (MIP) address or a Subnet IP (SNIP) address is not configured on the NetScaler appliance.

NetScaler SDX Appliance

- Issue ID 0332251: You can now configure LACP from within a NetScaler VPX instance hosted on a NetScaler SDX appliance. Make sure that the interfaces that are part of the channel are not shared with other instances, and a dedicated channel is configured for an instance. For more information, see Configuring LACP on a NetScaler VPX Instance.

Bug Fixes

AAA Application Traffic

- Issue ID 0319434: If 401 basic authentication is enabled on a load balancing virtual server, and authentication fails either due to invalid credentials or a Kerberos authentication failure, the NetScaler packet engine might crash.

Access Gateway

- Issue ID 82828/0243556: You can configure a forced time-out to disconnect the Access Gateway Plug-in automatically with a value (in minutes) that exceeds 255. You can now enter a value as high as 3,000 (in minutes, which is equivalent to 50 hours).
- Issue ID 0331288: When split tunneling is OFF, when users try to connect with an Access Gateway Plug-in, occasionally host routes added by the plug-in may block communication between the Internet IP address and the Domain Name Server. Users may experience network connectivity issues, such as the inability to access file shares on the network.
- Issue ID 0329113: When you configure Intranet IP addresses on Access Gateway and bind the addresses to a virtual server, the bound IPs addresses do not appear in the configuration utility.
- Issue ID 0329603: When you enable a preauthentication scan, and you enable the user device to connect through a proxy server, when users log on with the Access Gateway Plug-in for the Mac OX X Version 2.1.3, Access Gateway fails.
- Issue ID 0336499: When users log on to Access Gateway by using Citrix Receiver and then log off by using the Receiver icon in the taskbar, the computer loses network access. To restore network access, users must either disable and then enable their network interface or restart their computer. To avoid the issue, users can log off from the Access Interface home page.
- Issue ID 0338220: If you configure client certificate-based expressions for preauthentication or post-authentication scans, when users try log on to Access Gateway, occasionally, the scan fails. To avoid the issue, you can use the classic or MPX 5500 platforms or you can bind the certificate-based policy globally to a virtual server.

Application Firewall

- Issue ID 0329401: On a NetScaler appliance that has the Application Firewall enabled and both cookie transformation and encryption on, secure memory usage increases slowly and continuously until the NetScaler appliance starts to drop connections.
- Issue ID 0332176: On a NetScaler appliance that has the application firewall enabled, user logons can be extremely slow. The cause is that a back-end server does not set a Content-Length header that the NetScaler expects. As a result the NetScaler appliance does not close the connection with the user's browser. To work around this issue, you can do one of the following:
  - Add a rewrite policy to the configuration that appends a content-length header of zero ('Content-Length: 0') to the logon page.
  - Disable the application firewall.
- Issue ID 0333332: When signatures that work on post body are enabled, a large post request may cause an HA failover.
- Issue ID 0335102: On a NetScaler appliance that has the application firewall enabled, adding a large number of signatures objects can cause high CPU loads.

CloudBridge

- Issue ID 0313629: When the time on a NetScaler is modified, either due to Network Time Protocol Daemon (NTPD) or other external factors to the time lesser than the boot time, the iked process may start consuming 100% of CPU resources.
- Issue ID 0334949: If you use configuration utility to remove an IPv4 tunnel for CloudBridge from a NetScaler appliance, the remove process succeeds but the following Java exception is displayed 'ClassNotFoundException'.

Cluster

- Issue ID 0332594: The RIP (Routing Information Protocol) and Cache Redirection features cannot be enabled in a NetScaler cluster setup.

Configuration Utility

- Issue ID 93754/0257608: When you view the configuration difference between files, the corrective commands generated for bind or unbind commands of load balancing and content switching virtual servers might not be accurate in some cases.
- Issue ID 0305248: In the Reporting tool, when users try to generate a 'system entities statistics' report for load balancing virtual servers, the load balancing virtual servers configured on the appliance might be displayed as being inactive. Users cannot choose the virtual server to view the statistics.
- Issue ID 0310203: In the Reporting tool, when users try to generate a custom report for load balancing virtual servers, the virtual servers might be displayed as being inactive. Users cannot choose the virtual server to view the statistics.
- Issue ID 0333577: When configuring the Transformation URL Profile, an error occurs if you set Priority to a value higher than 2147483647 (maximum allowed value).
- Issue ID 0333836: If you have configured global server load balancing by using the GSLB wizard, Wizard for Citrix XenApp, or Wizard for Citrix XenDesktop, and you attempt to view the GSLB Visualizer, Prefuse information might be logged to the Java console. However, you can view the GSLB Visualizer, and the functionality is not affected.
- Issue ID 0334280: After you rename a compression policy, the new name might not be reflected in the configuration utility.
- Issue ID 0334284 If you navigate to HTTP Compression > Policies and click Policy Manager in the task pane, the following error message might appear: No such policy exists.
- Issue ID 0334773: In the Synchronize 'GSLB Configuration' dialog box, the Command parameter is unavailable when the 'Synchronization Option' parameter is set to its default value (automatic synchronization).
- Issue ID 0335008: The exception 'netscape.javascript.JSException' is logged to the Java console when you create a DNS key by using the NetScaler configuration utility. However, the DNS key is created, and there is no loss in functionality.
- Issue ID 0335235: The NetScaler configuration utility does not show globally bound AppFlow policies in the policy manager. This issue is observed only in a cluster setup.
- Issue ID 0335701: You cannot add an SSL service with the Clear Text Port option in the configuration utility, because the option is disabled.
- Issue ID 0335719: The exception 'netscape.javascript.JSException' is logged to the Java console when you sign a DNS zone by using the NetScaler configuration utility, and the browser’s status bar does not report the status of the zone-signing operation. However, the zone is signed, and there is no loss in functionality.
- Issue ID 0335913: In a cluster setup, you cannot enable a server entry that is disabled, because the 'Enable' button is unavailable. However, you can disable a server entry by using the NetScaler command line interface.

Domain Name System

- Issue IDs 0268748 and 0333310: In a cluster setup, if you save the configuration and reboot an appliance, the default name-server records for the thirteen root servers, and their associated address records, become unavailable. If you need them, you have to add them manually after you perform a reboot.
- Issue ID 0318199: If core memory is not available when the NetScaler appliance is processing an RRSIG record received in a response, the appliance fails.
- Issue ID 0319100: Default DNS actions, policies, and policy bindings are not displayed in a cluster setup.

Integrated Caching

- Issue ID 0334895: On a NetScaler appliance configured with five policy engines, responses might not be cached even if memory is available for caching.
- Issue ID 0337446: When a byte-range request sent to integrated cache is larger than the size of cached object and the if-range header is also set, the NetScaler appliance fails.

Load Balancing

- Issue ID 0314738: If you issue the 'force HA sync -force' command when HA synchronization is disabled on both nodes, the services on the secondary node are marked as DOWN. The services remain in that state until after a failover. When a failover occurs, the failover of some services might be delayed by a few seconds while monitors learn the actual states of those services. Until the monitors learn and correct the states, new connections to those services might be rejected. Consequently, you might also observe a brief period of outage following a failover.
- Issue ID 0318310: While creating a load balancing monitor, you cannot specify a send string that has a length of more than 76 characters. This issue is observed only in a cluster setup.
- Issue ID 0336400: In a two-node cluster that has been configured with a small number of services, if you restart a node or disable and reenable a node, the node might indefinitely remain in the service-state-synchronization stage.

NetScaler SDX Appliance

- Issue ID 0331900: If you try to upload a file larger than 300 MB to the NetScaler SDX appliance, the upload fails.
- Issue ID 0332313: 100 percent CPU usage is observed when the Management Service takes daily backup.
- Issue ID 0332819: If you try to create a high availability pair between two VPX instances without explicitly logging on to the second instance, an error message appears.
- Issue ID 0334340: If you upgrade the Management Service on which a NetScaler instance with a description of greater than 32 characters is provisioned, the instance is not migrated, and therefore, complete data related to the instance is not available in the database. Later, if you delete this instance and provision a new instance with the same IP address, the operation fails.
- Issue ID 0337090: A NetScaler VPX instance provisioned on an SDX appliance might fail if a warm restart is performed on the instance.

Networking

- Issue ID 0322026: In an L2 DSR configuration, packets arriving on the loop back interface are dropped even when the traffic rate on the interface is low.

Platform

- Issue ID 0321989: NetScaler release 10 build 71.x is supported on the new MPX 5550/5650 platforms.

Policies

- Issue ID 0291975: The SYS.VSERVER('<vserver_name>').THROUGHPUT expression returns an incorrect throughput value.
- Issue ID 0337576: The Netscaler might become unresponsive, if you used a request URL with encoding (for example, using %20) in an expression to the left of ALT, &&, or ||, and clauses to the right used strings. In addition, if the request URL was concatenated with another string, the final result would incorrectly contain a decoded URL, not the encoded one.
- Issue ID 0338916: Policies that are bound to policy labels are not available in the ns.conf file after saving the configurations. As a result, these bindings are lost after the appliance is rebooted.

SSL

- Issue ID 0257122: The close-notify parameter setting for an entity no longer has to be inherited from the global settings. You can set the close-notify parameter at the entity (virtual server, service, or service group) level. This enhancement provides the flexibility to set this parameter for one entity and unset it for another entity. However, make sure that you set this parameter at the global level. Otherwise, the setting at the entity level does not apply.
- Issue ID 0336920: On a cluster setup, replicating session entries across the nodes of the cluster is not supported.

System

- Issue ID 0277102: When you execute the 'show events' command, the NetScaler appliance might fail if the number of events to be displayed is more than 2^31.
- Issue ID 0333385: A hash collision might put the NetScaler aggregator into a recursive loop, causing the aggregator to fail. The NetScaler appliance might also fail, because of the aggregator failure.
- Issue ID 0336838: If HTML Injection and EdgeSight Monitoring are enabled on a NetScaler appliance and an HTTP request with a blank referer header is received, the appliance fails.
- Issue ID 0338244: The CallHome feature checks for compact flash drive and hard disk drive errors every six minutes instead of every six hours. If any errors are found, the appliance's data is uploaded to the Citrix Technical Support server.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberoes authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, and then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.

- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

- Issue ID 0327446: On an Outlook for Web Access (OWA) 2010 server that is protected by AAA-TM with single sign-on (SSO) enabled, when a user who uses the Firefox or Chrome browsers logs off, some OWA 2010 images do not appear.

- Issue ID 0334363: In the Citrix NetScaler configuration utility, when a user clicks the AAA-Application Traffic Wizard link, the configuration utility displays error message of 'Unknown Error'. The browser is then frozen til the session times out.

Access Gateway

- Issue ID 0340346: If you configure a session time-out setting, after users connect to Access Gateway, even though the session expires according to the value you enter, the actual process of closing the session takes longer.

- Issue ID 0278218: If you configure an endpoint policy, the preauthentication policy runs as expected. When users try to log on with the Access Gateway Plug-in, however, occasionally the post-authentication policy does not work as expected and authentication fails.

  - Issue ID 0327433: If you configure a virtual server by using the Remote Access wizard and configure a Secure Ticket Authority (STA), the status of the server appears as UP. However, in the configuration utility, on the Home tab, under Alerts, a message states that the STA server is not configured. You must bind the server globally in order to clear the message.
- Issue ID 0275079: When users access applications published on XenApp, each user consumes multiple Access Gateway licenses per application. Instead, one session ID should be shared across the applications the user accesses. As a result, users exceed their allocated license count and an SSL error occurs.

- Issue ID 92543/0251596: After you configure Access Gateway to provide user connections through Citrix Receiver, when users right-click the Receiver icon in the notification area, the Log on option does not appear. Users must connect by using the Web browser or they must right-click the Receiver icon and then, depending on the version of Receiver they are using, click About or Preferences from the Receiver menu and Plug-in Status or Advanced from the Receiver panel. You can also enable the log on option to appear when users right-click the Receiver icon by adding the following settings in the registry:

  - Add the Receiver key (if the key does not already exist) under the following registry locations:

    - `HKEY_CURRENT_USER\Software\Citrix\`

    - `HKEY_LOCAL_MACHINE\Software\Citrix\`
  - Add the Inventory key in the following registry locations:

    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`

    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`
  - In the Inventory key, configure the following **REG_SZ** values:

    - **VPNAddress**. Provide the value as the Web address for the Access Gateway appliance; for example, https://<AccessGatewayFQDN>.

    - **VPNPrompt1**. Provide the value as 'UserName'.

    - **VPNPrompt2**. Provide the value as '*Password'.

      Note: To mask the password, enter an asterisk (*) before the word.

      In addition, if you configure double-source authentication that requires authentication with LDAP plus RSA authentication, you need to also add the following as **REG_SZ**:

    - **VPNPrompt3**. Provide the value as '*Passcode'.

- Issue ID 0261547: When you enable Access Gateway as a reverse proxy and you enable basic preauthentication and post- authentication scans, as well as encryption and client choices, when users log on with the Access Gateway Plug-in, the preauthentication scan passes, but the post-authentication scan fails.

- Issue ID 0285995: If you configure Access Gateway to assign an intranet IP address to user devices that connect to Access Gateway, when users log on with the Access Gateway Plug-in, the secure DNS dynamic update does not occur and the intranet IP address is not registered with the DNS Server.

- Issue ID 0288469: After you configure a virtual server to use the Access Gateway Plug-in for Java, when users log on with the Access Gateway Plug-in by using a browser that has a 64-bit Java Runtime Environment (JRE) installed, the plug-in fails to establish a connection.

- Issue ID 0291264: If you create a Web Interface 5.4 site and enable authentication through Access Gateway, and you enable single sign-on with a smart card to the Web Interface that enables smart card pass-through, when users log on with the Access Gateway Plug-in, the users' desktops are not listed on the Web Interface.

- Issue ID 0291821: If you create a Web Interface 5.4 site and enable authentication with a smart card through Access Gateway, and you configure the 'Single Sign-on Domain' on the 'Published Applications' tab using the format domainname.com instead of domainname, when users start a published application or desktop, authentication fails.

- Issue ID 0292005: When users connect with clientless access and try to download a file larger than 1 gigabyte (GB) from the file share on the home page, as the file is downloading, if an upload is attempted, the download process fails but the upload continues.

- Issue ID 0298971: When users log on with the Access Gateway Plug-in for Java and the Web Interface opens in Internet Explorer 9, if users do not turn on Compatibility View in Internet Explorer, when they click a published application, the following error appears: Resource shortcuts are not available.

- Issue ID 0299515: If you configure an intranet IP address on Access Gateway, when users connect with the Access Gateway Plug-in on a computer running Windows XP Service Pack 3 and try to access a CIFS share hosted on a computer in the secure network, users receive an error that the share is inaccessible.

- Issue ID 0300511: When users log on using clientless access and click a bookmark from the home page to open a Distributed File Share (DFS), if the target folder resides on a different computer than the computer where the domain DFS server resides, the share does not open.

- Issue ID 0309017: When you configure a preauthentication and post-authentication policy with an expression to scan a user device for a file, Access Gateway does not check for expression syntax. As a result, Access Gateway accepts inappropriate syntax configuration and the scan fails.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

AppFlow

- Issue ID 0333560 (nCore): AppFlow records generated by the NetScaler appliance might contain junk characters.

Application Firewall

- Issue ID 0282932: If you use the Signature Editor to add a signature rule for a response-side check (such as the Credit Card or Safe Object check), in addition to one or more response patterns you must also add at least one request pattern. If you do not, then when you try to save the new signature rule, the configuration utility displays an error message and does not save the rule.

- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked. To work around this issue, if you configure Sessionless URL Closure, set Validate Referer Header to Off.

- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported for importing as application firewall signature rules. WAS 2.0 scan reports are not supported.

- Issue ID 0303060: Application firewall statistics are not supported for NetScaler classic policies. If you need to see numbers of policy hits and other statistics, you must use NetScaler default syntax policies.

Cache Redirection

- Issue ID 0287688: If you set the 'L2Conn' parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the 'L2Conn' parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

Cluster

- Issue ID 0343514: The cluster instance view in the configuration utility does not display which node is the configuration coordinator.
- Issue ID 0343137: The configuration utility does not display the "Add" button while configuring linksets.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click 'Application Firewall' in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0303279: In the configuration utility, in the 'Rewrite Policies' pane, clicking 'Add' does not display the 'Create Rewrite Policy' dialog box but disables the main configuration utility window.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0324797: The NetScaler configuration utility does not display the queue depth value for the configured priority queuing policies. This issue is observed only in a cluster setup.

  Workaround: You can view the queue depth of the policy by using the 'show pq policy' command on the command line interface.

- Issue ID 0332839: If you access the configuration utility through Internet Explorer 8, the System > Settings > Configure TCP Parameters, dialog box has no spaces between field names and fields.

- Issue ID 0333048: Using the Configuration Utility in Internet Explorer version 8, when you attempt to bind 250 or more VIP addresses to a VLAN, the Configuration Utility displays an unresponsive script error.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0334042: The configuration utility does not display a details panel for all the entities.

  Workaround: Click 'Edit' to display the details.

- Issue ID 0334292: If you navigate to HTTP Compression > Policies or HTTP Compression > Actions, the 'Remove' button is disabled in the task pane.

  Workaround: Use the command line interface to remove the policy or action.

  Note: You can access the command line interface from the configuration utility. Navigate to System > Diagnostics > Command Line interface.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the 'Create DNS View' dialog box, the 'Service(s) in this view' and 'Policy(s) in this view' lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs.

  Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0335701: You cannot add an SSL service with the Clear Text Port option in the configuration utility, because the option is disabled.

- Issue ID 0338513: When you log on to NetScaler configuration utility using Internet Explorer 8 or Internet Explorer 9, the web browser displays a blank screen as the browser is displaying the compatibility view.

  Workaround: Change to the standard view, in the Compatibility View Settings dialog box, by clearing the Display all websites in Compatibility View check box.

- Issue ID 0342735: Users might not be able to enable or disable NTP synchronization using the configuration utility.

  Workaround: Use command-line interface to enable or disable NTP synchronization.

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated.

Domain Name System

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

- Issue IDs 0330529 and 0322151: The following message might be displayed if you disable a virtual server-based DNS name server: 'ERROR: Name server does not exist. [nsnet_recvrpcioctl]'

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If a GSLB virtual server’s primary GSLB method is set to round trip time (RTT) and backup GSLB method is set to static proximity, or if the primary GSLB method is set to static proximity and backup GSLB method is set to RTT, and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

Load Balancing

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the 'show lb persistentSessions' CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 91711/0250846: If the string (or 'token') that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR('string2').AFTER_STR('string1') if the string that is enclosed by 'string1' and 'string2' is not larger than 64 KB.

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

- Issue ID 0278377 (nCore): Cache policy labels cannot be bound to MYSQL or MSSQL virtual servers.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

Load Balancing/SSL

- Issue ID 0331621: While creating SSL or load balancing virtual servers with default responder action, the NetScaler appliance throws a 'No such resource' error. This issue is observed only in a cluster setup.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type:

  #/etc/rc.d/svmd restart

- Issue ID 0337386: When restored from a backup, a NetScaler instance reverts to the release and build in which it was originally provisioned, even if the backup was taken from an upgraded configuration.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.
- Issue ID 0283035 and 0299716: In a cluster setup, the 'bind vlan' command throws an error when interface and IP address are specified together.
- Issue ID 0288450: The 'show lacp' command does not display the lacp configurations. This issue is observed only in a cluster setup.
- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command 'set ptp -state disable' and configure NTP to synchronize the time across the cluster nodes.
  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator, and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed.

  Workaround: Copy the certkey under /nsconfig/ssl/ folder on all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.

XML API

- Issue ID 0321005: The API to set the hostname for a NetScaler appliance is changed to include the owner node parameter for a cluster node.

Build 70.7

Release version: Citrix® NetScaler® release 10 build 70.7

Replaces build: None

Release date: September 2012

Release notes version: 4.0

Language supported: English (US)

Review the following sections:

- Changes and Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler and Citrix Access Gateway.

Changes and Fixes

AAA Application Traffic

- Issue ID 0327114: On a NetScaler appliance with NetScaler 10 build 69.4 nc installed, if you use the configuration utility to configure authentication on a load-balancing virtual server, the following error message appears:

  No Authentication Host specified

  The configuration utility then removes the authentication host from the configuration. This behavior occurs regardless of whether you are configuring authentication host settings on the virtual server for the first time, or modifying existing authentication host settings on the virtual server.

Access Gateway

- Issue ID 0308733: If you configure Access Gateway with additional appliances in which global server load balancing (GSLB) is enabled, when users log on with the Access Gateway Plug-in, occasionally the connection times out, a time-out error appears, such as 'Your Citrix Access Gateway session timed-out and you are not connected,' and the session disconnects.

- Issue ID 0319901: If you enable Integrated Caching and Web Interface on Netscaler on an Access Gateway appliance, and then change the URL for the Web Interface, Access Gateway might fail.

- Issue ID 0320210: When users connect with the Access Gateway Plug-in on a computer running Windows XP, the Group Policy Object is not applied.

- Issue ID 0321425: If you configure a virtual server with a default authentication type by using the Access Gateway wizard, if Access Gateway restarts, the configuration is not maintained and authentication fails.

- Issue ID 0329621: If you configure an endpoint policy and bind the policy to a virtual server, the preauthentication policy is not working as expected. Users with devices that meet the requirements may not be able to log on to Access Gateway.

AppFlow

- Issue ID 0288343: You can now configure the source IP address (SNIP or MIP address), to be used for AppFlow traffic. When you add an Appflow collector by using the add appflow collector command, you can use the -netprofile option to associate a netprofile to which the source IP address is bound. By default, the Appflow exporter takes NSIP address as the source IP address if you do not specify the -netprofile option.

  > add appflow collector <col_name> -IPAddress <IP_addr> [-netprofile {netprofile_name}]

- Issue ID 0311033 (nCore): AppFlow records can now log X-Forwarded-For HTTP header information. You can enable the logging with the set appflow param -httpXForwardedFor ENABLED command or by using the configuration utility.

- Issue ID 0313091: AppFlow records might not display the start time of the current transaction. Instead, they display the start time of the previous transaction due to reuse of connections.

- Issue ID 0320239 (nCore): HTTP method names might be occasionally truncated in the AppFlow records.

Application Firewall

- Issue ID 0299940: The change profile type command does not work correctly.

  - If you try to change a profile type to Web 2.0, the profile type remains HTML.

  - If you try to change a profile type to XML, the Profile Type field disappears completely.

  When you use the configuration utility to change the profile type, the profile type is actually changed correctly, but the display is incorrect. When you use the NetScaler command line, the actual profile type is set as shown above.

- Issue ID 0302294: Learned relaxations are sometimes not removed from the review list after they have been deployed. To manually remove a learned relaxation that has already been deployed, in the Manage Learned Rules dialog box select the relaxation and then click Skip.

- Issue ID 0329539 (nCore): On a NetScaler appliance with the application firewall enabled, occasionally the NetScaler appliance crashes when retrieving a page from a protected web site that sets one or more cookies.

- Issue ID 0330642: On a NetScaler appliance with both the application firewall and Integrated Caching features enabled, the NetScaler appliance might experience occasional resets when its memory fills up. The cause is a small memory leak.

- Issue ID 0331112 (nCore): In the NetScaler 9.3 58.2.nc build, when applying the HTML or XML SQL Injection check the application firewall does not transform special strings even when Transformation is enabled. This issue was fixed in build 58.4.nc.

Cache Redirection

- Issue ID 0328353: When you use the configuration utility to bind a cache redirection policy to a cache redirection virtual server, the policy is added to the content switching (CSW) policy tab instead of cache redirection (CRD) policy tab. If you try to resolve this issue by using the CR virtual server wizard, the following error message appears: 'Please specify Target.'
- Issue ID 0330033: Tabs for filter/compression policy bindings are not displayed for a cache redirection virtual server, and it is not possible to bind those policies to a cache redirection virtual server.
- Issue ID 0330139: If you use the configuration utility to unset a cache virtual server for a cache redirection virtual server, the process fails and the following error message appears: invalid argument.

Call Home

- Issue ID 0311617: When upgrading the NetScaler appliance to 10.70 or a later build, the appliance prompts you to enable the Call Home feature.

Cloud Gateway

- Issue ID 0327119: When you create policy rules from the configuration utility, an error occurs and the policies are not configured.

Configuration Utility

- Issue ID 0298686 (nCore): If the details pane contains too may records to display on one screen, the header row moves off the screen if you scroll down.
- Issue ID 0311358: The NetScaler configuration utility fails to load when accessed from Internet Explorer version 7 browser running on Windows 2003 or Windows XP.
- Issue ID 0314769: When the certificate used to sign the JAR files expires, the application's digital signature cannot be verified. An error is displayed when the user tries to access the NetScaler GUI.
- Issue ID 0319061: The configuration utility does not throw the 'Feature not supported' prompt when configuring the following unsupported features on a NetScaler cluster: Bridge groups, Network Bridge, VMAC6, and FIS.
- Issue ID 0322821: When the SRADV (Static Route Advertisement) mode is ON, the static routes which are not explicitly disabled for advertisement will be advertised using all the routing protocols. However, the advertised protocols column for route in the configuration utility does not show any protocol list. This issue is observed only in a cluster setup.
- Issue ID 0322894: The configuration utility displays an inappropriate error message when adding a forwarding session that has an invalid subnet mask. This issue is observed only in a cluster setup.
- Issue ID 0322914: When the IP is not resolved for a hostname based SNMP manager, the 'Resolved IP' column of the SNMP Manager table is shown as blank instead of 'Unresolved IP'. This issue is observed only in a cluster setup.
- Issue ID 0323175: The configuration utility displays a negative value for the index of the data set or pattern set, when the index is set to its maximum value. The command line interface displays the correct value.
- Issue ID 0325400: After adding a local authentication policy by using the configuration utility, the request profile field is showing blank. By default, the request profile must be Local. This issue is observed only in a cluster setup.
- Issue ID 0326018: The dashboard does not display the Precision Time Protocol (PTP) counters for the cluster node. This issue is observed only in a cluster setup.
- Issue ID 0326354: In System > Settings > Change global system settings, regardless of the base threshold value configured for surge protection, the value is displayed as 0. This issue is observed only in a cluster setup.
- Issue ID 0326413: An error occurs if you use the NetScaler configuration utility to configure a large preauthentication policy (for example, a policy with 900 characters).
- Issue ID 0327136: The configuration utility does not allow you to set the 'Max Clients' parameter of a service to its maximum value of 4294967294. This issue is observed only in a cluster setup.
- Issue ID 0327551: In the configuration utility, all features appear to be enabled even when the features are disabled.

- Issue ID 0328660: In the configuration utility, when you view the virtual server persistence sessions, a persistence type setting of DIAMETER is displayed as SOURCE IP.

- Issue ID 0328715: In the configuration utility, the details of the monitor bound to a service do not include response codes for a monitor of type DIAMETER.

- Issue ID 0328747: In the Reporting tool, when users try to generate 'system entities statistics' report for GSLB domains, the GSLB domain names configured on the appliance might not be displayed in the entities list.

- Issue ID 0328844: While configuring the OCSP responder through the configuration utility, the default value of the HTTP response timeout is erroneously taken as 0ms. The default value of the HTTP response timeout must be 2000ms. This issue is observed only in a cluster setup.

- Issue ID 0329154: In System > Auditing > Recent audit messages, when you set number of audit messages to be displayed to 256 (maximum allowed value), a 'Value entered is out of range' error message is displayed on clicking Refresh. This issue is observed only in a cluster setup.

- Issue ID 0329826: If you use the configuration utility to view the license for features, warning messages are seen for the features that are licensed but not supported. This issue is observed only in a cluster setup.

- Issue ID 0331158: When you access NetScaler configuration utility from Internet Explorer 8 or Internet Explorer 9, the web browser displays only a grey bar at the top of the screen as the browser is displaying the compatibility view.

- Issue ID 0331604: If you access a load balancing virtual server after a NOPOLICY is bound to it, the configuration utility might display the following error: 'no such policy exists'

- Issue ID 0332795: On systems that have JRE 1.6.0_24 and 1.7.0_06, the configuration utility cannot load the Java applet. Therefore, you cannot perform any operations on the configuration utility.

- Issue ID 0332876: When you use the configuration utility to change the password of a user, the Change Password dialog displays encrypted password in the Password and Confirm Password fields.

- Issue ID 0333026: On a system running the Windows 7, 64-bit operating system, the configuration utility cannot load the Java applet. Therefore, you cannot perform any operations on the configuration utility.

Content Switching

- Issue ID 0230903: The content switching feature now supports the ability to bind a policy to multiple virtual servers or policy labels. To support multiple policy bind functionality, the target load balancing virtual server is specified in the action and attached to the policy. This enhancement enables you to reuse an existing policy by binding it to the virtual servers. You can also combine multiple policies in a policy label and apply the policy label to the virtual server.

- Issue ID 0330045: The configuration changes made by using the bind cs vserver and bind cs policylabel commands are not saved in the configuration file. Therefore, the CS policy bindings are lost the first time the NetScaler appliance is restarted after an upgrade to release 10.

- Issue ID 0330290: You cannot use the configuration utility to bind a content switching policy to a content switching virtual server if the policy is configured with only a domain value. The bind fails, and the following error message appears: 'Priority cannot be specified for URL-based content switching policy.'

- Issue ID 0331029: If you use the configuration utility to open a content switching virtual server that has a default policy bound to it, the process fails and the following error message appears: No Such Resource.

DataStream

- Issue ID 0323442: The DataStream feature does not support dynamic stored procedures. Consequently, dynamic stored procedures fail if they use the sp_prepexec and sp_prepare stored procedures.

Global Server Load Balancing

- Issue ID 0324486: When creating a local GSLB site in the NetScaler configuration utility, if you set the Trigger Monitors option to MEPDOWN, the GSLB site does not appear in the details pane until after you click 'Refresh'.

- Issue ID 0326364: Even though a GSLB virtual server is configured with the static proximity method, and some requests match a DNS policy whose action uses a DNS view to restrict matching requests to only a subset of the bound services, the NetScaler appliance uses the round robin method to load balance requests across all of the GSLB services that are bound to the GSLB virtual server. The issue can occur if the locations that correspond to the source IP addresses in the DNS requests are not found in the location database.

- Issue ID 0328911: When configuring monitoring for a GSLB service by using the NetScaler configuration utility, if you include monitors that cannot be used with GSLB services (for example, ARP monitors) along with monitors that can be used with GSLB services (for example, TCP monitors), the configuration utility displays an error message for the invalid monitor bindings, but the valid bindings succeed. When you unbind an invalid monitor from the service, the message 'Error' is displayed. No further information is provided in the message.

Integrated Caching

- Issue ID 0329485: When the NetScaler appliance responds to a byte range request, it might get into an infinite loop for one specific request, which might cause the appliance to fail.

Load Balancing

- Issue ID 0314738: If you issue the 'force HA sync -force' command when HA synchronization is disabled on both nodes, the services on the secondary node are marked as DOWN. The services remain in that state until after a failover. When a failover occurs, the failover of some services might be delayed by a few seconds while monitors learn the actual states of those services. Until the monitors learn and correct the states, new connections to those services might be rejected. Consequently, you might also observe a brief period of outage following a failover.

- Issue ID 0323317: The configuration commands for binding views to GSLB services are not shown in the output of the show ns runningConfig or show gslb runningConfig commands. Additionally, the configuration commands are lost during a reboot or upgrade.

- Issue ID 0323891: The NetScaler CLI and configuration utility display incorrect values for the following counters, which are used for monitoring services, including GSLB services :

  - Total number of monitoring probes sent

  - Total number of failed probes

  - Current number of failed probes
- Issue ID 0324061: When you configure a SIP-UDP load balancing virtual server by using the NetScaler command-line interface, the default setting for persistence type is CALLID. However, when you use the configuration utility to configure a SIP-UDP virtual server, the default setting for persistence type is NONE.

- Issue ID 0324576: The automatic domain based service group scaling option (the autoScale parameter) has been moved from the bind serviceGroup command to the add serviceGroup command. The possible values of the parameter have changed from YES and NO to DNS and DISABLED, respectively.

  To configure a service group to scale automatically, using the NetScaler command line, at the NetScaler command prompt, type the following command:

  add serviceGroup <serviceGroupName>@ <serviceType> -autoScale DNS

  To configure a service group to scale automatically, using the NetScaler configuration utility, go to Load Balancing > Service Groups > Add. In the Create Service Group dialog box, on the Advanced tab, from the Auto Scale Mode list, select DNS.

- Issue ID 0329191 (nCore): If an AppExpert application that was used to load user configuration to the NetScaler appliance is removed, the appliance becomes unavailable.

- Issue ID 0330276: The virtual router IDs (VRIDs) that are configured on the NetScaler appliance are not available in the Virtual Router ID list in the Create IP and Configure IP dialog boxes (Network > IPs > Add/Open). Consequently, you cannot use the configuration utility to bind a VRID to a virtual server.

Monitoring

- Issue ID 0320571: The state of a service is shown as UP even when the service is down. Consequently, the NetScaler appliance continues to forward requests to that service, and clients do not receive responses to their requests.

NetScaler SDX Appliance

- Issue ID 0326655: If you upgrade the Management Service from an earlier build to build 56.x or 57.x, restarting the appliance while data migration is in progress might corrupt your data contents.
- Issue ID 0326663: In release 9.3, the upgrade process fails if you attempt to upgrade the Management Service from build 48.6 to build 56.5 or 57.5.
- Issue ID 0326878: The Management Service shows duplicate entries for NetScaler VPX instances because of intermittent database connection failures. This is only a display issue. However, if a VPX instance is configured with an external authentication server for the nsroot (administrator) user, the authentication server might show several authentication failures.
- Issue ID 0327984: You can now apply a hotfix for XenServer from the Management Service. On the Configuration tab, expand Management Service, and then click XenServer Files. In the details pane, click Hotfixes, and then click Upload. After uploading the hotfix to the appliance, click Apply. If an error occurs in the process of applying the hotfix, an error message displays the cause of the problem.

NetScaler VPX Appliance

- Issue ID 0328540: After you install the initial NetScaler virtual appliance, if you try to save the configuration and licenses are not present on the appliance, the appliance becomes unresponsive. Restart the appliance and load the licenses. Restart the appliance again for the changes to take effect. Then save the configuration.
- Issue ID 0329966: After you install the initial NetScaler virtual appliance (.xva image) for build 69.4, if you run the 'save config' command and licenses are not present on the appliance, the appliance becomes unresponsive. Restart the appliance and load the licenses. Restart the appliance again for the changes to take effect. Then run the 'save config' command.

Networking

- Issue ID 0321868: BGP does not advertise default route to the peer, with default-originate flag, if the state of a learnt default route toggles.
- Issue ID 0324432: The NetScaler appliance forwards (L3 mode) certain response packets with IP header checksum value 0xFFFF, which is an invalid value according to RFC 1624. As a result, the router drops these packets.
- Issue ID 0330118: OSPF maximum age link-state advertisements (LSAs) are not removed from the NetScaler appliance because the maximum age walker processes suspended indefinitely.
- Issue ID 0330165: After upgrading the Netscaler appliance to 10.69.4 build, the appliance does not learn a ARP entry from a ARP reply packet, if the MAC addresses in the Ethernet header (Source MAC) and ARP header(Sender MAC) of the ARP reply packet are different.

Platform

- Issue ID 0276184: NetScaler release 10 build 70.x is supported on the new MPX 8200/8400/8600 platform.

Policy

- Issue ID 0291487: NetScaler appliances running version 9.2 build 52.1 or later and have a large number (in the hundreds) of policy bindings can experience performance issues on 'save ns config' and 'show config' operations. This can lead to interruption in services.
- Issue ID 0322964: Removed the 'unset audit syslogPolicy' and 'unset audit nslogPolicy' commands from NetScaler release 10 build 70 onwards.
- Issue ID 0324700: Removed the 'unset filter policy' command from NetScaler release 10 build 70 onwards.

Responder

- Issue ID 0324200 (nCore): On a NetScaler appliance with the responder feature configured to redirect requests from authenticated members of a particular group to a custom web page, the redirections sometimes fail. The reason is that, when the responder feature is invoked before the AAA session is completely established (as is the case when a user selects a choice after initial logon), the user's AAA session is not transferred from one core to the other. Responder therefore fails to identify the user as a member of the targeted group.
- Issue ID 0330133: On a NetScaler appliance with the responder feature enabled and a respondWith response configured, if a user sends a request with a large Content-Length header, the NetScaler appliance might appear to hang. The cause of the apparent hang is that the NetScaler appliance expects a request of the specified Content-Length, and waits for the rest of the request before responding to it.

Rewrite

- Issue ID 0301481: On a NetScaler appliance that has a response-side rewrite policy configured and bound to a load balancing virtual server, a request sent to the virtual server might trigger a sequence of events that causes the NetScaler appliance to fail.

SSL

- Issue ID 0327173: The ciphers bound to an SSL virtual server are not displayed in the configuration utility.

System

- Issue ID 0271783: If you configure an RNAT rule and enable the TCP proxy option for RNAT, the NetScaler appliance functions as a proxy for internal clients and maintains separate client-side and server-side connections. In certain scenarios, this behavior might result in a service type mismatch between the client-side and server-side connections, and the appliance might reboot with a core dump.

- Issue IDs 0306352 and 0332253: When using the configuration utility or SSH to log on to the appliance, the "Connection limit to CFE exceeded" message might be displayed. This message is displayed if an earlier session was closed without logging out of the session.

- Issue ID 0306660 (nCore): You can now use the 'set ns tcpparam connFlushIfNoMem <connFlushIfNoMem>' command on a NetScaler appliance to close existing connections if memory is not available for a new connection. When using this command, you must specify the type of connection to be closed. By default, this feature is disabled on the appliance.

- Issue IDs 0312893 and 0331073: When you run the 'show run' command, the NetScaler appliance might fail even if the you have permission to run the command.

- Issue ID 0325665: An unrelated error code is displayed on executing the ‘set filter prebodyinjection/postbodyinjection’ commands.

- Issue ID 0323190: In rare cases, the NetScaler appliance fails when some pages are recovered from the free queue before the page table scan is complete.

- Issue ID 0327118: In the configuration utility, the minimum and maximum values allowed for number of audit messages is incorrect. The maximum and minimum values displayed are 255 and 0, but the correct values are 256 and 1.

- Issue ID 0330336 (nCore): IPv6 addresses might occasionally be captured in the audit log, even though IPv6 addresses are not configured.

Web Interface

- Issue ID 0306731: If the Rewrite feature is not enabled, the Enable access through receiver client option for a Web Interface(WI) site does not work. This is because the functionality of the option depends on some rewrite policies on the appliance.

- Issue ID 0315502: The Configuration Utility displays an error message when you try to disable the Web Interface feature.

- Issue ID 0315951: If the Responder feature is not enabled, the Make Site Path Case Insensitive option for a Web Interface(WI) site does not work. This is because the functionality of the option depends on some Responder polies on the appliance.

- Issue ID 0324373: In the Web Interface (WI) configuration wizard, for a WI site in gateway direct mode, the state of the Enable Access through Receiver Client option is shown selected even when there are no rewrite policies bound to the selected Access Gateway virtual server.

- Issue ID 0331904: In the Web Interface (WI) configuration wizard, the Enable Access through Receiver Client option remain selected even when you try to clear the option.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberoes authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, adn then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.

- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

- Issue ID 0327446: On an Outlook for Web Access (OWA) 2010 server that is protected by AAA-TM with single sign-on (SSO) enabled, when a user who uses the Firefox or Chrome browsers logs off, some OWA 2010 images do not appear.

- Issue ID 0334363: In the Citrix NetScaler configuration utility, when a user clicks the AAA-Application Traffic Wizard link, the configuration utility displays error message of 'Unknown Error'. The browser is then frozen til the session times out.

Access Gateway

- Issue ID 0249975: When users log on with the Access Gateway Plug-in, the 'File Transfer' tab on the Access Interface is available, but the 'File Transfer option' is not available if users right-click the Access Gateway icon in the notification area.

- Issue ID 92543/0251596: After you configure Access Gateway to provide user connections through Citrix Receiver, when users right-click the Receiver icon in the notification area, the Log on option does not appear. Users must connect by using the Web browser or they must right-click the Receiver icon and then, depending on the version of Receiver they are using, click About or Preferences from the Receiver menu and Plug-in Status or Advanced from the Receiver panel. You can also enable the log on option to appear when users right-click the Receiver icon by adding the following settings in the registry:

  - Add the Receiver key (if the key does not already exist) under the following registry locations:

    - `HKEY_CURRENT_USER\Software\Citrix\`

    - `HKEY_LOCAL_MACHINE\Software\Citrix\`
  - Add the Inventory key in the following registry locations:

    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`

    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`
  - In the Inventory key, configure the following **REG_SZ** values:

    - **VPNAddress**. Provide the value as the Web address for the Access Gateway appliance; for example, https://<AccessGatewayFQDN>.

    - **VPNPrompt1**. Provide the value as 'UserName'.

    - **VPNPrompt2**. Provide the value as '*Password'.

      Note: To mask the password, enter an asterisk (*) before the word.

      In addition, if you configure double-source authentication that requires authentication with LDAP plus RSA authentication, you need to also add the following as **REG_SZ**:

    - **VPNPrompt3**. Provide the value as '*Passcode'.
- Issue ID 0261547: When you enable Access Gateway as a reverse proxy and you enable basic preauthentication and post- authentication scans, as well as encryption and client choices, when users log on with the Access Gateway Plug-in, the preauthentication scan passes, but the post-authentication scan fails.

- Issue ID 0275079: When users access applications published on XenApp, each user consumes multiple Access Gateway licenses per application. Instead, one session ID should be shared across the applications the user accesses. As a result, users exceed their allocated license count and an SSL error occurs.

- Issue ID 0278218: If you configure an endpoint policy, the preauthentication policy runs as expected. When users try to log on with the Access Gateway Plug-in, however, occasionally the post-authentication policy does not work as expected and

authentication fails.

- Issue ID 0285995: If you configure Access Gateway to assign an intranet IP address to user devices that connect to Access Gateway, when users log on with the Access Gateway Plug-in, the secure DNS dynamic update does not occur and the intranet IP address is not registered with the DNS Server.

- Issue ID 0288469: After you configure a virtual server to use the Access Gateway Plug-in for Java, when users log on with the Access Gateway Plug-in by using a browser that has a 64-bit Java Runtime Environment (JRE) installed, the plug-in fails to establish a connection.

- Issue ID 0291264: If you create a Web Interface 5.4 site and enable authentication through Access Gateway, and you enable single sign-on with a smart card to the Web Interface that enables smart card pass-through, when users log on with the Access Gateway Plug-in, the users' desktops are not listed on the Web Interface.

- Issue ID 0291821: If you create a Web Interface 5.4 site and enable authentication with a smart card through Access Gateway, and you configure the 'Single Sign-on Domain' on the 'Published Applications' tab using the format domainname.com instead of domainname, when users start a published application or desktop, authentication fails.

- Issue ID 0292005: When users connect with clientless access and try to download a file larger than 1 gigabyte (GB) from the file share on the home page, as the file is downloading, if an upload is attempted, the download process fails but the upload continues.

- Issue ID 0298971: When users log on with the Access Gateway Plug-in for Java and the Web Interface opens in Internet Explorer 9, if users do not turn on Compatibility View in Internet Explorer, when they click a published application, the following error appears: Resource shortcuts are not available.

- Issue ID 0299515: If you configure an intranet IP address on Access Gateway, when users connect with the Access Gateway Plug-in on a computer running Windows XP Service Pack 3 and try to access a CIFS share hosted on a computer in the secure network, users receive an error that the share is inaccessible.

- Issue ID 0300511: When users log on using clientless access and click a bookmark from the home page to open a Distributed File Share (DFS), if the target folder resides on a different computer than the computer where the domain DFS server resides, the share does not open.

- Issue ID 0309017: When you configure a preauthentication and post-authentication policy with an expression to scan a user device for a file, Access Gateway does not check for expression syntax. As a result, Access Gateway accepts inappropriate syntax configuration and the scan fails.

- Issue ID 0319607: If an authentication server and Access Gateway reside in the same domain, the appliance may fail.

- Issue ID 0327433: If you configure a virtual server by using the Remote Access wizard and configure a Secure Ticket Authority (STA), the status of the server appears as UP. However, in the configuration utility, on the Home tab, under Alerts, a message states that the STA server is not configured. You must bind the server globally in order to clear the message.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

AppFlow

- Issue ID 0333560 (nCore): AppFlow records generated by the NetScaler appliance might contain junk characters.

Application Firewall

- Issue ID 0282932: If you use the Signature Editor to add a signature rule for a response-side check (such as the Credit Card or Safe Object check), in addition to one or more response patterns you must also add at least one request pattern. If you do not, then when you try to save the new signature rule, the configuration utility displays an error message and does not save the rule.

- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked. To work around this issue, if you configure Sessionless URL Closure, set Validate Referer Header to Off.

- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported for importing as application firewall signature rules. WAS 2.0 scan reports are not supported.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

CloudBridge

- Issue ID 0334949: If you use configuration utility to remove an IPv4 tunnel for CloudBridge from a NetScaler appliance, the remove process succeeds but the following Java exception is displayed: 'ClassNotFoundException'.

Cluster

- Issue ID 0332594: The RIP (Routing Information Protocol) and Cache Redirection features cannot be enabled in a NetScaler cluster setup.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278002: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

- Issue ID 0278097: In the configuration utility, if you click Application Firewall in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0307039: The expression builder dialog does not show the possible functions in the following scenarios:

  - When '.' is entered after the (<expression>)

  - When '.' is entered in the expression which is used as function parameter.
- Issue ID 0319070: The Setup wizard is not launched automatically if a mapped IP (MIP) address or a Subnet IP (SNIP) address is not configured on the NetScaler appliance.

- Issue ID 0323172: The NetScaler configuration utility cannot group the neighbors according to the cluster node to which they belong. This issue is observed only in a cluster setup.

  Workaround: You must use the 'show nd6' command to view the neighbors node-wise.

- Issue ID 0323213: In a cluster setup, globally bound DNS policies are listed multiple times in the Bind/Unbind DNS Policy(s) to Global dialog box.

- Issue ID 0324797: The NetScaler configuration utility does not display the queue depth value for the configured priority queuing policies. This issue is observed only in a cluster setup.

  Workaround: You can view the queue depth of the policy by using the 'show pq policy' command on the command line interface.

- Issue ID 0332839: If you access the configuration utility through Internet Explorer 8, the 'System' > 'Settings' > 'Configure TCP Parameters,' dialog box has no spaces between field names and fields.

- Issue ID 0333048: Using the Configuration Utility in Internet Explorer version 8, when you attempt to bind 250 or more VIP addresses to a VLAN, the Configuration Utility displays an unresponsive script error.

- Issue ID 0333834: If the PDF reader plug-in is not set in your browser and you try to open an HTML document from the Downloads tab of the NetScaler configuration utility, you are prompted to open the document in Adobe Reader.

- Issue ID 0333836: If you have configured global server load balancing by using the GSLB wizard, Wizard for Citrix XenApp, or Wizard for Citrix XenDesktop, and you attempt to

view the GSLB Visualizer, Prefuse information might be logged to the Java console. However, you can view the GSLB Visualizer, and the functionality is not affected.

- Issue ID 0334042: The configuration utility does not display a details panel for all the entities.

  Workaround: Select the entity and click 'Open' to display the details.

- Issue ID 0333745: When you access the NetScaler configuration utility from a Mac machine, the keyboard short cut keys may be unresponsive. In the NetScaler configuration utility, short cut keys work differently in Java and HTML views. For example, in Java based views, short cut keys for the copy-paste functions are <CRTL C> and <CRTL V> and in HTML based views they are <CMD C> and <CMD V>.

  Workaround: Use the <CRTL key> short cut keys if the <CMD key> short cut keys are not working and vice-versa. For example, if <CRTL C> shortcut key is not working, use <CMD C> and vice-versa.

- Issue ID 0334280: After you rename a compression policy, the new name might not be reflected in the configuration utility.

  Workaround: Refresh the page to see the renamed policy.

- Issue ID 0334284: If you navigate to HTTP Compression > Policies and click 'Policy Manager' in the task pane, the following error message might appear: No such policy exists.

  Workaround: Refresh the page and try again.

- Issue ID 0334292: If you navigate to HTTP Compression > Policies or HTTP Compression > Actions, the Remove button is disabled in the task pane.

  Workaround: Use the command line interface to remove the policy or action.

  Note: You can access the command line interface from the configuration utility. Navigate to System > Diagnostics > Command Line interface.

- Issue ID 0334773: In the Synchronize GSLB Configuration dialog box, the Command parameter is unavailable when the Synchronization Option parameter is set to its default value (automatic synchronization).

- Issue ID 0335008: The exception 'netscape.javascript.JSException' is logged to the Java console when you create a DNS key by using the NetScaler configuration utility. However, the DNS key is created, and there is no loss in functionality.

- Issue ID 0335013: If no services are configured for a DNS view, and you use Windows Internet Explorer 9 to view the Create DNS View dialog box, the 'Service(s) in this view' and 'Policy(s) in this view' lists in the dialog box are not rendered correctly. The display issue is resolved if at least one service is configured for the DNS view.

- Issue ID 0335235: The NetScaler configuration utility does not show globally bound AppFlow policies in the policy manager. This issue is observed only in a cluster setup.

- Issue ID 0335701: You cannot add an SSL service with the Clear Text Port option in the configuration utility, because the option is disabled.

- Issue ID 0335719: The exception “netscape.javascript.JSException” is logged to the Java console when you sign a DNS zone by using the NetScaler configuration utility, and the browser’s status bar does not report the status of the zone-signing operation. However, the zone is signed, and there is no loss in functionality.

- Issue ID 0333577: When configuring the Transformation URL Profile, an error occurs if you set Priority to a value higher than 2147483647 (maximum allowed value).

- Issue ID 0335526: If you access the configuration utility through an Internet Explorer browser that has the Java Runtime Environment (JRE) disabled, an error occurs.

  Workaround: Make sure that at least one JRE is present and enabled under the Java Runtime Environment Settings, in the Java console, on the Java tab.

- Issue ID 0335913: In a cluster setup, you cannot enable a server entry that is disabled, because the Enable button is unavailable. However, you can disable a server entry by using the NetScaler command line interface.

- Issue ID 0338513: When you log on to NetScaler configuration utility from Internet Explorer 8 or Internet Explorer 9, the web browser displays a blank screen as the browser is displaying the compatibility view.

  Workaround: Change to the standard view, in the 'Compatibility View Settings' dialog box, by clearing the 'Display all websites in Compatibility View' check box.

- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated.

Domain Name System

- Issue IDs 0268748 and 0333310: In a cluster setup, if you save the configuration and reboot an appliance, the default name-server records for the thirteen root servers, and their associated address records, become unavailable. If you need them, you have to add them manually after you perform a reboot.

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

- Issue ID 0330529: The following message might be displayed if you disable a virtual server-based DNS name server: 'ERROR: Name server does not exist. [nsnet_recvrpcioctl]'

Global Server Load Balancing

- Issue ID 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0291053: The NetScaler appliance does not rewrite responses that are DNSSEC-enabled and/or sent over TCP. So, when a security-aware DNS server sends the NetScaler appliance a DNSSEC-enabled NXDOMAIN response, or when a DNS server sends the appliance an NXDOMAIN response over TCP, the appliance relays the negative response to the client and caches the negative response. For subsequent requests for the same non-existent domain, the appliance responds with the cached, DNSSEC-enabled response, even if the clients are security-oblivious or use UDP. This behavior is expected, and ensures that all clients receive the same response.

- Issue ID 0326001: If a GSLB virtual server’s primary GSLB method is set to round trip time (RTT) and backup GSLB method is set to static proximity, or if the primary GSLB method is set to static proximity and backup GSLB method is set to RTT, and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT as the primary GSLB method, do not use static proximity as the backup GSLB method. Similarly, if you use static proximity as the primary GSLB method, do not use RTT as the backup GSLB method.

Load Balancing

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the 'show lb persistentSessions' CLI command displays an internal representation of thepersistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 91711/0250846: If the string (or 'token') that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR('string2').AFTER_STR('string1') if the string that is enclosed by 'string1' and 'string2' is not larger than 64 KB.

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

- Issue ID 0318310: While creating a load balancing monitor, you cannot specify a send string that has a length of more than 76 characters. This issue is observed only in a cluster setup.

- Issue ID 0331621: While creating SSL or load balancing virtual servers with default responder action, the NetScaler appliance throws a 'No such resource' error. This issue is observed only in a cluster setup.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type : #/etc/rc.d/svmd restart

- Issue ID 0337386: When restored from a backup, a NetScaler instance reverts to the release and build in which it was originally provisioned, even if the backup was taken from an upgraded configuration.

NetScaler VPX Appliance

- Issue ID 0326388: In sparse traffic conditions on a NetScaler VPX virtual appliance installed on VMware ESX, some latency might be observed in releases after 9.3 as compared to release 9.2. If this latency is not acceptable, you can change a setting on the appliance. At the shell prompt, type:

  sysctl netscaler.ns_vpx_halt_method=2

  Perform a warm reboot for the above change to take effect. To have the new setting automatically applied every time the virtual appliance starts, add the following command to the /nsconfig/nsbefore.sh file:

  sysctl netscaler.ns_vpx_halt_method=2

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.

- Issue ID 0283035 and 0299716: In a cluster setup, the 'bind vlan' command throws an error when interface and IP address are specified together.

- Issue ID 0288450: The 'show lacp' command does not display the lacp configurations. This issue is observed only in a cluster setup.

- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command 'set ptp -state disable' and configure NTP to synchronize the time across the cluster nodes.

  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.

- Issue ID 0283661: In a cluster setup, if you add an SSL certificate on the configuration coordinator, and immediately execute the add certkey command, the command succeeds on the configuration coordinator but might fail on the other cluster nodes if the certificates on the configuration coordinator are not synchronized with the other cluster nodes before the command is executed.

  Workaround: Copy the certkey under /nsconfig/ssl/ folder on all the cluster nodes or confirm that the certificates are synchronized before executing the add certkey command on the configuration coordinator.

System

- Issue ID 0338244: The CallHome feature checks for compact flash drive and hard disk drive errors every six minutes instead of every six hours. If any errors are found, the appliance's data is uploaded to the Citrix Technical Support server.

Build 69.4

Release version: Citrix® NetScaler®, version 10 build 69.4

Replaces build: None

Release date: August 2012

Release notes version: 3.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Changes
- Bug Fixes
- Known Issues and Workarounds

Note: Unless stated otherwise, an issue applies to all build types (nCore and nCore VPX) of Citrix NetScaler and Citrix Access Gateway.

Enhancements

Smart Card Authentication for Web Interface Site using Access Gateway (Issue ID 0287639)

The NetScaler appliance now supports smart card authentication for web interface on NetScaler through Access Gateway. On using this enhancement, you can configure a web interface site that can be accessed by logging into an Access Gateway virtual server by using a smart card. To use this enhancement, you must upgrade the NetScaler to the latest build and install the new web interface tar file 'nswi-1.5.tgz'. For more information, see the 'Using Smart Card Authentication for Web Interface on NetScaler' topic in the 'Web Interface' chapter of the *Citrix NetScaler Administration Guide*.

Automatically Populating the Default Value of a Virtual Server on a Web Interface Site (Issue ID 0300470)

While modifying a web interface site configured in Direct mode, the default value for the virtual server is now automatically populated with one of the load balancing virtual servers configured during the creation of the web interface site.

Case Sensitivity on the Web Interface Wizard (Issue ID 0246466)

An option 'Make Site Path Case Insensitive' on the web interface wizard has been introduced. When you enable this option, the NetScaler appliance ignores case sensitivity in the site name part of the URL request for a web interface site configured on the NetScaler appliance.

Multiple Binding of Content Switching PI Policies to Content Switching Virtual Servers and Policy-labels (Issue ID 67323/0230903)

The multiple policy binding feature enables you to bind a policy to multiple virtual servers or policy labels. Earlier, you could bind a policy only to a single virtual server or policy label and to reuse an existing policy, you needed to create a copy of the same policy with a different name before attaching it to another virtual server. With the multiple policy binding feature, you can reuse an existing policy for multiple virtual servers.

Global State Update Option for Content Switching (Issue ID 0274449)

You can now enable the state update option globally for content switching virtual servers configured on the NetScaler appliance. If a specific virtual server's local state update option is set to DISABLED, that setting is overridden by a global ENABLED setting. However, a local setting of ENABLED overrides a global setting of DISABLED for the state update option. As shown in the following table, state update is not disabled for a virtual server unless both the global and local options are set to DISABLED.

Global state update setting	Virtual server state update setting	Effective state update setting on the virtual server
ENABLED	ENABLED	Enabled
ENABLED	DISABLED	Enabled
DISABLED	ENABLED	Enabled
DISABLED	DISABLED	Disabled

To configure the state update option globally by using the NetScaler command line, at the NetScaler command prompt, type the following command:

```
set cs parameter [-stateupdate ( ENABLED | DISABLED )]
```

To configure the state update option globally by using the NetScaler configuration utility

1. In the navigation pane, click 'Content Switching'.
2. In the details pane, click 'Configure Content Switching parameter'.
3. In the 'Set Content Switching Parameters' dialog box, select the 'State Update' check box.
4. Click 'OK'.

Support for Load Balancing Diameter Traffic (Issue ID 86737/0246690)

You can now load balance Diameter traffic. The Diameter protocol is a next generation Authentication, Authorization, and Accounting (AAA) signaling protocol mainly used on mobile devices such as laptops and mobile phones. It is a peer-to-peer protocol as opposed to the traditional client-server model that is used by most other protocols. For more information, see the 'Configuring Diameter Load Balancing' topic in the Load Balancing' chapter of the *Citrix NetScaler Traffic Management Guide*.

Stateless Connection Failover Supported for IPv6 (Issue ID 0276300)

You can now bind an IPv6 service to a load balancing virtual server with connection failover set to stateless.

Options for Branch IP Address in the Load Balancing wizard for Branch Repeater (Issue ID 0275289)

In the 'Load Balancing wizard for Branch Repeater', when specifying a branch whose traffic is to be accelerated, you can specify either the primary IP address or the accelerated pair A (apA) IP address of a Branch Repeater appliance.

NetScaler SDX - System Health Monitoring (Issue ID 0291018)

A supplemental software pack supports system health monitoring on the NetScaler SDX appliance for hardware and software components, disks, fan, voltage, temperature, and power supply sensors, and interfaces. For more information about this enhancement, see the 'System Health Monitoring' chapter in the *Citrix NetScaler SDX Administration Guide*. To install the supplemental software pack, see http://support.citrix.com/article/ctx132877.

New Health Monitoring Gadget on the NetScaler SDX Appliance (Issue ID 0313835)

You can now view the top 25 critical health monitoring events in the Health Monitoring gadget on the Home tab in the Management Service user interface. Select an event to view details or to delete the event.

Session Management for Communication with NetScaler Instances (Issue ID 0287133)

All HTTP and HTTPS communication between the Management Service and a NetScaler VPX Instance is now through a persistent session. A session ID is associated with each VPX instance and all HTTP and HTTPS communication between the Management Service and the instance uses this session ID.

Session Management for Communication with XenServer (Issue ID 0303527)

With XenServer version 6.0 and later, HTTP communication between the Management Service and XenServer is now over a persistent session. All HTTP communication between the Management Service and XenServer uses one session ID. For earlier versions of XenServer, basic authentication (user name and password) is used.

SNMP Support on the NetScaler SDX Appliance (Issue ID 94071/0257902)

You can now configure a Simple Network Management Protocol (SNMP) agent on the Citrix NetScaler SDX appliance to generate asynchronous events, which are called traps. For more information about this enhancement, see the 'SNMP' chapter in the *Citrix NetScaler SDX Administration Guide*.

Installing a Supplemental Pack for XenServer (Issue ID 0303515)

You can now install the NetScaler SDX supplemental packs from the Management Service without manually opening an ssh connection to XenServer. To install this pack, on the configuration tab, in the navigation pane, expand Management Service, and then click XenServer Files. In the details pane, click 'Supplemental Packs'. You can upload the supplemental pack to the SDX appliance and also download it to create a backup on your client.

Change Management on the NetScaler SDX Appliance (Issue ID 0291024)

You can now track any changes to the configuration on a NetScaler VPX instance from the Management Service. To view these changes, on the configuration tab, in the navigation pane, expand NetScaler, and then click Change Management. The details pane lists the device name with IP address, date and time when it was last updated, and whether there is a difference between the saved configuration and running configuration. Select a device to view its running configuration, saved configuration, revision history of configuration changes, and difference between the configuration before and after an upgrade. You can download the configuration of a NetScaler VPX instance to your client. By default, the Management Service polls all the instances every 24 hours but you can change this interval by clicking Configure Poll Interval in the details pane.

Configuring Tagged VLANs on the NetScaler SDX Appliance (Issue IDs 0278369 and 0284146)

You can now configure a tagged VLAN, without configuring an NSVLAN, at the time of provisioning a NetScaler instance. For more information about this enhancement, see the 'Provisioning NetScaler Instances' chapter in the *Citrix NetScaler SDX Administration Guide*.

Cloud Bridge CLI Commands Simplified (Issue ID 0307496)

Simplified the Cloud Bridge CLI commands for configuring IPSec Tunnel.

Filtering out Connection Table using CSW/LB vserver Policy Expressions (Issue ID 0302889)

Added policy expressions for the 'show connectiontable' command to filter out connections of a specific content switching or load balancing virtual server.

For example: `show connectiontable CONNECTION.LB_VSERVER.NAME.EQ("v1")`

Configuration Utility Simplified (Issue ID 0306109)

Simplified the configuration utility to ease the process to connect to the cloud service providers.

Application Firewall - Learning from Trusted Clients/Networks Only (Issue ID 86758/0246711)

You can now configure the application firewall learning feature to learn from trusted clients or networks only, instead of learning from all traffic that it processes. By restricting learning to trusted clients, you can prevent attacks against your protected web sites and web services from being learned as normal use and therefore not blocked. Currently trusted learning can be configured only from the NetScaler command line.

To configure the application firewall to learn from trusted clients or networks only, first enable the trusted learning feature. Next, add your trusted clients and networks. To add a trusted client, add the client's IP. IPv4 and IPv6 IPs are both supported. You can use a prefix of /0 after the IP, but that is not necessary. To add a trusted network, add the network in CIDR format.

To enable and configure trusted learning, at the NetScaler command line type the following commands:

set appfw profile <profileName> -enabletrustedLearning (on|off)
bind appfw profile <profileName> -trustedLearningClients (<ip_addr>|<ipv6_addr>|<cidr/prefix>) -state (ena

For <profileName>, substitute the name of the application firewall profile that you want to associate with these trusted learning settings. If you want to add a trusted client or network to the configuration but not configure the application firewall to learn from it yet, set state to disabled. You can add an optional comment to document which client or network you added and why.

The following commands enable trusted learning, add a trusted client at 10.178.16.34, and add a trusted network at 10.102.30.0/24.

set appfw profile TestProfile -enabletrustedLearning on
bind appfw profile TestProfile -trustedLearningClients 10.178.16.34 -state enabled -comment "Trusted client
bind appfw profile TestProfile - trustedLearningClients 10.102.30.0/24 -state enabled -comment "Trusted ne

New TACACS+ Configuration Parameter (Issue ID 0257671)

If you configure a TACACS+ server for authentication, when users without the appropriate permissions enter a command, the command does not execute, but the command is recorded in an accounting log. A new configuration parameter corrects this behavior.

New Syntax for Binding Content Switching Policies and Load Balancing Virtual Servers to a Content Switching Virtual Server (Issue ID 0291791)

For the 'bind cs vserver command', the 'targetVserver' parameter is now deprecated. If you attempt to set the parameter, the following warning appears: “Warning: Argument deprecated [targetVserver].”

This release introduces the 'lbvserver' parameter, for binding the default load balancing virtual server to the content switching virtual server, and the 'targetLBVserver' parameter, for binding other load balancing virtual servers through content switching policies.

In the NetScaler configuration utility, there are no changes in how you bind a default load balancing virtual server or a load balancing virtual server that is not the default.

To specify a default load balancing virtual server by using the NetScaler command line, at the NetScaler command prompt, type the following command:

```
bind cs vserver <csvservername> -lbvserver <targetVservername>
```

To specify a load balancing virtual server other than the default virtual server by using the NetScaler command line, at the NetScaler command prompt, type the following command:

```
bind cs vserver <csvservername> -policyName <policyname> [-priority <positive_integer>] -targetLBVserve
```

Application Firewall Profile Comment Support (Issue ID 0291927)

You can now add a comment to an archived application firewall profile to describe the contents and state of the archive more fully. The comment can be from 1 to 255 characters in length, and can contain letters, numbers, and most punctuation. In the configuration utility, you add a comment on the Export Application Firewall Profile dialog box, in the Comments text box. At the NetScaler command line, you add a comment by typing the following command:

archive appfw profile -comment "<string>"

For <string>, substitute the comment.

Rich policy support for SIP-UDP (Issue ID 0309107)

RULE based persistence now support SIP based policies as part of rule based persistence for SIP-UDP virtual servers. You can configure SIP based policies using the add lb vserver command. For example, the following code shows how to configure RULE based persistence for SIP-UDP virtual server:

add lb vserver sipvip1 SIP_UDP 10.102.27.68 5060 -persistenceType RULE -lbMethod CALLIDHASH -rule sip.re

Note: Only SIP request based policies are supported, rate limiting policies cannot be configured as part of the rule.

Option to Save the Config in Remote GSLB Sites after Config Synchronization (Issue ID 0287324)

The new Save Configuration option specifies that all participating nodes automatically save their configurations after synchronization. The master saves its configuration immediately before synchronization begins. Slave nodes save their configurations after the synchronization process is complete. A slave node saves its configuration only if it is successfully updated to match the master node's configuration. If synchronization fails on a slave node, you must manually investigate the cause of the failure and take corrective action.

To specify the option when using the NetScaler configuration utility to synchronize GSLB configurations, select the Save Configuration check box in the Save GSLB Configuration dialog box. If using the CLI, specify the saveConfig option for the sync gslb config command. The saveConfig option is mutually exclusive with the command's preview option.

SAML IDP and SP-Initiated Logouts Support for AAA-TM (Issue ID 0286268)

Support for SAML IDP- and SP-initiated logouts has been added to AAA-TM. An SP-initiated logout is performed when a user logs out of a AAA-TM session, but not when a user's AAA-TM session times out or when the 'kill aaa sessions' command is used. An IDP-initiated logout is performed when the IDP sends a 'clear session' request to the NetScaler appliance.

Searching NetScaler Entities in the Configuration Utility

You can use the 'Search' functionality to search for NetScaler entities displayed in the details or the data pane of the NetScaler configuration utility. If you want to perform string matching operations that are more complex than the operations that you perform with the simple CONTAINS search, you can use regular expressions.

Support for AES Ciphers on SSLv3 (Issue ID 0302510)

The following AES ciphers are now supported on the SSLv3 protocol.

1. Cipher Name: TLS1-AES-256-CBC-SHA

   Description: TLSv1 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1

2. Cipher Name: TLS1-AES-128-CBC-SHA

   Description: TLSv1 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1

3. Cipher Name: TLS1-DHE-DSS-AES-256-CBC-SHA

   Description: TLSv1 Kx=DH Au=DSS Enc=AES(256) Mac=SHA1

4. Cipher Name: TLS1-DHE-DSS-AES-128-CBC-SHA

   Description: TLSv1 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1

5. Cipher Name: TLS1-DHE-RSA-AES-256-CBC-SHA

   Description: TLSv1 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1

6. Cipher Name: TLS1-DHE-RSA-AES-128-CBC-SHA

   Description: TLSv1 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1

7. Cipher Name: TLS1-ADH-AES-128-CBC-SHA

   Description: TLSv1 Kx=DH Au=None Enc=AES(128) Mac=SHA1

8. Cipher Name: TLS1-ADH-AES-256-CBC-SHA

Description: TLSv1 Kx=DH Au=None Enc=AES(256) Mac=SHA1

Changes

Compression

- Issue ID 0299887: The output of the 'show cmp global' command is now similar to the output of the 'show' commands that you use for viewing global bindings for other types of default syntax policies. The 'show cmp global' command continues to display all the globally bound classic policies along with their priority values. But, for default syntax policies, the command displays only those global bind points to which policies are bound, along with a count of the number of policies that are bound to each of them.

  To view the details for a given global bind point, you can specify the bind point as the argument to the 'type' parameter. When you specify a global bind point, the command displays all the policies that are bound to the bind point, along with their priorities and Goto expressions. Classic policy bindings are not displayed if you specify a global bind point.

  Example:

  ```
  > sh cmp global -type RES_DEFAULT
  ```

  Advanced Policies:

  1. Policy Name: ns_adv_nocmp_xml_ie

     Priority: 8700

     GotoPriorityExpression:END

  2. Policy Name: ns_adv_nocmp_mozilla_47

     Priority: 8800

     GotoPriorityExpression: END

  3. . . .

     Done

     >

Load Balancing

- Issue ID 0302112: The use of SIP rate limiting expressions for rewrite policies is disabled to prevent the NetScaler from becoming unavailable.

SSL

- Issue ID 0316577: The SSL crypto card instrumentation is enhanced to provide more information on error status during initialization and at runtime.
- Issue ID 0325800: There are changes to the 'add ssl cipher' and 'bind ssl cipher' commands in NetScaler release 10 build 69.4. Now, there are two commands to create a cipher group and bind ciphers to this cipher group. The command to bind an SSL cipher to a virtual server or service has also changed. For more information about these changes, see http://support.citrix.com/article/CTX134118.

XML API

- Issue ID 0299194: The following XML APIs related to ACL and PBR features are deprecated:
  - unsetnspbr6_icmptype
  - unsetnspbr6_nexthopval
  - setnspbr_state
  - setnsacl_state
  - setnspbr6_state
  - setnsacl6_state

Bug Fixes

AAA Application Traffic

- Issue ID 0288572: On a NetScaler appliance with AAA-TM enabled and Kerberos/NTLM authentication configured, Likewise support fails to start, and the following error message is displayed: /libexec/ld-elf.so.1: Shared object 'libkrb5support.so' not found, required by 'libgssapi_krb5.so'

- Issue ID 0307258: When you create a AAA-TM profile by using the configuration utility, the configuration utility displays the global persistency settings as the settings that it assigned to the profile. However, instead of actually deriving the persistency values from the global persistency settings, it sets persistency for the profile to zero (0). You can verify this issue by typing the following command at the NetScaler command line:

  show tm sessionaction <profileName>

  You can fix the persistency settings for any AAA-TM profile that is affected by this issue by typing the following command at the NetScaler command line:

  set tm sessionAction <profileName> -persistentCookie ENABLED -persistentCookieValidity <positive_integ

  For <positive_integer>, substitute the number of minutes that the persistency cookie is to remain valid. Then, use the 'show tm sessionaction' command to verify your changes.
- Issue ID 0313931: On a NetScaler appliance that has AAA-TM enabled, if a user takes more than four minutes to finish authenticating and the AAA session expires, the user is unable to authenticate. When the user clicks the 'click here' link to return to the logon page, instead of being redirected to the logon page, the user is redirected to the 'Expired Session' page repeatedly.

- Issue ID 0314561: On a NetScaler appliance with AAA-TM enabled and single sign-on (SSO) configured, if a user who uses the Google Chrome browser takes more than four minutes to authenticate and the session expires, the browser displays a blank page instead of the Session Expired page.

- Issue ID 0322445: On a NetScaler appliance that has AAA-TM enabled and a load balancing virtual server configured to support 401 basic authentication, if a user sends a GET request that does not contain a Host header, the NetScaler appliance crashes.

Access Gateway

- Issue ID 90726/0249979: If you configure client certificate-based expressions for preauthentication or post-authentication scans and if users log on with a client certificate on an nCore Access Gateway model MPX 7500 appliance or higher, the scan fails and users cannot log on. This issue does not occur on the MPX 5500 appliance.

- Issue ID 0289662: If you disable split tunneling, When users log on with the Access Gateway Plug-in and try to make a Voice over Internet Protocol (VoIP) call to a mobile phone by using Cisco Unified Personal Communicator application, the call does not connect.

- Issue ID 0289686: If users connect with the Access Gateway Plug-in for Mac and then log off from the Web Interface, if users log on again within five minutes, the connection fails. This only occurs if you enable ICA proxy in Access Gateway.

- Issue ID 0290220: When users log on to Access Gateway with the Access Gateway Plug-in for Mac OS X, the home page is slow to appear or does not appear in the Web browser.

- Issue ID 0290976: When you configure a post authentication policy on Access Gateway and configure the policy to redirect the connection to the Web Interface if the endpoint analysis fails, when users log on with the Access Gateway Plug-in, if the user device fails the endpoint analysis scan, users receive the Access Gateway logon page instead of the Web Interface.

- Issue ID 0299406: If you configure a policy to restrict access to certain files, when users log on with clientless access and try to access the file, Access Gateway fails.

- Issue ID 0300221: When users log on to an nCore Access Gateway model MPX 7500 or higher, if there is high memory usage, the Access Gateway might fail. This issue does not occur on the MPX 5500.

- Issue ID 0301060: When you configure address pools, enable intranet IP addresses, and disable spillover, when users log on with the Access Gateway Plug-in and then try to log on from a second user device, the Transfer Login page appears. However, the message appears incorrectly as text only on a blank page. When users click 'Cancel', the button is disabled, rather than redirecting users to the logon page again.

- Issue ID 0301338: If a user password is longer than 31 characters, when users try to log on through the 'Access Gateway Plug-in logon' dialog box rather than through a Web browser, logon fails. A message appears stating that the user name and password are invalid.

- Issue ID 0301557: If users connect with the Access Gateway Plug-in and two network adapters have active connections on the user device, DNS resolution does not occur and users cannot access internal resources. If users disable one network adapter, users can then access internal resources.

- Issue ID 0301799: Access Gateway might not release all user sessions, which results in maximum usage of the licenses. When this occurs, users cannot log on and you must restart Access Gateway.

- Issue ID 0302268: After the preauthentication scan passes and users log on, if an internal processing error occurs, Access Gateway fails.

- Issue ID 0302490: If users log on with Receiver for Chromebook through Access Gateway, when users log off, Access Gateway does not release the session. Users must close the Web browser to log on again.
- Issue ID 0303265: If servers in the internal network return a UDP packet with zero length, Access Gateway fails.
- Issue ID 0306346: When users log on to the configuration utility, the following issues occur:
  - When using an Internet Explorer 8 Web browser, a blank page appears.
  - When using a Firefox 11 Web browser, many features in the navigation tree do not appear.
  - When using a Google Chrome Web browser, the only features that appear in the navigation tree are System, Network, DNS, SSL, VPN, and AppExpert.
- Issue ID 0320493: If your authentication policies include the rules REQ.SSL.CLIENT.CERT.EXISTS and REQ.SSL.CLIENT.CERT.NOTEXISTS, and users log on with a smart card, the following might occur:
  - If smart card authentication fails, users are redirected to the Web Interface and prompted again for the smart card credentials.
  - If users do not enter smart card credentials, they are redirected to the Web Interface and prompted for their user name and password in order to authenticate with RADIUS.

AppFlow

- IssueID 0301461 (nCore): If you enable the 'clientTrafficOnly' parameter when the AppFlow feature is enabled, the NetScaler appliance fails. By default, the 'clienttrafficonly' parameter is disabled.
- Issue ID 0302578 (nCore): If you enable AppFlow when the NetScaler device is in transparent mode, or when the load balancing virtual servers use wildcards for the IP address and port to dynamically learn the backend services, the NetScaler device fails.

Application Firewall

- Issue ID 51944/0219171: Imported application firewall objects -- such as WSDLs and XML Schemas -- cannot be removed from the NetScaler appliance by using the 'clear config' command. You must explicitly remove these objects. To remove an imported object by using the NetScaler command line, open a Unix shell and type 'rm <objectFilename>'. To remove an imported object by using the configuration utility, select the object, and then click Remove.

- Issue ID 85151/0245424: You can now add a comment to an application firewall profile to describe it more fully. The comment can be from 1 to 255 characters in length, and can contain letters, numbers, and most punctuation. In the configuration utility, you add a comment on the Create Application Firewall Profile dialog box or Configure Application Firewall Profile dialog box, General tab, in the Comments text box. At the NetScaler command line, you add a comment by typing the following command:

  ```
  set appfw profile -comment "<string>"
  ```

  For <string>, substitute the comment.

- Issue ID 87741/0247559: Handling of half-width and double-width characters by the HTML SQL Injection check transformation feature has been modified to ensure that these characters are identified as special characters, preventing inappropriate blocking and transformation.

- Issue ID 0284784: When a web site sends a MIME-encoded web form to a user with the MIME boundary enclosed in double quotations, and the user returns the web form as a POST request, the application firewall resets the connection with a reset code of 9845.

- Issue ID 0291389: When you configure an audit policy to send the application firewall logs to a remote Syslog server, the logs do not contain the profile name and URL of the connection that generated the log, and field names and values are incorrect. If you configure the audit policy to create local logs, the missing information is included in the logs.

- Issue ID 0300223: In the configuration utility, 'Application Firewall Profiles' pane, when you import a profile, the configuration utility is not automatically refreshed, giving the impression that the import failed. The profile is actually imported successfully. To see it in the Profiles list, click 'Refresh'.

- Issue ID 0300383: On a NetScaler classic build that has the application firewall learning feature enabled, under heavy load the configuration utility can become unavailable and the NetScaler can freeze or hang.

- Issue ID 0300465: When upgrading from the NetScaler 9.3 to the NetScaler 10 release, all signature rules, SQL special strings, and SQL keywords are now automatically upgraded to the new schema.

- Issue IDs 0301817 and 0302295: Local safe object signature rules work only if the Location is set to HTTP_RESP_BODY, and maxLength is defined.

- Issue ID 0302282: If a local safe object signature rule is defined, and the signatures object is bound to a profile, the safe object check is not run on traffic that is processed through that profile.

- Issue ID 0302368: In the 'Manage Learned Rules' dialog box, you might not be able to deploy or remove certain learned relaxations that contain special characters.
- Issue ID 0303057: If a log for a Transform action has missing parameters, the fields that contain those parameters are not clickable in the Syslog Viewer, and that log cannot be deployed to create a new rule or relaxation.
- Issue ID 0307082: When the NetScaler appliance sends an HTTP/1.0 100-Continue response on behalf of a protected web server, it now also sets the TCP Push flag in the response packet. This change resolves certain performance issues that might have been encountered when enabling the application firewall for some XML-based web services.
- Issue ID 0307542: If a hostname greater than 93 characters in length is assigned to a NetScaler appliance that has the application firewall enabled, the application firewall learning feature crashes.
- Issue ID 0309289: When a client sends a chunked POST request to an application firewall-protected web server, the request might not be correctly transmitted to the web server, resulting in a failed connection.
- Issue ID 0319787: On a NetScaler appliance with the application firewall feature enabled, the comment stripping feature does not correctly parse web pages that have an HTML comment that is terminated with two hyphens, a space, two more hyphens, and a greater-than symbol (-- -->). In other words, you cannot have a string consisting of two hyphens and a space immediately preceding the usual comment termination string (-->). If you do, the comment stripping feature does not detect the final two hyphens and greater-than symbol as a comment terminator. The comment stripping feature therefore strips all content that follows the missed comment terminator.
- Issue ID 0320145: If a user requests a URL from an application-firewall protected web site, and the requested web page has embedded URL links that contain hash (#) characters, the request might trigger a Start URL check violation. If blocking is enabled for the Start URL check, the request might be blocked.

Cluster

- Issue ID 0276162: Cluster commands are not propagated from the configuration coordinator to other nodes, when you log on to the cluster IP address using the Password Authentication mechanism. However, the commands are propagated when you log on to the cluster IP address using the Keyboard Interactive mechanism.
- Issue ID 0290504: You cannot form a cluster of NetScaler appliances by using the configuration utility, if you are accessing the configuration utility over a secure channel (https instead of http.)
- Issue ID 0302924: In the configuration utility, the NetScaler appliances that are added to the cluster by using the 'Discover NetScalers' option, are not automatically saved and rebooted.
- Issue ID 0318723: When a new node joins the cluster or an existing node is rebooted, the ACL, ACL6, SIMPLEACL, and SIMPLEACL6 configurations with TTL value are not automatically synchronized on that node.

Command Line Interface

- Issue ID 0262838: The CLI man page for the set dns parameter command has the following errors:
  - It displays 'ENABLED' as the default value for the 'cacheRecords' parameter. The possible values are only 'YES' and 'NO', and the default value is 'YES'.
  - It displays NS_FOUR as the default value for the 'resolutionOrder' order parameter. The possible values are only 'OnlyAQuery', 'OnlyAAAAQuery', 'AThenAAAAQuery', and 'AAAAThenAQuery'. The default value is 'OnlyAQuery'.

Configuration Utility

- Issues IDs 0244945, 0245825, and 0273344: When viewed in Internet Explorer version 8 or 9, the Dashboard page has several display issues (for example, excessive scroll bars, inconsistent column width, horizontal scroll bar missing from the Vserver view).
- Issue ID 0299883: When users access NetScaler using the configuration utility, the following issues are observed:
  - When you select a policy on the DNS Policies page, the Global Bindings button becomes inactive.
  - On the 'Virtual Servers' page, under 'Load Balancing', the header bar in the details pane moves off the page if you scroll down.
  - The configuration difference command produces an error message: Secondary NS not found.
- Issue ID 0300376: If you create an SSL service by modifying an existing virtual server and set some parameters in the 'Advanced' tab, the service is not created. The service is created if you do not set any advanced parameters or do not click the 'Advanced' tab.
- Issue ID 0302742: If you use the configuration utility to bind a compression policy (for example, app_cmp) to an AppExpert application, the following error message appears: Policy 'app_cmp' cannot be inserted. It does not have expression with advanced syntax.
- Issue ID 0303492: Creating an IP entity does not update the table that displays information about the configured IP addresses.
- Issue ID 0303494: Cache update causes issues with removal of an IP object.
- Issue ID 0303495: If you remove an IP object, cache-update issues cause Internet explorer to display unknown error.
- Issue ID 0303504: You cannot use the numeric keypad to specify values in the following text boxes:
  - Destination IP Address, in either the 'Create SNMP Trap Destinations' or the 'Configure Trap Destinations' dialog box.
  - IP Address, in the Create SNMP Managers dialog box.
- Issue ID 0303910: The Configuration page does not load if accessed from Internet Explorer 9 on a client machine running JRE 1.6 build 14.
- Issue ID 0308459: In 'Enable/disable service group member' view, the 'Enable' and 'Disable' buttons are inactive when the state of a service group member is one of the following - 'GOING OUT OF SERVICE', 'DOWN WHEN GOING OUT OF SERVICE' or 'GOING OUT OF SERVICE (graceful)'.
- Issue ID 0314258: When you modify any PBR rule from the configuration utility, the NetScaler appliance changes the APPLIED status of the PBR to NOTAPPLIED.
- Issue ID 0323197: An HTTP monitor with extended 'respCode' range cannot be configured through the configuration utility. If it is configured through the CLI, an error occurs when it is viewed in the configuration utility.

- Issue ID 0323890: An error occurs when a user tries to remove the monitors from a load balancing service by using the 'Remove' button in the configuration utility's Configure Service window.

Content Switching

- Issue ID 0308757: A TCP content switching virtual server with a wildcard port fails to respond to clients with a SYN-ACK. Consequently, the content switching functionality fails for the virtual server.

DataStream

- Issue ID 0303980: A monitor of type MSSQL becomes unavailable if you replace the existing query with a shorter query.

HTML Injection

- Issue ID 0302088: When HTML Injection is enabled for web forms that use the 'GET' method, ES monitoring does not function properly.

Integrated Caching

- Issue ID 0288716 (Cluster): In cases, where there is a delay in processing the cache invalidation request originating from other cluster nodes, if the client sends a request before the cache invalidation request is processed on the node, the cache will serve old content.

Load Balancing

- Issue ID 89129/0248646: For non-HTTP load balancing virtual servers for which rule based persistence has been configured, the appliance does not automatically refresh the session time-out setting during a file download. Therefore, if the download is not completed before the session times out (and another request does not arrive before the session times out), the time-out setting is not refreshed, and requests that arrive during what would otherwise have been the extended time-out interval are forwarded to whatever server is selected by the configured load balancing method.

  A consequence of this behavior is failure to accelerate some Repeater Plug-in connections in a WAN optimization configuration. If a persistence session that was created for a request from a Repeater Plug-in expires before the complete response is sent to the client, the next request from the Repeater Plug-in is sent to a different Branch Repeater appliance and is therefore not accelerated. When that happens, the Branch Repeater graphical user interface indicates that the reason for the connection not being accelerated is 'Not enough room left in the TCP packet header to append unit specific options (5).'

- Issue ID 0278377 (nCore): Cache policy labels cannot be bound to MYSQL or MSSQL virtual servers.

- Issue ID 0285672: When using load balancing of Branch Repeaters in a cluster setup, there is no response from the server and the request hangs.

- Issue ID 0289339: Service group members that are configured to scale automatically are not synchronized correctly with the secondary appliance in a high availability pair. The issue can lead to appliance failure during a failover event.

- Issue ID 0304847: In the load balancing monitor structure in the XML API, the 'flags' field is now deprecated.

- Issue ID 0305045: The WI-Extended monitor sends probes to port 80 regardless of the port number for which it is configured.

- Issue ID 0309954: A GSLB virtual server becomes unavailable if you use the same IP address as the public IP address for both a local and a remote GSLB service, bind monitors to the services, and then bind the services to the virtual server.

- Issue ID 0318838: A NetScaler policy or action fails if it uses a SIP expression that is based on the Contact header. For example, a rewrite action does not work if it is configured to rewrite the Contact header.

NetScaler SDX Appliance

- Issue ID 88556/0248194: When provisioning a NetScaler instance, if you have entered invalid NetScaler settings for any of the IP address, Netmask, or Gateway parameters, you cannot modify the values for those parameters.

- Issue ID 90586/0249864: Log on to the Management Service user interface fails after 25 days.

- Issue ID 0289151: If you provision a NetScaler VPX instance with approximately 12288MB (12GB) of memory and then upgrade the instance, the upgrade operation fails and the following error message appears:

  ERROR: NetScaler on nCore VPX requires minimum 2 Gigabytes and 2 CPUs to start.

- Issue ID 0310014: If you have provisioned a NetScaler VPX instance running release 9.3 on a NetScaler SDX appliance running release 10, and the instance is restarted, the existing session between the Management Service and the VPX instance expires and an error message appears if you try to modify any settings on that instance after it restarts.

- Issue ID 0313155: NTP synchronization might fail if you add a new NTP server by using the Management Service user interface because the default contents of the ntp.conf file are not flushed.

NetScaler VPX Appliance

- Issue ID 0302377: If you install a NetScaler VPX virtual appliance on Microsoft Server 2008 R2 by using Hyper-V Manager, or if you install a NetScaler VPX virtual appliance on VMware ESX 3.5 or 4.0, you are not prompted to specify the IP address, subnet mask, and gateway. The appliance starts with the default IP address of 192.168.100.1.

Networking

- Issue ID 0243105: When there are ECMP routes for a prefix, for every new route addition or deletion, the NetScaler appliance withdraws all the UP routes and adds them back again to its routing table. This results in a period of time when there are no routes to the prefix.
- Issue ID 0277297: NetScaler APIs do not display some of the attributes that are displayed in the output of 'show connectiontable -detail full' command.
- Issue ID 0300820: When the NetScaler appliance receives an unpredicted flow of SYNs, it blocks the connect system calls used by OSPF daemon. This causes delay in sending out the hello packets resulting in adjacency failure.
- Issue ID 0302613: When an OSPF connection times out, the NetScaler appliance removes and applies back the router configuration. This causes an adjacency flap which momentary drops all the advertised routes.
- Issue ID 0305420: If the NetScaler appliance receives any traffic which hits a virtual server of type ANY then only for the first packet of this traffic the TTL value set to 255 and for the remaining packets, belonging the same session, the TTL value remains same. This applies to even fragment packets, where only for the first fragment of the packet the TTL value is set to 255 and for the remaining fragments the TTL value is unchanged.
- Issue ID 0311243: When a virtual server, which has a listen policy bound to it, receives IPv4 fragments of a request that evaluates the policy to TRUE, the NetScaler appliance becomes unresponsive while performing service lookup on the received IPv4 fragments
- Issue ID 0312412: The command 'sh ip ospf <1-65535> database', in the VTYSH command prompt, displays the database for all the OSPF processes instead of just for the process id specified.
- Issue ID 0318668: A virtual server of type ANY drops the IPv6 ECHO reply if the ECHO request didn't pass through the appliance and the related IPv6 to IPv4 mapping is not present in appliance.

Platform

- Issue ID 0275149 (nCore): On a NetScaler appliance that has LACP configured and interface speed set to AUTO, if the link speed on one of the interfaces in a channel is reduced after autonegotiation with the device at the other end, the interface is treated as DOWN by the LACP channel on the peer device. However, the NetScaler appliance does not identify the new reduced link speed and continues to treat the interface as UP.

Policy

- Issue ID 0291487: NetScaler appliances running version 9.2 build 52.1 or later and have a large number (in the hundreds) of policy bindings can experience performance issues on 'save ns config' and 'show config' operations. This can lead to interruption in services.
- Issue ID 0291975: The SYS.VSERVER('<vserver_name>').THROUGHPUT expression returns an incorrect throughput value.
- Issue ID 0311268: You cannot add a rule of the form 'HTTP.REQ/RES.BODY(<num>).CONTAINS(<string2>)' where <string2> has the property that its length is greater than the length of <string1>. <string1> is already existing string in the already configured policy expression 'HTTP.REQ/RES.BODY(<num>).CONTAINS(<string1>)'.

  For example, the second command provided below might not succeed if there exists some request for which the evaluation of rule in cs_example is in progress.

  -> add cs policy cs_example -rule 'HTTP.REQ.BODY(1000).CONTAINS("MyLengthIs12")
  -> add cs policy cs_example_break -rule 'HTTP.REQ.BODY(1000).CONTAINS("MyLengthIsBIG15")

Reporting

- Issue ID 0313793: You can now include period (.), colon (,), and hyphen (-) special characters in report titles.

SNMP

- Issue ID 0309930: The SNMP OID for vsvrCurSslVpnUsers is getting counter values only from core 0.

SSL

- Issue ID 0316577: The SSL crypto card instrumentation is enhanced to provide more information on error status during initialization and at runtime.

Stream Analytics

- Issue ID 0307283: NetScaler supports a maximum of 500 stream session records. Stream records beyond the maximum supported value are not tracked. The statistics command, 'stat stream identifier', displays a maximum 500 stream records.

System

- Issue ID 93169/0257092 (nCore): NetScaler nCore appliances now support keep-alive for TCP connections. When this feature is enabled, with the default settings, the appliance probes any TCP connection that has been idle for 15 minutes. If the appliance does not receive a response from the peer within 75 seconds, it sends a second probe. If no response to that probe is received within 75 seconds, the appliance sends a third, final probe. If no response to the final probe is received within 75 seconds, the appliance resets the connection.

  By default, this feature is disabled. In addition to enabling the feature, you can change the default values for connection idle time, number of probes to send to the peer, and the interval at which to send probes. In the CLI, use the following command to change the default settings:

  set ns tcpProfile <name> [-KA ENABLED] [-KAconnIdleTime <positive_integer>] [-KAmaxProbes <positive_

  In the configuration utility, you can change the settings in the System > Profiles > TCP Profiles > Add TCP Profile or Configure TCP Profile dialog box.

- Issue ID 0270163: When the NetScaler appliance runs processes such as gzip, the usage of the management CPU increases. Hence, high CPU usage alerts may get generated even though the packet engines are not actively processing packets.

- Issue ID 0275501: A user can view all of the virtual servers configured on the NetScaler appliance, even though the user is bound to a command policy that has a condition for restricting the user to view only a set of virtual servers.

- Issue ID 0285015: Requests buffers larger than 24KB lead to buffer overflow and result in the web log module not working.

- Issue ID 0302004: For load balancing virtual servers that have SOURCEIP persistence configured, client IP header insertion might fail for HTTP CONNECT requests sent to that virtual server.

- Issue ID 0319417: Server response in which the HTTP header spans more than 16 nsbs is reset even if the 'drop invalid requests' flag is disabled.

Web Interface

- Issue ID 86538/0246528: The following dialog boxes under 'Upload Plugins' available in the 'Web Interface' pane of the configuration utility do not work as expected:

  - Windows Client

  - Linux Client

  - Macintosh Client

- Issue ID 0322207: In a high availability setup, delays in Apache Tomcat start-up might prevent the propagation of web interface configurations to the secondary appliance. As a result, the web interface configurations are not available when the secondary appliance becomes primary.

XML

- Issue ID 0304314: SOAP requests that do not conform to a WSDL are not handled properly by the XML validation module.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0303507: NetScaler automatic domain join is failing with Likewise 6.1. If you attempt to create a Kerberoes authentication action, the attempt fails with the following error message:

  ```
  LsaAdJoinDomain (40041) Invalid parameter
  ```

  To work around this issue, at the NetScaler command line open a Unix shell, adn then type the following command to manually join the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join <DOMAINNAME>
  <DomainUserName>
  ```

  Note: You must issue this command after each reboot.

- Issue ID 0310205: If you attempt to kill a user session by using the username parameter with either the NetScaler command line 'kill session' command or the configuration utility, the session is not terminated on either the NetScaler appliance or the client.

- Issue ID 0327114: On a NetScaler appliance with NetScaler 10 build 69.4 nc installed, if you use the configuration utility to configure authentication on a load-balancing virtual server, the following error message appears:

  No Authentication Host specified

  The configuration utility then removes the authentication host from the configuration. This behavior occurs regardless of whether you are configuring authentication host settings on the virtual server for the first time, or modifying existing authentication host settings on the virtual server.

Access Gateway

- Issue ID 90722/0249975: When users log on with the Access Gateway Plug-in, the 'File Transfer' tab on the Access Interface is available, but the 'File Transfer option' is not available if users right-click the Access Gateway icon in the notification area.

- Issue ID 92543/0251596: After you configure Access Gateway to provide user connections through Citrix Receiver, when users right-click the Receiver icon in the notification area, the Log on option does not appear. Users must connect by using the Web browser or they must right-click the Receiver icon and then, depending on the version of Receiver they are using, click About or Preferences from the Receiver menu and Plug-in Status or Advanced from the Receiver panel. You can also enable the log on option to appear when users right-click the Receiver icon by adding the following settings in the registry:

  - Add the Receiver key (if the key does not already exist) under the following registry locations:

    - `HKEY_CURRENT_USER\Software\Citrix\`

    - `HKEY_LOCAL_MACHINE\Software\Citrix\`
  - Add the Inventory key in the following registry locations:

    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`

    - `HKEY_CURRENT_USER\Software\Citrix\Receiver`
  - In the Inventory key, configure the following **REG_SZ** values:

    - **VPNAddress**. Provide the value as the Web address for the Access Gateway appliance; for example, https://<AccessGatewayFQDN>.

    - **VPNPrompt1**. Provide the value as 'UserName'.

    - **VPNPrompt2**. Provide the value as '*Password'.

      Note: To mask the password, enter an asterisk (*) before the word.

      In addition, if you configure double-source authentication that requires authentication with LDAP plus RSA authentication, you need to also add the following as **REG_SZ**:

    - **VPNPrompt3**. Provide the value as '*Passcode'.
- Issue ID 0261547: When you enable Access Gateway as a reverse proxy and you enable basic preauthentication and post- authentication scans, as well as encryption and client choices, when users log on with the Access Gateway Plug-in, the preauthentication scan passes, but the post-authentication scan fails.

- Issue ID 0275079: When users access applications published on XenApp, each user consumes multiple Access Gateway licenses per application. Instead, one session ID should be shared across the applications the user accesses. As a result, users exceed their allocated license count and an SSL error occurs.

- Issue ID 0285995: If you configure Access Gateway to assign an intranet IP address to user devices that connect to Access Gateway, when users log on with the Access Gateway Plug-in, the secure DNS dynamic update does not occur and the intranet IP

address is not registered with the DNS Server.

- Issue ID 0288469: After you configure a virtual server to use the Access Gateway Plug-in for Java, when users log on with the Access Gateway Plug-in by using a browser that has a 64-bit Java Runtime Environment (JRE) installed, the plug-in fails to establish a connection.

- Issue ID 0291264: If you create a Web Interface 5.4 site and enable authentication through Access Gateway, and you enable single sign-on with a smart card to the Web Interface that enables smart card pass-through, when users log on with the Access Gateway Plug-in, the users' desktops are not listed on the Web Interface.

- Issue ID 0291821: If you create a Web Interface 5.4 site and enable authentication with a smart card through Access Gateway, and you configure the 'Single Sign-on Domain' on the 'Published Applications' tab using the format domainname.com instead of domainname, when users start a published application or desktop, authentication fails.

- Issue ID 0292005: When users connect with clientless access and try to download a file larger than 1 gigabyte (GB) from the file share on the home page, as the file is downloading, if an upload is attempted, the download process fails but the upload continues.

- Issue ID 0298971: When users log on with the Access Gateway Plug-in for Java and the Web Interface opens in Internet Explorer 9, if users do not turn on Compatibility View in Internet Explorer, when they click a published application, the following error appears: Resource shortcuts are not available.

- Issue ID 0299515: If you configure an intranet IP address on Access Gateway, when users connect with the Access Gateway Plug-in on a computer running Windows XP Service Pack 3 and try to access a CIFS share hosted on a computer in the secure network, users receive an error that the share is inaccessible.

- Issue ID 0300511: When users log on using clientless access and click a bookmark from the home page to open a Distributed File Share (DFS), if the target folder resides on a different computer than the computer where the domain DFS server resides, the share does not open.

- Issue ID 0308733: If you configure Access Gateway with additional appliances in which global server load balancing (GSLB) is enabled, when users log on with the Access Gateway Plug-in, occasionally the connection times out, a time-out error appears, such as 'Your Citrix Access Gateway session timed-out and you are not connected,' and the session disconnects.

- Issue ID 0309017: When you configure a preauthentication and post-authentication policy with an expression to scan a user device for a file, Access Gateway does not check for expression syntax. As a result, Access Gateway accepts inappropriate syntax configuration and the scan fails.

- Issue ID 0319607: If an authentication server and Access Gateway reside in the same domain, the appliance may fail.

- Issue ID 0319901: If you enable Integrated Caching and Web Interface on Netscaler on an Access Gateway appliance, and then change the URL for the Web Interface, Access Gateway might fail.

AppExpert

- Issue ID 0323436: The NetScaler configuration utility can display a maximum of 4500 bound patterns of a pattern set.

Application Firewall

- Issue ID 0284009: If sessionless URL closure is enabled, and Validate Referer Header is set to If Present, a spurious Referer header check error is generated and logged when a web form with an action URL is submitted. If blocking is enabled for the Start URL check, then requests that contain web forms with action URLs are blocked. To work around this issue, if you configure Sessionless URL Closure, set Validate Referer Header to Off.

- Issue ID 0299940: The change profile type command does not work correctly.

  - If you try to change a profile type to Web 2.0, the profile type remains HTML.

  - If you try to change a profile type to XML, the Profile Type field disappears completely.

  When you use the configuration utility to change the profile type, the profile type is actually changed correctly, but the display is incorrect. When you use the NetScaler command line, the actual profile type is set as shown above.

- Issue ID 0301813: When deploying a learned Cross-Site Request Forgery relaxation from the Syslog Viewer, the configuration utility does not deploy the relaxation, but displays the following error message: 'CSRF Tag validation failed'.

- Issue ID 0302294: Learned relaxations are sometimes not removed from the review list after they have been deployed. To manually remove a learned relaxation that has already been deployed, in the Manage Learned Rules dialog box select the relaxation and then click 'Skip'.

- Issue ID 0303044: Only QualysGuard WAS 1.0 scan reports are supported when importing signature rules. WAS 2.0 scan reports are not supported.

Cache Redirection

- Issue ID 0287688: If you set the L2Conn parameter for a cache redirection virtual server before you finish setting up the cache redirection configuration (including the other participating entities, such as the load balancing virtual server and the services that should be bound to the load balancing virtual server), the NetScaler appliance sends clients the SYN-ACK segments that it receives from the cache or origin servers during connection establishment with those servers. Clients respond to the SYN-ACK segments with a TCP RESET. Consequently, the requests are dropped.

  Workaround: Enable the L2Conn parameter for the cache redirection virtual server after you finish setting up the cache redirection configuration.

- Issue ID 0328353: When you use the configuration utility to bind a cache redirection policy to a cache redirection virtual server, the policy is added to the content switching (CSW) policy tab instead of cache redirection (CRD) policy tab. If you try to resolve this issue by using the CR virtual server wizard, the following error message appears: 'Please specify Target.'

- Issue ID 0330033: Tabs for filter/compression policy bindings are not displayed for a cache redirection virtual server, and it is not possible to bind those policies to a cache redirection virtual server.

- Issue ID 0330139: If you use the configuration utility to unset a cache virtual server for a cache redirection virtual server, the process fails and the following error message appears: invalid argument.

Command Line Interface

- Issue ID 92269/0251344: If you upgrade from an earlier build to a later build within release 9.2 or release 9.3, or upgrade from release 9.2 to release 9.3, or upgrade from an earlier release to release 10, the time zone settings may be lost on upgrade.

  Workaround: Delete the time zone from the configuration (ns.conf), upgrade to the target build or release, and then reconfigure the time zone.

Configuration Utility

- Issue ID 0251463: When you click the Applications node in AppExpert, the configuration utility throws a null pointer exception. The issue occurs sporadically.

- Issue ID 0269337: If you use the Google Chrome browser, with the toolbars installed, to access the configuration utility, the toolbars distort the views.

  Workaround: Hide the toolbars in Chrome browser when you access the configuration utility.

- Issue ID 0278097: In the configuration utility, if you click Application Firewall in the navigation pane, the scroll bar moves up and the subnodes of the Application Firewall node disappear. You have to scroll down to view the subnodes.

- Issue ID 0298686: If the details pane contains too may records to display on one screen, the header row moves off the screen if you scroll down.

- Issue ID 0300506: On the MPX 17000 platform, if you use the configuration utility to upgrade from release 9.2 build 55.5 to release 10, the appliance does not restart automatically after the upgrade.

  Workaround: Restart the appliance manually by using the command line or the configuration utility.

- Issue ID 0303279: In the configuration utility, in the Rewrite Policies pane, clicking Add does not display the Create Rewrite Policy dialog box but disables the main configuration utility window.

- Issue ID 0311358: The NetScaler configuration utility fails to load when accessed from Internet Explorer version 7 browser running on Windows 2003 or Windows XP.

  Workaround: Use Internet Explorer version 8 and above.

- Issue ID 0319061: The configuration utility does not throw the 'Feature not supported' prompt when configuring the following unsupported features on a NetScaler cluster: Bridge groups, Network Bridge, VMAC6, and FIS. This issue is observed only in a cluster setup.

- Issue ID 0322821: When the SRADV (Static Route Advertisement) mode is ON, the static routes which are not explicitly disabled for advertisement will be advertised using all the routing protocols. However, the advertised protocols column for route in the configuration utility does not show any protocol list. This issue is observed only in a cluster setup.

- Issue ID 0322894: The configuration utility displays an inappropriate error message when adding a forwarding session that has an invalid subnet mask. This issue is observed only in a cluster setup.

- Issue ID 0322914: When the IP is not resolved for a hostname based SNMP manager, the 'Resolved IP' column of the SNMP Manager table is shown as blank instead of 'Unresolved IP'. This issue is observed only in a cluster setup.

- Issue ID 0323175: The configuration utility displays a negative value for the index of the data set or pattern set, when the index is set to its maximum value. The command line

interface displays the correct value.

- Issue ID 0325400: After adding a local authentication policy by using the configuration utility, the request profile field is showing blank. By default, the request profile must be Local. This issue is observed only in a cluster setup.

- Issue ID 0326354: In System > Settings > Change global system settings, regardless of the base threshold value configured for surge protection, the value is displayed as 0. This issue is observed only in a cluster setup.

  Workaround: You can view the base threshold vale by using the 'show ns spParams' command.

- Issue ID 0326018: The dashboard does not display the Precision Time Protocol (PTP) counters for the cluster node. This issue is observed only in a cluster setup.

  Workaround: PTP counters can be viewed by using the 'stat cluster node' command.

- Issue ID 0327136: The configuration utility does not allow you to set the 'Max Clients' parameter of a service to its maximum value of 4294967294. This issue is observed only in a cluster setup.

  Workaround: You can set the maximum value by using the “set service” command.

- Issue ID 0327551: In the configuration utility, all features appear to be enabled even when the features are disabled.

- Issue ID 0328660: In the configuration utility, when you view the virtual server persistence sessions, a persistence type setting of DIAMETER is displayed as SOURCE IP.

- Issue ID 0328715: In the configuration utility, the details of the monitor bound to a service do not include response codes for a monitor of type DIAMETER.

- Issue ID 0328844: While configuring the OCSP responder through the configuration utility, the default value of the HTTP response timeout is erroneously taken as 0ms. The default value of the HTTP response timeout must be 2000ms. This issue is observed only in a cluster setup.

  Workaround: You must explicitly set the HTTP response timeout in the configuration utility.

- Issue ID 0329154: In System > Auditing > Recent audit messages, when you set number of audit messages to be displayed to 256 (maximum allowed value), a 'Value entered is out of range' error message is displayed on clicking Refresh. This issue is observed only in a cluster setup.

- Issue ID 0329826: If you use the configuration utility to view the license for features, warning messages are seen for the features that are licensed but not supported. This issue is observed only in a cluster setup.

- Issue ID 0332768: On Internet Explorer 8, the configuration utility does not show the pop-up for installing the JRE plugin.

- Issue ID 0332795: On systems that have JRE 1.6.0_24 and 1.7.0_06, the configuration utility cannot load the Java applet. Therefore, you cannot perform any operations on the configuration utility.

Workaround: Uninstall JRE 1.6.0_24 and 1.7.0_06 and install JRE 1.6.0_31.

- Issue ID 0332876: When you use the configuration utility to change the password of a user, the Change Password dialog displays encrypted password in the Password and Confirm Password fields.
- Issue ID 0333026: On a system running the Windows 7, 64-bit operating system, the configuration utility cannot load the Java applet. Therefore, you cannot perform any operations on the configuration utility.
- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

  Workaround: Search for the virtual server names with the expressions "*" or "app" by using the search utility.

Cloud Gateway

- Issue ID 0327119: When you create policy rules from the configuration utility, an error occurs and the policies are not configured.

Content Switching

- Issue ID 0330290: You cannot use the configuration utility to bind a content switching policy to a content switching virtual server if the policy is configured with only a domain value. The bind fails, and the following error message appears: 'Priority cannot be specified for URL-based content switching policy.'
- Issue ID 0331029: If you use the configuration utility to open a content switching virtual server that has a default policy bound to it, the process fails and the following error message appears: No Such Resource.

Documentation

- Issue ID 0277923: The documentation for the Content Switching feature states that if a policy that is bound to a content switching virtual server evaluates to TRUE, and the policy's Goto expression specifies END, policy evaluation terminates at that policy. However, the documentation does not mention that, if the content switching virtual server has a default virtual server, the request is forwarded to the default load balancing virtual server when policy evaluation is terminated.

Domain Name System

- Issue ID 0291053: Under the following sequence of events, the NetScaler appliance sends the client a cached NXDOMAIN response instead of the IP addresses that are configured in the DNS action for response rewrite:

  1. A security-aware name server sends the appliance a DNSSEC-enabled NXDOMAIN response for a non-existent domain. The appliance, which is designed to not rewrite DNSSEC-enabled responses, relays the negative response to the client without modifying it. The appliance also caches the response.

  2. A client sends the appliance a request for the same domain, but it does not set the DNSSEC OK EDNS header bit.

  This behavior is expected, and ensures that security-aware and security-oblivious clients receive the same response.

- Issue ID 0301348: Even though the NetScaler user interface allows you to create DNS policy labels, the DNS policy label functionality is not supported in this release.

Global Server Load Balancing

- Issue IDs 0287825 and 0287827: If the master node and slave node in a Global Server Load Balancing (GSLB) configuration are running different NetScaler releases, the site synchronization process fails when the master node is collecting GSLB configuration information from the slave node. The issue is specific to NetScaler releases 9.2, 9.3, and 10. The issue occurs if one node (either the master or the slave) is running NetScaler release 10 and the other node is running NetScaler release 9.2 or 9.3.

- Issue ID 0324486: When creating a local GSLB site in the NetScaler configuration utility, if you set the Trigger Monitors option to MEPDOWN, the GSLB site does not appear in the details pane until after you click Refresh.

- Issue ID 0326001: If a GSLB virtual server's primary and backup GSLB methods are both set to round trip time (RTT) or static proximity and source IP persistence is enabled, when the primary GSLB method fails, the backup GSLB method also fails.

  Workaround: If you use RTT or static proximity as the primary GSLB method, do not use the same method as the backup GSLB method.

- Issue ID 0328911: When configuring monitoring for a GSLB service by using the NetScaler configuration utility, if you include monitors that cannot be used with GSLB services (for example, ARP monitors) along with monitors that can be used with GSLB services (for example, TCP monitors), the configuration utility displays an error message for the invalid monitor bindings, but the valid bindings succeed. When you unbind an invalid monitor from the service, the message 'Error' is displayed. No further information is provided in the message.

Load Balancing

- Issue ID 0248750: NetScaler now supports dynamic selection of a load balancing virtual server. The lb virtual server is identified at the run time using an expression in the content switching action.

- Issue ID 90395/0249705: If the rule that is used for creating rule based persistence sessions is a compound expression, the 'show lb persistentSessions' CLI command displays an internal representation of the persistence parameter instead of the actual persistence parameter.

- Issue ID 90875/0250110: On a TCP load balancing virtual server, if persistence is defined with the rule 'client.tcp.payload(n)', and a request is received in multiple parts such that there is a delay between the parts and a FIN is sent from client before the expected number of bytes (n), the NetScaler appliance creates an undesired session with the received number of bytes (which is less than n).

- Issue ID 91711/0250846: If the string (or 'token') that is used for creating rule based persistence sessions for load balancing virtual servers is larger than 64 KB, the NetScaler appliance fails to create persistence sessions. For example, the appliance fails to create persistence sessions with the rule CLIENT.TCP.PAYLOAD(70000) because the token that is used is larger than 64 KB. However, the appliance creates persistence sessions successfully with a rule such as CLIENT.TCP.PAYLOAD(70000).BEFORE_STR('string2').AFTER_STR('string1') if the string that is enclosed by 'string1' and 'string2' is not larger than 64 KB.

- Issue ID 94405/0258207: If you specify a persistence rule for a load balancing virtual server without specifying a persistence type or setting the load balancing method to TOKEN, the NetScaler appliance discards the rule without checking its validity. This behavior is by design.

- Issue ID 0324061: When you configure a SIP-UDP load balancing virtual server by using the NetScaler command-line interface, the default setting for persistence type is CALLID. However, when you use the configuration utility to configure a SIP-UDP virtual server, the default setting for persistence type is NONE.

- Issue ID 0330276: The virtual router IDs (VRIDs) that are configured on the NetScaler appliance are not available in the Virtual Router ID list in the Create IP and Configure IP dialog boxes (Network > IPs > Add/Open). Consequently, you cannot use the configuration utility to bind a VRID to a virtual server.

- Issue ID 0351632: A NetScaler nCore appliance uses multiple CPU cores for packet handling. Every session on the appliance is owned by a CPU core. If the appliance receives a request for which a session does not already exist, a session is created, and one of the cores is designated as the owner of that session. Subsequent requests that belong to that session might not always arrive at and be handled by the owner core. In that case, inter-core messaging ensures that the session information on the owner core is always current. However, when a core receives a request that belongs to a persistence session owned by another core, the inter-core messaging does not refresh the timeout value for the persistence session. Consequently, in the output of successively executed show lb persistentSessions commands, which display timeout values from owner cores only, the timeout value for a persistence session might diminish to 0 (zero), even if the persistence session continues to be active.

NetScaler SDX Appliance

- Issue ID 0261232: If you set the date on the Management Service to an earlier date, the inventory and stats are not updated in the Management Service user interface.

  Workaround: Log on to the Management Service by using an SSH client, such as PuTTY. At the shell prompt, type: #/etc/rc.d/svmd restart

Networking

- Issue ID 0276933: When you change the next hop parameter of a PBR for IPv4 traffic, the new hop is taken into account even if you have not applied the PBRs.
- Issue ID 0299716: In a cluster setup, the 'bind vlan' command throws an error when interface and IP address are specified together.

  Workaround: Bind the interface and IP address individually, by using separate 'bind vlan' commands.
- Issue ID 0316144: In a cluster setup, the Precision Time Protocol (PTP) time across cluster nodes will not be synchronized when PTP packets are dropped due to backplane switch or if the physical resources are over-committed in a virtual environment.

  Workaround:

  - Disable PTP using the command 'set ptp -state disable' and configure NTP to synchronize the time across the cluster nodes.
  - If the backplane switch is like the Extreme switch, disable the multicast PTP packets from reaching the CPU by using the following command (this might cause some relevant features, such as routing, from not working):

    ```
    ipmcforwarding to-cpu off ports 41-48 <backplane-interfaces>
    ```

Rewrite

- Issue ID 0305831: The man pages for add and set rewrite action do not include xpath_html (xp<delimiter>xpath expression<delimiter>) as a search expression.

SSL

- Issue ID 74279/0236509: The cipher TLS1-EXP1024-DES-CBC-SHA is not supported by the NetScaler appliance.
- Issue ID 0327173: The ciphers bound to an SSL virtual server are not displayed in the configuration utility.

System

- Issue ID 0325665: An unrelated error code is displayed on executing the 'set filter prebodyinjection/postbodyinjection' commands.

- Issue ID 0327118: In the configuration utility, the minimum and maximum values allowed for number of audit messages is incorrect. The maximum and minimum values displayed are 255 and 0, but the correct values are 256 and 1.

Web Interface

- Issue ID 0306731: If the Rewrite feature is not enabled, the Enable access through receiver client option for a Web Interface(WI) site does not work. This is because the functionality of the option depends on some rewrite policies on the appliance.

- Issue ID 0315502: The Configuration Utility displays an error message when you try to disable the Web Interface feature.

- Issue ID 0315951: If the Responder feature is not enabled, the Make Site Path Case Insensitive option for a Web Interface(WI) site does not work. This is because the functionality of the option depends on some Responder polies on the appliance.

  Workaround: Enable the Responder feature before you select the Make Site Path Case Insensitive option for a WI site.

- Issue ID 0324373: In the Web Interface (WI) configuration wizard, for a WI site in gateway direct mode, the state of the Enable Access through Receiver Client option is shown selected even when there are no rewrite policies bound to the selected Access Gateway virtual server.

- Issue ID 0331904: In the Web Interface (WI) configuration wizard, the Enable Access through Receiver Client option remain selected even when you try to clear the option.

Enhancement Releases

This section describes the enhancements, changes, bug fixes, and known issues provided in the enhancement releases of the Citrix® NetScaler® and Citrix® NetScaler® SDX.

Build 75.7007.e

Release version: Citrix NetScaler release 10.e build 75.7007.e

Replaces build: None

Release date: July 2013

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Bug Fixes
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 75.7. The release notes are available in the Build 75.7 section on Citrix eDocs.
- The enhancements, bug fixes, and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Enhancements

CloudBridge Release 7.0

- To learn about the enhancements in CloudBridge Release 7.0, see the "Enhancements" section of the CloudBridge 7.0 release notes at Citrix CloudBridge 7.0 Release Notes.

Bug Fixes

AAA Application Traffic

- Issue ID 0372362: When Kerberos Constrained Delegation is configured with a content switching virtual server, the NetScaler appliance might hang or crash. The cause is a GET request with multiple authorization headers. (Only one authorization header is expected.)

- Issue ID 0387076: On a NetScaler appliance with AAA enabled and Kerberos Constrained Delegation single sign-on configured, after several single sign-on requests are successfully authenticated, the virtual server principle can unexpectedly become blank. When this happens, subsequent authentication requests fail.

Known Issues and Workarounds

Application Firewall

- Issue ID 0363711: On a NetScaler appliance that has AAA, Kerberos authentication, KCD, and MSSQL monitor enabled, each monitor probe causes a memory leak that eventually results in the NetScaler appliance experiencing an out-of-memory condition that requires a restart to clear.

NetScaler VPX on AWS

- Issue ID 0337614: Custom scriptable monitors do not work on NetScaler VPX on AWS.
- Issue ID 0340395: While configuring HA between two VPX instances in AWS, if you first configure HA on the VPX instance with a single ENI, HA configuration does not work as expected.

  Workaround: Configure the instance with two or more ENIs before configuring HA on the instance with one ENI.
- Issue ID 0344678: If you remove HA configuration from the primary instance first, HA configuration is not removed and causes the primary instance to reboot.

  Workaround: Remove HA configuration from the secondary instance first before removing HA configuration from the primary instance.
- Issue ID 0346689: In INC mode, HA configuration between two NetScaler VPX instances in AWS does not work properly.

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.
- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.
- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

Build 74.4006.e

Release version: Citrix NetScaler release 10.e build 74.4006.e

Replaces build: None

Release date: April 2013

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 74.4. The release notes are available in the Build 74.4 section on Citrix eDocs.
- The enhancements and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Enhancements

Offload DNSSEC Operations to the NetScaler Appliance

- Issue IDs 0246717 and 0249691: For DNS zones for which your DNS servers are authoritative, you can offload DNSSEC operations to the NetScaler appliance. When a DNS server sends a response, the appliance signs the response on the fly before relaying it to the client. The appliance also caches the signed response. Apart from reducing the load on the DNS servers, offloading DNSSEC operations to the appliance gives you the following benefits:

  - You can sign records that the DNS servers generate programmatically. Such records cannot be signed by routine zone signing operations performed on the DNS servers.

  - You can serve signed responses to clients even if you have not implemented DNSSEC on your servers.

  To configure DNSSEC offloading for a zone, you add the zone to the NetScaler appliance and set the zone's Proxy Mode and DNSSEC Offload parameters to YES and ENABLED, respectively. Optionally, you configure NSEC record generation for that zone.

  To enable DNSSEC offload for a zone by using the NetScaler command line

  At the NetScaler command line, type:

  add dns zone <zoneName> **-proxyMode YES -dnssecOffload ENABLED [-nsec (ENABLED | DISABLED)]**

  To enable DNSSEC offload for a zone by using the configuration utility

  1. In the navigation pane, expand DNS, and then click Zones.

  2. In the details pane, do one of the following:

     - To create a zone on the appliance, click Add.

     - To configure DNSSEC offloading for an existing zone, click the zone, and then click Open.

  3. In the Create DNS Zone or Configure DNS Zone dialog box, select the Proxy Mode and DNSSEC Offload check boxes.

  4. Optionally, if you want the NetScaler appliance to generate NSEC records for the zone, select the NSEC check box.

  5. Click OK.

  You must also generate DNS keys for the zone, add the keys to the zone, and then sign the zone with the keys. These configuration tasks are the same as the tasks you perform for configuring DNSSEC on the NetScaler appliance.

  After you configure DNS offload, you must flush the DNS cache on the appliance. Flushing the DNS cache ensure that any unsigned records in the cache are removed and subsequently replaced by signed records.

  Note: DNSSEC offload is supported on all NetScaler MPX platforms, except the NetScaler MPX 9700/10500/12500/15500 FIPS platform. The feature is also supported on NetScaler VPX appliances hosted on NetScaler SDX platforms.

DNSSEC offload is not supported in a NetScaler cluster.

Known Issues and Workarounds

Application Firewall

- Issue ID 0363711: On a NetScaler appliance that has AAA, Kerberos authentication, KCD, and MSSQL monitor enabled, each monitor probe causes a memory leak that eventually results in the NetScaler appliance experiencing an out-of-memory condition that requires a restart to clear.

Domain Name System

- Issue ID 0376662: The NetScaler appliance might fail in the following scenario:
  - You have configured DNSSEC offload and enabled NSEC record generation for a zone on the appliance.
  - The appliance receives a DNS NODATA/NXDOMAIN query for that zone, over TCP, and the DNSSEC OK bit in the query is set.

NetScaler VPX on AWS

- Issue ID 0337614: Custom scriptable monitors do not work on NetScaler VPX on AWS.
- Issue ID 0340395: While configuring HA between two VPX instances in AWS, if you first configure HA on the VPX instance with a single ENI, HA configuration does not work as expected.

  Workaround: Configure the instance with two or more ENIs before configuring HA on the instance with one ENI.
- Issue ID 0344678: If you remove HA configuration from the primary instance first, HA configuration is not removed and causes the primary instance to reboot.

  Workaround: Remove HA configuration from the secondary instance first before removing HA configuration from the primary instance.
- Issue ID 0346689: In INC mode, HA configuration between two NetScaler VPX instances in AWS does not work properly.

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.
- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.
- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

Build 73.5002.e

Release version: Citrix® NetScaler® release 10.e build 73.5002.e

Replaces build: None

Release date: March 2013

Release notes version: 2.0

Language supported: English (US)

Review the following sections:

- Bug Fixes
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 73.5. The release notes are available in the Build 73.5 section on Citrix eDocs.
- The bug fixes and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Bug Fixes

AAA Application Traffic

- Issue ID 0349418: The NetScaler appliance now supports the exclusive normalization method with SAML. For that reason, assertions posted by any SAML 2.0 compliant IDP (such as the Pingone IDP server or Oracle ID server) are now handled correctly.

NetScaler SDX Appliance

- Issue ID 0367461: If a NetScaler VPX instance provisioned on a NetScaler SDX appliance is upgraded to release 10.0 build 71.6014.e or release 10.0 build 72.5005.e, all existing LA channels, and any new channels that you create, acquire the same, incorrect, MAC address. As a result, the services might go down and you might not be able to access the VPX instance by using the NetScaler IP (NSIP) address.

Known Issues and Workarounds

Application Firewall

- Issue ID 0363711: On a NetScaler appliance that has AAA, Kerberos authentication, KCD, and MSSQL monitor enabled, each monitor probe causes a memory leak that eventually results in the NetScaler appliance experiencing an out-of-memory condition that requires a restart to clear.

NetScaler VPX on AWS

- Issue ID 0337614: Custom scriptable monitors do not work on NetScaler VPX on AWS.
- Issue ID 0340395: While configuring HA between two VPX instances in AWS, if you first configure HA on the VPX instance with a single ENI, HA configuration does not work as expected.

  Workaround: Configure the instance with two or more ENIs before configuring HA on the instance with one ENI.
- Issue ID 0344678: If you remove HA configuration from the primary instance first, HA configuration is not removed and causes the primary instance to reboot.

  Workaround: Remove HA configuration from the secondary instance first before removing HA configuration from the primary instance.
- Issue ID 0346689: In INC mode, HA configuration between two NetScaler VPX instances in AWS does not work properly.

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.
- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.
- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

Build 72.5005.e

Release version: Citrix® NetScaler® release 10.e build 72.5005.e

Replaces build: None

Release date: January 2013

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Bug Fixes
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 72.5. The release notes are available in the Build 72.5 section on Citrix eDocs.
- The enhancements, bug fixes, and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Enhancements

GUI Support for Kerberos Protocol Transition and Constrained Delegation

- Issue ID 0288056: Kerberos Protocol Transition (KPT) and Kerberos Constrained Delegation (KCD) can now be configured by using the configuration utility as well as the NetScaler command line.

KCD Support for Microsoft SQL Data Stream

- Issue IDs 0307491 and 0329542: Kerberos Constrained Delegation (KCD) is now supported for the Microsoft SQL server and the MSSQL data stream.

Bug Fixes

AAA Application Traffic

- Issue ID 0325382: To configure Kerberos-Constrained Delegation (KCD) on a NetScaler appliance with AAA-TM enabled, the appliance must be part of the authentication server's domain. You can add the appliance to that domain by creating a negotiate policy as if a client-side negotiation were intended, or by using the Likewise domainjoin command.

- Issue ID 0354718: On a NetScaler appliance that has AAA and Kerberos Constrained Delegation (KCD) enabled, if you configure a service without first configuring the associated server, the appliance might hang.

Known Issues and Workarounds

Application Firewall

- Issue ID 0363711: On a NetScaler appliance that has AAA, Kerberos authentication, KCD, and MSSQL monitor enabled, each monitor probe causes a memory leak that eventually results in the NetScaler appliance experiencing an out-of-memory condition that requires a restart to clear.

NetScaler VPX on AWS

- Issue ID 0337614: Custom scriptable monitors do not work on NetScaler VPX on AWS.
- Issue ID 0340395: While configuring HA between two VPX instances in AWS, if you first configure HA on the VPX instance with a single ENI, HA configuration does not work as expected.

  Workaround: Configure the instance with two or more ENIs before configuring HA on the instance with one ENI.
- Issue ID 0344678: If you remove HA configuration from the primary instance first, HA configuration is not removed and causes the primary instance to reboot.

  Workaround: Remove HA configuration from the secondary instance first before removing HA configuration from the primary instance.
- Issue ID 0346689: In INC mode, HA configuration between two NetScaler VPX instances in AWS does not work properly.

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.
- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.
- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

Build 71.6016.e

Release version: Citrix® NetScaler® release 10.e build 71.6016.e

Replaces build: None

Release date: December 2012

Release notes version: 2.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 71.6. The release notes are available in the Build 71.6 section on Citrix eDocs.
- The enhancements and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Enhancements

AutoScale: Automatically Scaling Your Application Fleet in a CloudPlatform Environment

- Issue ID 0311703: In an environment deployed and managed by using Citrix® CloudPlatform, automatic scaling of an application fleet can be achieved by using the Citrix® NetScaler® appliance. CloudPlatform provides a feature called AutoScale, as part of its elastic load balancing feature. A CloudPlatform user can use the AutoScale feature to specify thresholds for various conditions for automatically scaling the application fleet upward and downward. The scale up and scale down conditions can vary from simple use cases, such as a server's CPU usage, to complex use cases, such as a combination of a server's CPU usage and responsiveness. CloudPlatform, in turn, configures the NetScaler appliance to load balance traffic to the application virtual machines (VMs), monitor application thresholds and performance, and trigger scale up and scale down actions to add or remove VMs from the application fleet.

  For more information about how AutoScale works on the NetScaler appliance, see http://support.citrix.com/proddocs/topic/ns-system-10-map/ns-autoscale-automatic-scaling-in-cloudplatform-env-wrapper-con.html.

  For answers to frequently asked questions, see http://support.citrix.com/proddocs/topic/ns-faq-map/ns-faq-autoscale-ref.html.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0325382: To configure Kerberos-Constrained Delegation (KCD) on a NetScaler appliance with AAA-TM enabled, the appliance must be part of the authentication server's domain. You can add the appliance to that domain by creating a negotiate policy as if a client-side negotiation were intended, or by using the Likewise 'domainjoin' command.

  1. To create a negotiate policy, at the NetScaler command prompt type the following commands:

     > add authentication negotiateAction <negActionName> -domain <domain> -domainUser <domainuse
     > add authentication negotiatePolicy <negPolName> ns_true <negActionName>

     For <negActionName>, substitute a name for the negotiation action. For <domain>, substitute the domain of the authentication server. For <domainuser>, substitute the user name for logging on. For <passwd>, substitute the password for that user name. For <negPolName>, substitute a name for the negotiation policy.
  2. To use the Likewise 'domainjoin' command, at the NetScaler command prompt type the following commands to open a shell and then run domainjoin:

     > shell
     # /opt/likewise/bin/domainjoin-cli join <domain> <domainuser>

     For <domain>, substitute the domain of the authentication server. For <domainuser>, substitute the user name that is used to log on to the domain.

NetScaler VPX on AWS

- Issue ID 0337614: Custom scriptable monitors do not work on NetScaler VPX on AWS.
- Issue ID 0340395: While configuring HA between two VPX instances in AWS, if you first configure HA on the VPX instance with a single ENI, HA configuration does not work as expected.

  Workaround: Configure the instance with two or more ENIs before configuring HA on the instance with one ENI.
- Issue ID 0344678: If you remove HA configuration from the primary instance first, HA configuration is not removed and causes the primary instance to reboot.

  Workaround: Remove HA configuration from the secondary instance first before removing HA configuration from the primary instance.
- Issue ID 0346689: In INC mode, HA configuration between two NetScaler VPX instances in AWS does not work properly.

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.
- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.
- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

Build 71.6008.e

Release version: Citrix® NetScaler® release 10.e build 71.6008.e

Replaces build: None

Release date: November 2012

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 71.6. The release notes are available in the Build 71.6 section on Citrix eDocs.
- The enhancements and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Enhancements

NetScaler VPX on AWS

- Issue ID 0248904: You can now launch an instance of Citrix® NetScaler® VPX within Amazon Web Services (AWS). NetScaler VPX is available as an Amazon Machine Image (AMI) from AWS Marketplace. NetScaler VPX on AWS enables customers to leverage AWS Cloud computing capabilities and use NetScaler load balancing and traffic management features for their business needs. NetScaler VPX on AWS supports all the traffic management features of a physical NetScaler appliance. NetScaler VPX instances running in AWS can be deployed in standalone mode or in pairs for High Availability (HA) setup.

  Note: The NetScaler AMI launches on Windows EC2 instance types because it runs as a hardware virtual machine (HVM). HVM is currently available on Windows EC2 instances. The Windows OS is not running and is not used in any way.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0325382: To configure Kerberos-Constrained Delegation (KCD) on a NetScaler appliance with AAA-TM enabled, the appliance must be part of the authentication server's domain. You can add the appliance to that domain by creating a negotiate policy as if a client-side negotiation were intended, or by using the Likewise 'domainjoin' command.

  1. To create a negotiate policy, at the NetScaler command prompt type the following commands:

     > add authentication negotiateAction <negActionName> -domain <domain> -domainUser <domainuse
     > add authentication negotiatePolicy <negPolName> ns_true <negActionName>

     For <negActionName>, substitute a name for the negotiation action. For <domain>, substitute the domain of the authentication server. For <domainuser>, substitute the user name for logging on. For <passwd>, substitute the password for that user name. For <negPolName>, substitute a name for the negotiation policy.
  2. To use the Likewise 'domainjoin' command, at the NetScaler command prompt type the following commands to open a shell and then run domainjoin:

     > shell
     # /opt/likewise/bin/domainjoin-cli join <domain> <domainuser>

     For <domain>, substitute the domain of the authentication server. For <domainuser>, substitute the user name that is used to log on to the domain.

NetScaler VPX on AWS

- Issue ID 0337614: Custom scriptable monitors do not work on NetScaler VPX on AWS.
- Issue ID 0340395: While configuring HA between two VPX instances in AWS, if you first configure HA on the VPX instance with a single ENI, HA configuration does not work as expected.

  Workaround: Configure the instance with two or more ENIs before configuring HA on the instance with one ENI.
- Issue ID 0344678: If you remove HA configuration from the primary instance first, HA configuration is not removed and causes the primary instance to reboot.

  Workaround: Remove HA configuration from the secondary instance first before removing HA configuration from the primary instance.
- Issue ID 0346689: In INC mode, HA configuration between two NetScaler VPX instances in AWS does not work properly.

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.
- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.
- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

Build 70.7012.e

Release version: Citrix® NetScaler® release 10.e build 70.7012.e

Replaces build: None

Release date: November 2012

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Bug Fixes
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 70.7. The release notes are available in the Build 70.7 section on Citrix eDocs.
- The enhancements, bug fixes, and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Enhancements

Kerberos Constrained Delegation (KCD) Support

- Issue ID 0288056: The AAA-TM feature now supports the constrained delegation feature of the Kerberos version 5 authentication protocol (KCD). KCD allows you to configure the list of services that a Kerberos user can access after authentication.

Bug Fixes

AAA Application Traffic

- Issue ID 0327102: On a NetScaler appliance with AAA-TM enabled and Kerberos-constrained delegation (KCD) configured, if the first request after authentication is not a 401-based request, KCD can fail. If KCD fails, the individual resource that the user requested prompts the user to re-enter their credentials. The user can either re-enter the credentials as prompted, or can simply cancel the request and then request the resource a second time. In either case, the user can access the resource.

- Issue ID 0328546: On a NetScaler appliance with AAA-TM enabled and Kerberos-constrained delegation (KCD) configured, under heavy load intermittent failures of KCD can cause individual resources to prompt users to re-enter their credentials.

- Issue ID 0329020: On a NetScaler appliance with AAA-TM enabled and Kerberos-constrained delegatino (KCD) configured, after upgrading the NetScaler operating system to version 10.0.9.45, KCD does not start properly.

- Issue ID 0329280: On a NetScaler appliance with AAA-TM enabled and Kerberos-constrained delegation (KCD) configured, if you change the authentication method on the traffic management virtual server from form-based to 401-based authentication, this might cause intermittent hangs or crashes.

Known Issues and Workarounds

AAA Application Traffic

- Issue ID 0325382: To configure Kerberos-Constrained Delegation (KCD) on a NetScaler appliance with AAA-TM enabled, the appliance must be part of the authentication server's domain. You can add the appliance to that domain by creating a negotiate policy as if a client-side negotiation were intended, or by using the Likewise "domainjoin" command.

  1. To create a negotiate policy, at the NetScaler command prompt type the following commands:

     > add authentication negotiateAction <negActionName> -domain <domain> -domainUser <domainuse
     > add authentication negotiatePolicy <negPolName> ns_true <negActionName>

     For <negActionName>, substitute a name for the negotiation action. For <domain>, substitute the domain of the authentication server. For <domainuser>, substitute the user name for logging on. For <passwd>, substitute the password for that user name. For <negPolName>, substitute a name for the negotiation policy.
  2. To use the Likewise "domainjoin" command, at the NetScaler command prompt type the following commands to open a shell and then run domainjoin:

     > shell
     # /opt/likewise/bin/domainjoin-cli join <domain> <domainuser>

     For <domain>, substitute the domain of the authentication server. For <domainuser>, substitute the user name that is used to log on to the domain.

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.

- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.

- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.

Build 70.7002.e

Release version: Citrix® NetScaler® release 10.e build 70.7002.e

Replaces build: None

Release date: September 2012

Release notes version: 1.0

Language supported: English (US)

Review the following sections:

- Enhancements
- Known Issues and Workarounds

Note:

- This release is based on Citrix NetScaler release 10 build 70.7. The release notes are available in the Build 70.7 section on Citrix eDocs.
- The enhancements and known issues in this release apply to Citrix NetScaler 10.e nCore™.

Enhancements

Stateless NAT46 Translation

- Issue ID 0284926: The stateless NAT46 feature enables the communication between IPv4 and IPv6 networks by way of IPv4 to IPv6 packet translation and vice versa without maintaining any session information on the NetScaler appliance.

  A stateless NAT46 configuration on the NetScaler appliance has the following components:

  - **IPv4-IPv6 INAT entry**. An entry defining a 1:1 relationship between a public IPv4 address and an IPv6 address. In other words, a public IPv4 address on the appliance listens to connection requests on behalf of an IPv6 server

  - **NAT46 IPv6 prefix**. A global IPv6 prefix of length 96 bits (128-32=96) configured on the appliance. During IPv4 packet to IPv6 packet translation, the appliance sets the source IP address of the translated IPv6 packet to a concatenation of the NAT46 IPv6 prefix [96 bits] and the IPv4 source address [32 bits] that was received in the request packet.

  For more information, see Stateless NAT46 Translation.

Known Issues and Workarounds

Networking

- Issue ID 0331220: In a stateless NAT46 configuration, the NetScaler appliance translates corrupted ICMPv4 error messages instead of dropping them.
- Issue ID 0334959: When configuring an INAT rule for stateless NAT46 translation, the NetScaler appliance accepts a VIP address for the Public IPv4 parameter even if the VIP is already set for a non-wildcard load balancing virtual server.
- Issue ID 0336393: In a stateless NAT46 configuration, the NetScaler appliance sets an incorrect value for the MTU field of the translated ICMPv4 messages when the appliance receives ICMPv6 'packet too big' error messages that have dummy fragment headers.