Citrix NetScaler 10.1 Release Notes

Citrix NetScaler 10.1

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler appliance. If the NetScaler equipment causes interference, try to correct the interference by using one or more of the following measures:

Move the NetScaler equipment to one side or the other of your equipment.

Move the NetScaler equipment farther away from your equipment.

Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

Last Updated: May 2013

Document code: May 31 2013 01:15:27

Contents

Release Notes

These topics describe enhancements in NetScaler 10.1 nCore and NetScaler 10.1 nCore VPX releases. The nCore NetScaler uses multiple CPU cores for packet handling, which greatly improves the performance of many NetScaler features.

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 10.1 release provides enhancements for the following NetScaler features.

AAA Application Traffic

Two-Factor SAML Authentication

Issue ID 0277562: AAA now supports two-factor SAML authentication. When a user requests a resource, AAA checks for SAML policies. If a SAML policy with two-factor authentication is present, AAA redirects the user to the specified third-party authentication server. Once the user has authenticated and obtained a valid assertion, AAA redirects the user to the secondary login page for the resource.

To enable two-factor SAML authentication, type the following command at the NetScaler command line:

```
> add authentication samlAction <name> -samlTwoFactor ON
```

For more information, see SAML Authentication Policies.

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.

For more information, see Kerberos Protocol Transition and Constrained Delegation.

AAA Kerberos Constrained Delegation (KCD) Support

Issue IDs 0288056, 0307491, and 0329542: The Authentication, Authorization and Auditing (AAA) feature now supports Kerberos Constrained Delegation (KCD). KCD is a new feature in the Kerberos protocol, version 5, that allows the system administrator

to limit the web application services that a specified Kerberos service account can grant users access. The administrator does this by specifying a list of web application services for which the service account is authorized to issue tickets. If a user requests a ticket for a web application that is not on the list, the service account does not issue the ticket. In addition to standard web services, KCD is supported with Microsoft SQL server.

For more information, see Kerberos Protocol Transition and Constrained Delegation.

Extracting Group Credentials from a Third Authentication Server

Issue ID 0308118: When performing two-factor authentication, the AAA feature now supports extraction of the group membership credential from a third authentication server. This function is supported by use of a third authentication chain that is invoked only if the first and second authentication attempts succeed.

To enable extraction of group membership credentials from a third authentication server, create an LDAP policy with authentication disabled. Then, bind that policy to the authentication virtual server, with the -groupExtraction flag set, as shown below.

```
bind authentication vserver <name> [-policy <string> [-
priority <positive_integer>] [-groupExtraction]]
```

If -groupExtraction is set, the policy is an LDAP policy, and the policy has authentication disabled, then the policy is added to the third authentication chain. Otherwise, the binding will fail.

For more information, see Authentication Policies.

LDAP Referral Support

Issue IDs 0327591, 0329887, and 0330819: AAA now supports LDAP referrals. If this feature is enabled, and the NetScaler appliance receives an LDAP_REFERRAL response to a request, AAA follows the referral to the active directory (AD) server contained in the referral and performs the update on that server, First, AAA looks up the referral server in DNS, and connects to that server. If the referral policy requires SSL/TLS, it connects via SSL/TLS. It then binds to the new server with the binddn credentials that it used with the previous server, and performs the operation which generated the referral. This feature is transparent to the user.

LDAP referral support is disabled by default, and must be explicitly enabled for each ldapAction. This feature cannot be turned on globally. The system administrator must also make sure that the AD server accepts the same binddn credentials that are used with the referring (GC) server.

To enable LDAP referrals, type the following commands at the NetScaler command line:

```
set authentication ldapAction <name> -followReferrals ON
set authentication ldapAction <name> -maxLDAPReferrals
<integer>
```

For <integer>, substitute the maximum level of referrals. By default, one referral level is allowed.

For more information, see LDAP Authentication Policies.

Smart Group Option for LDAP Authentication

Issue ID 0357837. When configuring AAA for LDAP, you can now set the default authentication group attribute explicitly, instead of allowing AAA to set the Group attribute from information that it extracts from credentials. In complex organizations that have multiple domains, smart group support allows simpler and more fool-proof implementation of SSO.

To configure the smart group option at the command line, type the following command:

```
set aaa ldapParams -defaultAuthenticationGroup <string>
```

For <string>, substitute the group identifier that you want to use.

To configure the smart group option by using the configuration utility, in the Create Authentication Server or Modify Authentication Server dialog box, fill in the Default Authentication Group text box.

AppExpert

Configure a Persistency Group for Application Units

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.

For more information about configuring a persistency group for the application units in an AppExpert application, see Configuring Persistency Groups for Application Units.

Enhanced Target Support for RefineSearch Parameter in Rewrite

Issue ID 0245438: The RefineSearch and Target parameters can now be used together in a single Rewrite action. The following types of search are supported:

- TCP with regular expressions
- HTTP with regular expressions
- HTTP with XPath expressions
- HTTP body payload expressions

The following expression illustrates how TARGET and the search and refineSearch parameters can be used together to search for and replace all instances of the string

"str" that appears as part of a larger string enclosed in angle brackets with the string "str2":

```
Add rewrite action rewrite-action-1 REPLACE_ALL
'HTTP.REQ.BODY(10000)' 'TARGET + "str2"' -search
'regex(re/my.*str/)' -refineSearch
'EXTEND(10,20).AFTER_STR(">").BEFORE_STR("<")'
```

AppExpert Template for Microsoft Outlook Web Access

Issue ID 0246845: An AppExpert template has been created to help users configure the application firewall to protect a web server that runs Microsoft Outlook Web Access. The template and associated signatures file provide an appropriate default configuration for the application firewall when protecting OWA. The template is posted on the Citrix Community Web Site, and can be downloaded from within the configuration utility, in the main AppExpert pane, by clicking Download AppExpert Templates.

To install the downloaded templates, first extract them from the archive to a temporary location on your local computer. The archive contains four files:

- OWA_Template.xml—The actual template
- OWA_signatures.xml—The associated signatures
- OWA_deployment.xml—The deployment file
- OWA_NS10_what is new.txt—A brief list of changes to the template since the previous version

After you extract the template archive, in the AppExpert pane click Import AppExpert Template to run the AppExpert wizard, and follow the instructions in the Wizard to install the template and create the OWA configuration.

For more information, see AppExpert.

Service and Service Group Configurations Exported to Application Templates

Issue ID 0248273: When you export an AppExpert application, all services and service groups that are part of the application configuration are exported to the deployment file. During import, the appliance compares the deployment file's contents with its own configuration, and manages conflicts in the following way:

- If a service in the file has the same name and service type as a service on the appliance, the appliance does not import the service. It binds the existing service to all the application units created during import.
- If a service in the file has the same name as a service on the appliance, but its service type is different, the appliance does not import the service. It displays a message indicating a protocol mismatch.
- If a service in the file has the IP address and port combination of a service on the appliance, and both services use the same underlying transport protocol (for example, HTTP and SSL services both use TCP), the appliance does not import the service, even if their names are different. It displays a message indicating a port and service type conflict. If the IP address and port combination is same, but the

name and underlying transport protocol are different, the appliance imports the service.

- If a service group in the file has the same name and service type as a service group on the appliance, the appliance does not import the service group. It binds the existing service group to all application units created during import.
- If a service group in the file has the same name as a service group on the appliance, but its service type is different, the appliance does not import the service group. It displays a message indicating a protocol mismatch.

If a conflict is detected during import, the appliance ends the import process and rolls back any configuration changes that were made, preserving the configuration that was in place before the template was imported.

Support for Additional Public Endpoints

Issue ID 0259600: AppExpert applications and the deployment files created from them now support two or more endpoints. However, when importing an AppExpert template file, if you do not include a deployment file, the AppExpert Template Wizard displays a screen on which you can configure a maximum of two public endpoints—one endpoint of type HTTP and one endpoint of type HTTPS—for the application. So, if you want more than two endpoints, you have to configure additional endpoints after you create the application. You can then export the application to obtain a deployment file that contains all the configured endpoints.

For information about importing an AppExpert template, configuring public endpoints after importing an application, and exporting an AppExpert to a template file, see Getting Started with an AppExpert Application.

Rewrite Support for the Diameter Protocol

Issue ID 0318382: The Rewrite feature now supports the Diameter protocol. A number of NetScaler expressions have been added that allow you to examine the header and the attribute-value pairs (AVPs) in a diameter packet. These expressions allow you to look up AVPs by index, ID or name. You can extract information from the header or avp, insert or delete an AVP at a specified index position or at the end of the diameter packet, replace an AVP at a specified index position with a different AVP, and much more.

For more information, see Rewrite and Policies and Expressions.

Responder Support for the Diameter Protocol

Issue ID 0318387: The Responder feature now supports the Diameter protocol. A number of NetScaler expressions have been added that allow you to examine the header and the attribute-value pairs (AVPs) in a diameter packet. These expressions allow you to look up AVPs by index, ID or name, examine the information in the AVP, and send a response based on that information.

For more information, see Rewrite and Policies and Expressions.

AppFlow

Configuring SourceIP for AppFlow Traffic

Issue ID 0288343: You can now specify 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 parameter to associate a net profile to which the source IP address is bound. If you do not set the -netprofile parameter, the Appflow exporter uses the NSIP address as the source IP address.

```
> add appflow collector <col_name> -IPAddress <IP_addr>  [-
netprofile {netprofile_name}]
```

X-Forwarded-For HTTP Header Support

Issue ID 0311033: 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.

Export Multiple Set-cookies in AppFlow Records

Issue ID 0329122: Multiple values of the set-cookie HTTP header can now be exported in AppFlow records.

Application Firewall

Application Firewall Improved Diagnostics and Tracking Tools for Troubleshooting

Issue IDs 0248186, 0266782, 0316311, and 0326638: The application firewall now generates log messages for system resets, packets dropped because of violations of RFC strict checks or malformed request/response header checks, or due to errors within the application firewall itself. These logs provide additional information for troubleshooting.

Application Firewall Scan Tool Integration

Issue IDs 0317580 and 0317582: The Citrix NetScaler Application Firewall now supports signatures generated by the IBM AppScan, Trend Microsystems, and Whitehat vulnerability scanners. You can import Whitehat WASC 1.0, WASC 2.0, and best practices signatures, IBM AppScan Standard and Enterprise signatures, and Trend Microsystems Vulnerability Scanner (TMVS) signatures into the application firewall. These signatures can either be added to existing signatures objects, or can be used to create new signatures objects. Once imported, the signatures can be used to protect web applications exactly like any other signatures.

Once imported, the signatures can be used to protect web applications exactly like any other signatures.

For more information, see Signatures and Updating a Signatures Object from a Supported Vulnerability Scanning Tool.

Application Firewall Signature Enhancements

Issue IDs 0318148 and 0334210: The Citrix NetScaler Application Firewall Signatures feature has received a number of enhancements. The Signatures feature now includes the following new and enhanced functions:

- Automatic updates—You can configure automatic updates for the default application firewall signatures or any signatures object that you have created from a cloud-based service. This feature is disabled by default. You enable and configure it in the configuration utility Signatures pane by selecting the signatures that you want to update, then choosing Auto-Update Settings in the Action drop-down list. If signature updates are enabled, the NetScaler appliance checks the specified URL for updates at the designated interval, hourly by default. If it finds updated signatures, it downloads and installs them.
- Manual per-signature updates—Manual per-signature updates--You can manually update the default application firewall signatures or any signatures object taht you have created by using the command line or the configuration utility. To update signatures from the command line, use the following command:

  ```
  update appfw signatures <name> [-mergeDefault]
  ```

  For <name>, substitute the name of signatures object to update. If you want to merge updates with thhe default signatures, include the -mergeDefault parameter.

  To update signatures by using the configuration utility, in the Signatures pane select the signatures that you want to update, then select Merge from the Action drop-down list. In the Update Signatures Object dialog box, type in the path and name of the signatures update file or use the browse dialog to select it, and then click Update.
- Signature patterns support for JSON payloads—The signatures feature now matches JSON in HTTP requests. You can create patterns that examine JSON payloads for patterns that might signify a security breach on your protected web server or application.
- Signature patterns support for HTTP responses—The signatures feature now matches patterns in the HTTP response as well as the request. You can create patterns that examine HTTP response headers and bodies for patterns that might signify a security breach on your protected web server or application.

  The following new patterns apply specifically to responses:

  - Credit cards
  - Safe objects
- Per-signature counters—Signature statistics are now maintained on a per-signature basis, allowing you to see exactly how many times a specific signature has matched a request or response.

For more information about enhanced Signatures features, see Signatures.

Application Firewall Cluster Support

Issue IDs 0326635 and 0348164: Support for the application firewall has been added to the NetScaler cluster when operated in single node spotted VIP mode. Application

firewall commands run correctly at the command line, and the configuration utility displays the application firewall node and screens. Users should keep in mind that session state sharing between nodes is disabled when using the application firewall on a cluster.

Application Firewall Learning Support on Cluster

Issue IDs 0327601 and 0327602: Support for the application firewall learning feature has been added to the NetScaler cluster. The cluster controller node now aggregates learning data from all nodes in the cluster and stores the learned data in a temporary database file. It then provides the data set to each node in the cluster upon request, enabling the learning feature to operate on the complete set of requests and responses to a protected web server, application, or service.

Application Firewall Performance Improvements

Issue IDs 0327608, 0327613, and 0366700: A number of performance improvements have increased the performance of the application firewall overall by approximately 10%. These improvements include caching of frequently used objects, significant enhancements to processing of HTTP POST bodies, and more efficent Signatures string operations.

HTML Cross-Site Scripting Check Might Transform Allowed Tags and Attributes

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.

Cache Redirection

Cache Redirection Changes

Issue ID 0319966: The following changes have been made in the cache redirection feature:

- The cacheVserver parameter is no longer part of the **add cr vserver** command. To specify a cache server, you must use the **bind cr vserver** –lbvserver <string> command.

  In the configuration utility, in the **Create Virtual Server (Cache Redirection)** and **Configure Virtual Server (Cache Redirection)** dialog boxes, the **Cache Server** list has been renamed to **Default Cache Server** and has been moved from the **Advanced** tab to the area above the tabs. Additionally, a hit counter has been added next to the list. The hit counter maintains a count of the number of hits received by the cache server.

- In the **Create Virtual Server (Cache Redirection)** and **Configure Virtual Server (Cache Redirection)** dialog boxes, on the **Policies** tab, when you click the **CSW** button and then the **Insert Policy** button, the list that appears in the **Policy Name** column no longer includes a **Default** content switching policy.

Issue ID 0330033: You can now bind compression and filter policies to a cache redirection virtual server by using the configuration utility.

To bind a compression or filter policy to a cache redirection virtual server:

1. In the navigation pane, expand **Traffic Management**, expand **Cache Redirection**, and then click **Virtual Servers**.
2. In the details pane, click the cache redirection virtual server to which you want to bind a compression or filter policy, and then click **Open**.
3. In the **Configure Virtual Server (Cache Redirection)** dialog box, on the **Policies** tab, do one of the following:
   - To bind a compression policy, click **Compression**.
   - To bind a filter policy, click **Filter**.
4. Click **Insert Policy**, and then, in the list that appears in the **Policy Name** column, click the policy that you want to bind to the virtual server.
5. Click **OK**.

Cloud Integration

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 AutoScale.

For answers to frequently asked questions, see AutoScale FAQs.

Cluster

Cluster Support for NetScaler Features

The NetScaler cluster now supports the following features:

- Issue ID 0269113: IP-IP Tunneling
- Issue ID 0274535: ISIS routing protocol
- Issue ID 0283450: Branch Repeater load balancing

- Issue ID 0341764: Rate Limiting
- Issue ID 0341764: Action Analytics
- Issue ID 0317324: Content Switching Actions
- Issue ID 0327601: Application Firewall on spotted virtual servers
- Issue ID 0346786: Spillover based on bandwidth
- Issue ID 0317306: AAA-TM on spotted virtual server

Removing a Cluster Node

Issue ID 0291771: You can now remove a cluster node through a single-step procedure. You must log on to the cluster IP address and execute the **rm cluster node** command.

For more information, see Removing a Cluster Node.

Viewing and Clearing Node-Specific Routing Information

Issue ID 0309178: You can now retrieve node-specific routing configurations by specifying the node(s) in the owner-node argument as follows:

```
> vtysh
ns# owner-node 0 1
ns(node-0 1)# show cluster state
ns(node-0 1)# exit-owner-node
```

Similarly, you can also clear node-specific routing configurations by specifying the node(s) in the owner-node argument as follows:

```
> vtysh
ns# owner-node 0 1
ns(node-0 1)# clear config
ns(node-0 1)# exit-owner-node
```

Partially Striped Configurations in a NetScaler Cluster

Issue ID 0335401: You can now define some configurations to be active only on specific cluster nodes. For example, you can define a virtual server to be active on only three nodes of a 5-node cluster. Such a configuration is referred to as *partially striped*. To define a partially striped configuration, use a node group, which is a set of cluster nodes to which you can bind the following virtual servers (load balancing, content switching, cache redirection, and authentication).

Note: An entity that is bound to a node group that includes all the cluster nodes is striped across the cluster. Similarly, an entity that is bound to a node group that includes only one node is spotted on that node.

For more information, see Node Groups and Configuring a Node Group.

Configuring priority for the configuration coordinator

Issue ID 0359806: You can now configure the priority for a cluster node to be selected as a configuration coordinator. The node with the highest priority (lowest priority

number) is made the configuration coordinator. If the current configuration coordinator goes down, the node with the next lowest priority number takes over as the configuration coordinator. If the priority is not set or if there are multiple nodes with the lowest priority number, the configuration coordinator is selected from one of the available nodes.

You can set the node priority by using the priority parameter of the add cluster node command.

Configuration Utility

PHP Version Upgraded from 5.3.10 to 5.3.17

Issue IDs 0333572 and 0334881: PHP has been upgraded from version 5.3.10 to version 5.3.17 on the NetScaler appliance to resolve security vulnerabilities and stability issues with PHP.

NetScaler Configuration Utility

Issue ID 0360658: Features in the NetScaler configuration utility navigation tree have been reorganized to provide greater logical consistency and ease of navigation. The feature nodes are grouped under the following top-level nodes:

- **System**—System and infrastructure features
- **AppExpert**—Grouping of all Application, Policies, templates and Layer 7 features
- **Traffic Management**—Core traffic management features such as load balancing, GSLB, content switching, cache redirection, SSL, and SSL offload
- **Optimization**—Core optimization features such as caching and compression
- **Security**—Security oriented features and functionalities

For more information, see Configuration Utility Changes.

Embedded Java views moved to Overview Pages

Issue ID 0381622: In addition to the reorganization of the nodes within the navigation tree, some of the nodes are now grouped with the configurations options in the details pane (the pane on the right side of the screen) of the configuration utility. For example, LDNS entries, which were a subnode of GSLB, are now with the global GSLB configuration items in the details pane.

The following embedded Java views have been moved to the Overview pages:

- Auto Detected Services Detail View
- FIPS Detail View
- Applications Detail View
- Access Gateway Applications Detail view
- Template Detail view

- GSLB LDNS entries Detail View
- Cache Objects

For more information, see Configuration Utility Changes.

Content Switching

Actions for Content Switching Policies

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 Configuring a Content Switching Action.

Global Setting for Using a Proxy Port

Issue ID 0302646: You can now use the NetScaler user interface to configure the Use Proxy Port setting globally.

For more information, see Configuring the Source Port for Server-Side Connections.

Rename a Content Switching Policy Label

Issue ID 0312929: You can now rename a content switching policy label, even if the label is already referenced by existing policies. The new name is automatically incorporated into all configurations that include the old name.

For more information, see Configuring Content Switching Policy Labels.

Configure Policy Based Logging for Content Switching

Issue ID 0328777: You can configure policy based logging for a content switching policy. Policy based logging enables you to specify a format for log messages. The contents of the log message are defined by using a default syntax expression in the content switching policy. When the content switching action specified in the policy is

performed, the NetScaler appliance constructs the log message from the expression and writes the message to the log file. Policy based logging is particularly useful if you want to test and troubleshoot a configuration in which content switching actions identify the target load balancing virtual server at run time.

For more information about policy based logging for content switching, see Configuring Policy Based Logging for Content Switching.

Rename Content Switching Policies

Issue ID 0329521: You can now rename a content switching policy, even if the policy is bound to a content switching virtual server or policy label. The new name is automatically incorporated into all configurations that include the old name. For example, if the old name was used to bind the policy, you have to use the new name if you want to unbind the policy.

For more information, see Configuring Content Switching Policies.

DataStream

Transparent Mode for Logging MSSQL Transactions

Issue ID 0319464: You can configure the NetScaler appliance to operate transparently between MSSQL clients and servers, and to only log or analyze details of all client-server transactions. Transparent mode is designed so that the NetScaler appliance only forwards MSSQL requests to the server, and then relays the server's responses to the clients. As the requests and responses pass through the appliance, the appliance logs information gathered from them, as specified by the AppFlow configuration, or collects statistics, as specified by the Action Analytics configuration.

For more information, see Logging MSSQL Transactions in the Transparent Mode.

Database Profiles

Issue ID 0343179: You can now configure a database profile for virtual servers of type MSSQL and MYSQL. A database profile is a named collection of parameters that is configured once but applied to multiple virtual servers that require those particular parameter settings. After creating a database profile, you bind it to load balancing or content switching virtual servers. You can create as many profiles as you need.

For more information, see Configuring a Database Profile.

Database Specific Load Balancing of Services

Issue ID 0358254: You can now configure the Citrix NetScaler appliance to retrieve a list of databases that are active on a service and, for a given query, to load balance only the services on which the requested database is available. If the requested database is unavailable on a service, the appliance excludes the service from load balancing decisions until it becomes available. This behavior ensures uninterrupted service to clients.

For more information about database specific load balancing, see Database Specific Load Balancing.

Support for Microsoft SQL Server 2012

Issue ID 0354723: The Citrix NetScaler appliance now supports Microsoft SQL Server 2012. To load balance SQL 2012 database servers, you must set the Server Version (mssqlServerVersion) parameter to `2012` on each of the load balancing and content switching virtual servers in the configuration.

If you have configured availability groups for read-only routing, the appliance can handle the redirect packets with which the primary database server responds to clients who declare read-only application intent in their connection properties. However, when deployed to manage traffic associated with an availability group, the NetScaler appliance provides additional benefits. With the help of content switching policies, the appliance can differentiate between connections in which the `ApplicationIntent` connection property is set to `ReadWrite` and those in which the property is set to `ReadOnly`. A content switching virtual server can then forward all ReadWrite requests to a load balancing virtual server to which you have bound the primary database instance, and all ReadOnly requests to a load balancing virtual server to which you have bound the secondary database servers.

In this configuration, ReadOnly requests are load balanced across all the secondary servers (unlike configurations involving a redirect response, in which only one secondary server is selected for serving ReadOnly requests). In this way, the appliance can optimally utilize all of the secondary database servers while eliminating redirect traffic from your network.

Domain Name System

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.

For more information about offloading DNSSEC operations to the NetScaler appliance, see Offloading DNSSEC Operations to the NetScaler Appliance.

Global Server Load Balancing

View Site Persistence Cookies for GSLB Services

Issue ID 0242446: If site persistence is configured for GSLB services, and the services are bound to a GSLB virtual server, the NetScaler appliance generates a site persistence cookie for each service. Unlike in earlier NetScaler releases, the NetScaler user interface now displays the site persistence cookies that the appliance generates.

To view site persistence cookies by using the NetScaler command line

At the NetScaler command prompt, type:

```
show gslb vserver <name>
```

To view site persistence cookies by using the NetScaler configuration utility

1. In the navigation pane, expand **GSLB**, and then click **Virtual Servers**.
2. In the details pane, select the virtual server for whose services you want to view site persistence cookies, and then click **Open**.
3. In the **Configure GSLB Virtual Server** dialog box, on the **Services** tab, select the service whose site persistence cookie you want to view.

   The site persistence cookie is displayed below the table of services.

Load Balancing

View the Global Spillover Count by Using SNMP

Issue ID 0229026: You can use the totSpilloverCount SNMP counter to retrieve a count of the number of times spillover has occurred on various load balancing and content switching virtual servers after the NetScaler appliance was last restarted. The SNMP OID is 1.3.6.1.4.1.5951.4.1.3.5.6.

Configure Spillover Based on NetScaler Policies

Issue ID 0257226: In earlier NetScaler releases, you can configure spillover by specifying only one of the following spillover methods along with a spillover threshold: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, and HEALTH. Also, of a backup virtual server is not available when spillover occurs, the NetScaler appliance responds to clients with a TCP reset

In this release, you can also use a NetScaler rule, of your choice, to specify the conditions that should be met for spillover to occur. You specify the rule in a spillover policy. Configuring a spillover rule enables you to configure the NetScaler appliance for a wider range of spillover scenarios. For example, you can configure spillover on the basis of the virtual server's response time, or on the basis of the load on the virtual server.

Support for Clearing a Specific Persistence Session

Issue ID 0258312: You can specify a persistence parameter in the "clear lb persistentSessions" command to clear the persistence session associated with only that parameter. Following is the command synopsis for clearing the session associated with a specific persistence parameter:

clear lb persistentSessions [<vServer> [-persistenceParam <string>]]

where

persistenceParam is the persistence parameter whose session you want to clear.

For more information about clearing a specific persistence session, see Clearing Persistence Sessions.

Support for Overriding Persistence for Overloaded Services

Issue ID 0258313: When a service is loaded or is otherwise unavailable, service to clients is degraded. To work around this situation, you might have to configure the NetScaler appliance to temporarily forward to other services the requests that would otherwise be included in the persistence session that is associated with the overloaded service. In other words, you might have to override the persistence setting that is configured for the load balancing virtual server until the service returns to a state in which it can accept requests. You can achieve this functionality by binding a load monitor to the virtual server and setting the “skippersistency” parameter for the virtual server.

For more information about overriding persistence for overloaded services, see Overriding Persistence Settings for Overloaded Services.

Counters for the Number of Active and Inactive Bound Services

Issue ID 0275028: The **stat lb vserver** and **stat gslb vserver** commands, and the **Monitoring** pages for load balancing and global server load balancing virtual servers, now display a count of the number of bound services that are UP and DOWN. The counters are called `actSvcs` (total active services) and `inactSvcs` (total inactive services), respectively.

Rate Statistics for Services Bound to a Load Balancing Virtual Server

Issue ID 0275029: The **stat lb vserver** command and the **Monitoring** page for a load balancing virtual server now display the hit rate (Hits/s), request rate(Req/s), and response rate (Rsp/s) for bound services.

Options for Branch IP Address in the Load Balancing wizard for Citrix Branch Repeater

Issue ID 0275289: In the Static Load Balancing wizard for Citrix 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.

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.

Ability to Specify a Name for a Persistence Cookie

Issue ID 0289773: Unlike in earlier releases, for load balancing virtual servers and load balancing persistency groups for which the COOKIEINSERT persistence type is configured, you can specify a name for the persistency cookie. You specify a name for the persistency cookie by setting the cookieName parameter. If you configure the COOKIEINSERT persistence type, but you do not specify the cookieName parameter, the NetScaler appliance inserts a cookie of the form <NSC_XXXX>= <serviceIP> <servicePort>, where <NSC_XXXX> is the virtual-server ID that is derived from the virtual server's name, <serviceIP> is the hexadecimal value of the IP address of the service, and <servicePort> is the hexadecimal value of the port of the service.

To specify a name for the persistence cookie for a load balancing virtual server by using the NetScaler command line

At the NetScaler command prompt, type:

- **set lb vserver** <name> -cookieName <string>

To specify a name for the persistence cookie for a load balancing virtual server by using the configuration utility

1. In the navigation pane, expand **Traffic Management**, expand **Load Balancing**, and then click **Virtual Servers**.
2. In the details pane, click the name of the virtual server for which you want specify a persistence cookie name, and then click **Open**.
3. In the **Configure Virtual Server (Load Balancing)** dialog box, click the **Method and Persistence** tab.
4. In the **Cookie Name** text box, type a name for the persistence cookie.
5. Click **OK**.

To specify a persistence cookie for a load balancing persistency group by using the NetScaler command line

At the NetScaler command prompt, type:

- **set lb group** <name> -cookieName <string>

To specify a name for the persistence cookie for a load balancing persistency group by using the configuration utility

1. In the navigation pane, expand **Traffic Management**, expand **Load Balancing**, and then click **Persistency Groups**.
2. In the details pane, click the name of the persistency group for which you want specify a persistence cookie name, and then click **Open**.
3. In the **Configure Persistency Group** dialog box, in the **Cookie Name** text box, type a name for the persistence cookie.

4. Click **OK**.

Diameter Expression Support

Issue IDs 0318377 and 0318381: Expressions to retrieve AVPs from a Diameter request or response are now available. You can use these expressions for configuring the token load balancing method and for rule-based persistency.

The expressions are of the form DIAMETER.REQ.AVP(<avpcode>). For example, to retrieve the Auth-Application-Id AVP (AVP code 258), you can use the expression: `DIAMETER.REQ.AVP(258)`.

Some important AVPs have aliases. For example, the Auth-Application_Id AVP has the alias AUTH_APPLICATION_ID. So, the expression to retrieve the Auth-Application_Id by using the alias is: `DIAMETER.REQ.AUTH_APPLICATION_ID`.

Increase in the Maximum Number of Persistence Sessions

Issue ID 0328498: The maximum number of persistence sessions per core on an nCore NetScaler appliance has been raised from 150,000 to 1,000,000 (1 million). The maximum number of persistence sessions that can coexist on an nCore NetScaler appliance is equal to the product of the number of cores and the per-core limit. For example, if the appliance has 6 CPU cores, the maximum number of persistence sessions that can coexist on the appliance is 6,000,000 (6 * 1000000).

For information about how to configure a limit for the number of persistence sessions that can coexist on the NetScaler appliance, see Configuring the Limit for Number of Persistence Sessions on the NetScaler Appliance.

Dynamic Load Balancing of Repeater Appliances

Issue ID 0333238: You can now configure the NetScaler appliance for dynamic load balancing of Repeater appliances, by using the Dynamic Load Balancing wizard for Citrix Branch Repeater. In the wizard, you specify the datacenter Repeater IP addresses and the datacenter server subnets to which the NetScaler appliance or instance must forward the branch-office traffic. The wizard creates the required configuration.

The wizard enables the load balancing feature and creates the following two virtual servers:

- One MAC-mode wildcard load balancing virtual server of type `ANY`, to load balance datacenter Repeater appliances. This virtual server uses a listen policy to identify traffic that arrives from a Branch Repeater, and implements rule based persistence on the basis of the Branch Repeater IP address included in the TCP options. Traffic received by this virtual server is accelerated. The listen policy for this virtual server has a higher priority than does the policy for the other virtual server.
- One MAC-mode wildcard load balancing virtual server of type `ANY`, to manage server-initiated connections, such as active FTP connections. This virtual server also accepts branch-office traffic that arrives without Branch Repeater parameters in the TCP options. Branch Repeater parameters might not be set if

the source Branch Repeater has an invalid license, acceleration is disabled, and so on. The virtual server implements `SRCIPDSTIP` persistence.

For both virtual servers, the wizard enables the L2Conn parameter and sets the skippersistency parameter to Bypass. When L2Conn is enabled on a virtual server, Layer 2 parameters (channel number, MAC address, and VLAN ID) are used to identify a connection. That is, they are used in addition to the `<source IP>:<source port>::<destination IP>:<destination port>` 4-tuple, enabling multiple connections with the same 4-tuple to coexist on the NetScaler appliance. The Bypass setting for skippersistency enables the virtual servers to bridge requests through to the physical servers, on the basis of the destination IP address in the request, whenever a data center Repeater appliance is overloaded. The wizard also does the following:

- Creates Access Control Lists (ACLs), to process only TCP traffic and bridge non-TCP traffic directly to the destination servers.
- Creates a forwarding session for each server subnet, to forward traffic processed by a Repeater appliance to the destination server. A forwarding session also ensures that a response returns along the path taken by the request.
- Creates NetScaler entities (metric tables and monitors) required for monitoring the load on the Repeaters.
- Enables MAC-based forwarding (MBF), to skip ARP/routing table lookup and forward packets to the Repeaters by using cached MAC addresses.
- Enables Layer 3 (L3) forwarding mode, for IP forwarding.
- Enables Use Source IP (USIP) mode, to use the client's IP address as the source IP address when the NetScaler appliance initiates a connection to a Repeater appliance.
- Configures values for idle timeouts, for any client or server, globally. The configured timeout values are large enough so that the appliance does not prematurely terminate idle connections (such as ICA and Telnet connections) that must be kept open for long periods of time.
- Sets the preferDirectRoute load balancing parameter to NO, so that the NetScaler appliance forwards packets to the Repeater appliances instead of looking up configured routes (if any).

To configure dynamic load balancing of Repeater appliances

1. In the navigation pane, expand **Traffic Management**, and then click **Load Balancing**.
2. In the details pane, click **Dynamic Load Balancing wizard for Citrix Branch Repeater**.
3. Follow the instructions in the wizard to complete the configuration.

Ability to Configure VLAN Transparency

Issue ID 0361552: You can now configure a load balancing virtual server to retain the client's VLAN identifier in packets that are to be forwarded to servers. The virtual

server must be a wildcard virtual server of type ANY, and must be functioning in MAC mode.

For instructions, see Retaining the VLAN Identifier for VLAN Transparency.

Automatic State Transition Based on Percentage Health of Bound Services

Issue ID 0361659: You can now configure a load balancing virtual server to automatically transition from the UP state to the DOWN state if the percentage of active services falls below a configured threshold. For example, if you bind 10 services to a load balancing virtual server and configure a threshold of 50% for that virtual server, it transitions from UP to DOWN if six or more services are DOWN. When the percentage health rises above the threshold value, the virtual server returns to the UP state. You can also enable an SNMP alarm called ENTITY-STATE if you want the NetScaler appliance to notify you when the percentage health of bound services causes a virtual server to change state.

For instructions, see Configuring Automatic State Transition Based on Percentage Health of Bound Services.

Monitor for Citrix StoreFront Stores

Issue ID 0366050: You can now configure a user monitor for a Citrix Storefront store.

For more information about monitoring a StoreFront store, see Monitoring Citrix StoreFront Stores.

Monitor for Accounting Information Delivery from a RADIUS Server

Issue ID 0348828: You can now configure a monitor called a *RADIUS accounting* monitor to determine whether the Radius server used for Authentication, Authorization, and Accounting (AAA) is delivering accounting information as expected.

For more information about monitoring accounting information delivery from a RADIUS server, see Monitoring Accounting Information Delivery from a RADIUS Server.

Load Balancing and AAA

Native Windows Authentication (Kerberos) for MSSQL Monitors

Issue ID 0329542: Microsoft SQL monitors on the NetScaler appliance now support the Kerberos authentication protocol, and can therefore monitor load-balanced application servers in a Kerberos 5 environment that employs Kerberos Protocol Transition (KPT) and Kerberos Constrained Delegation (KCD).

For more information, see Kerberos Protocol Transition and Constrained Delegation.

NetScaler SDX Appliance

Retrieving Tech Support tar file of Instances from Management Service Utility

Issue ID 0240391: Now you can generate support tar archive for instances running on SDX through the Management Service utility.

Display the Mapping of virtual interfaces on the VPX instance to the physical interfaces on the NetScaler SDX Appliance

Issue ID 0261346: If you log on to the NetScaler virtual instance, the configuration utility and the command line interface display the mapping of the virtual interfaces on the instance to the physical interfaces on the appliance.

For more information, see "Display the Mapping of Virtual Interfaces on the VPX Instance to the Physical Interfaces on the NetScaler SDX Appliance" in Managing Interfaces.

Support for System Notifications

Issue ID 0291016: You can now configure Syslog, mail, and SMS notifications on the SDX appliance.

For more information about Syslog notifications, see Configuring Syslog Notifications.

For more information about mail notifications, see Configuring Mail Notifications.

For more information about SMS notifications, see Configuring SMS Notifications.

Support of Regular Expressions for Search Text Fields

Issue ID 0309358: The Search text fields on the pagination views of the Management Service utility now support regular expressions.

Cluster of NetScaler Instances Provisioned on NetScaler SDX Appliances

Issue ID 0317258: You can now create a cluster of NetScaler instances that are provisioned on the NetScaler SDX appliance. The instances can be available on the same SDX appliance or on any SDX appliance within the same subnet.

For more information, see Setting up a Cluster of NetScaler Instances.

Configuring VLANs on Management Interfaces

Issue ID 0318609: You can now configure a VLAN on the management interfaces, 0/1 and 0/2, while provisioning a NetScaler instance.

Password Management on the 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.

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.

Audit Templates for NetScaler Instances

Issue ID 0322404: You can create an audit template by copying the commands from an existing configuration file. You can later use this template to find any changes in the configuration of an instance and take corrective action if required.

Changing the Hostname of the Appliance

Issue ID 0323534: You can now change the hostname of the Management Service. On the **Configuration** tab, navigate to **System**>**System Settings**>**Change Hostname**, and enter a new hostname.

Simplification of NetScaler SDX Licensing Process

Issue ID 0323681: The process of allocating your licenses has been greatly simplified. The new licensing framework allows you to focus on getting maximum value from Citrix products.

In the Management Service configuration utility (GUI), you can use your hardware serial number (HSN) or your license activation code (LAC) to allocate your licenses. Alternatively, if a license is already present on your local computer, you can upload it to the appliance.

Restrict a VLAN to a Specific Virtual Interface

Issue ID 0323926: The NetScaler SDX appliance administrator can enforce specific 802.1Q VLANs on the virtual interfaces associated with NetScaler instances. This capability is especially helpful in restricting the usage of 802.1Q VLANs by the instance administrators. If two instances belonging to two different companies are hosted on an SDX appliance, you can restrict the two companies from using the same VLAN ID, so that one company does not see the other company's traffic. If an instance administrator, while provisioning or modifying a VPX instance, tries to assign an interface to an 802.1Q VLAN, a validation is performed to verify that the VLAN ID specified is part of the allowed list.

For more information, see Restricting VLANs to Specific Virtual Interfaces.

MAC-Address Assignment by System Administrator

Issue ID 0325507: If, while you are provisioning a NetScaler instance on an SDX appliance, XenServer internally assigns a MAC address to a virtual interface associated with that instance, the same MAC address might be assigned to a virtual interface associated with another instance on the same appliance or on another appliance. To prevent assignment of duplicate MAC addresses, you can enforce unique MAC addresses.

For more information, see Assigning a MAC Address to an Interface.

Support for SNMPv3 Queries on the NetScaler SDX Appliance

Issue ID 0328392: Simple Network Management Protocol Version 3 (SNMPv3) queries are now supported on the NetScaler SDX appliance. SNMPv3 enhances the basic architecture of SNMPv1 and SNMPv2 to incorporate administration and security capabilities, such as authentication, access control, data integrity check, data origin verification, message timeliness check, and data confidentiality.

For more information, see Configuring the NetScaler for SNMPv3 Queries.

Networking

TFTP Support

Issue ID 0250958: The NetScaler appliance now supports communication between a client and a Trivial File Transfer Protocol (TFTP) server.

TFTP is a simple form of file transfer protocol and is based on the UDP protocol. TFTP does not provide any security features and is generally used for automated transfer of configuration and boot files between devices in a private network. TFTP support on the NetScaler appliance is compliant with RFC 1350. A server listens on port 69 for any TFTP request.

The following features are supported:

1. **Load balancing of TFTP servers**—The NetScaler appliance can now load balance TFTP servers.
2. **INAT processing compliant to TFTP**—When a request packet, with port 69 as the destination, received by the NetScaler appliance matches an INAT rule with **TFTP** option enabled, the appliance processes the request and the corresponding response as compliant with the TFTP protocol.
3. **RNAT processing compliant to TFTP**—When a request packet generated by a server is destined to a TFTP server, and the packet matches an RNAT rule on the NetScaler appliance, the appliance's processing of the request and the corresponding response from the TFTP server is compliant with the TFTP protocol.

Configure 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.

Clearing all Dynamic Routing Configurations

Issue ID 0285913: You can now at once clear all the routing configurations, which you created by using the VTYSH shell.

For clearing all the dynamic routing configurations, you run the clear config command in the Exec mode of the VTYSH shell. After clearing the configuration, you must run the write command in the VTYSH shell to save the changes.

IPv6 Protocol Compliance

The following features are supported with respect to the IPv6 protocol compliance:

- Issue ID 0286580: The appliance accepts all the ICMPv6 fragments of an ICMPv6 echo request that is destined to one of the NetScaler owned IPv6 address. The appliance also sends out all the ICMPv6 fragments of the corresponding ICMv6 echo response.
- Issue ID 0286577: You can configure multiple link-local addresses as type SNIP6. A link-local SNIP6 address can be bound to only one VLAN, and a VLAN can have only one link-local SNIP6 address. Because NetScaler owned IP addresses are of type floating, the link-local SNIP6 address bound to a VLAN is associated with all the interfaces bound to the VLAN. Any Neighbor Discovery for IPv6 (ND6) traffic going out of the interface is sourced as the link-local address associated with the interface, as specified by RFC 4861.
- Issue ID 0286578: The NetScaler appliance in L3 mode can now send out periodic Router Advertisement (RA) messages from its advertising interfaces. The appliance also sends RA messages in response to valid solicitations messages. The outgoing RA messages sent by the NetScaler appliance are compliant with RFC 4861 for Neighbor Discovery protocol for IP version 6 (IPv6). The NetScaler appliance can also send redirect messages to inform an originating host of a better router for reaching a specific destination.

Viewing the Details for an LACP channel

Issue ID 0288450: The show channel command now displays the LACP details such as (Port ID, Mux, Rx, Partner) for an LA channel created by using the LACP protocol.

Block Non-Session Packets

Issue ID 0289276: You can configure the NetScaler appliance to drop any non-session packet that it receives, that is, to drop any packet that does not belong to an established connections on the NetScaler appliance, including packets used for establishing new connections.

This feature can be useful in the following cases:

- To prevent security attacks based on non-session traffic
- To accommodate a use case requiring that no new connection requests to be accepted by the NetScaler appliance

To block any non-session packet, set the fwmode (**Network firewall mode**) parameter to EXTENDEDPLUS or FULL in one of the following ways:

- On the NetScaler command line, by running the **set ns config** command.
- In the configuration utility, by using the **Configure Network firewall mode settings** dialog box (System > Settings >Change Network firewall mode).

The NetScaler appliance ignores the fwmode= EXTENDEDPLUS setting for a non-session packet that matches the conditions specified in an extended ACL entry for which the action is ALLOW. In other words, Extended ACLs specifying the ALLOW action override the fwmode= EXTENDEDPLUS setting. For example, if the fwmode parameter is set to EXTENDEDPLUS, and an extended ACL with action and srcip parameters set to ALLOW and 192.0.2.0, respectively, is configured onthe appliance, any non-session packet matching the condition specified in the ACL is allowed onto the NetScaler appliance.

ACL Action in the ACL Log Messages

Issue ID 0290631: Each ACL log entry now includes a field that displays the action set for the ACL. This field tells you whether the packet that hit the ACL was passed onto the NetScaler appliance or was dropped.

The field takes one of the following values:

- ALLOW: A packet that matches the conditions specified in the ACL and is passed onto the NetScaler appliance.
- DENY: A packet that matches the conditions specified in the ACL and is dropped.

Following are two sample log entries:

```
19) 01/23/2013:18:48:53 GMT  Informational 0-PPE-0 : ACL
ACL_PKT_LOG 212 0 :  Source 10.102.56.26
--> Destination 10.102.56.40 - Protocol ICMP -Type 8 - Code 0
-TimeStamp 92612208(ms) - Hitcount 5 -
Hit Rule ACL1 - Action ALLOW - Data 08 00 51 ac 7e 73 00 5c
19 c4 ff 50 19 6c 0a 00 08 09 0a 0b 0c 0d 0e
0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22
23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31
32 33 34 35 36 37

20) 01/23/2013:18:48:58 GMT  Informational 0-PPE-0 : ACL
ACL_PKT_LOG 213 0 :  Source 10.102.56.99
--> Destination 10.102.56.45 - Protocol ICMP -Type 8 - Code 0
-TimeStamp 92617209(ms) - Hitcount 6 -
Hit Rule ACL2 - Action DENY - Data 08 00 c6 a6 7e 73 00 61 1e
c4 ff 50 9f 6c 0a 00 08 09 0a 0b 0c 0d 0e
0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22
23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31
32 33 34 35 36 37
```

Block Fragmented Packets

Issue ID 0299298: You can now configure the NetScaler appliance to drop any fragmented packets that it receives.

This feature can be useful in the following cases:

- To preventing security attacks based on fragmented packets
- To accommodate a use case requiring that the NetScaler appliance accept no fragmented packets.

To block any fragmented packet, enable the **Dropipfragments** (**Drop IP Fragments**) option in one of the following ways:

- On the NetScaler command line, by running the **set L3 param** command.
- In the configuration utility, by using the **Configure Layer 3 Parameters** dialog box (Network > Settings > Configure Layer 3 Parameters).

The **Dropipfragments** (**Drop IP Fragments**) option is also enabled automatically, when you set the fwmode (**Network firewall mode**) parameter to EXTENDED or EXTENDEDPLUS or FULL in one of the following ways:

- On the NetScaler command line, by running the **set ns config** command.
- In the configuration utility, by using the **Configure Network firewall mode settings** dialog box (System > Settings >Change Network firewall mode).

The following table lists the resulting setting of the Dropipfragments option for various combinations of Dropipfragments and fwmode settings.

Existing settings	Changes to the settings	Resulting settings
Dropipfragments = Disabled fwmode = None	fwmode = EXTENDED or EXTENDEDPLUS or FULL	Dropipfragments = Enabled
Dropipfragments = Disabled fwmode = None	Dropipfragments = Disabled	Dropipfragments = Enabled
Dropipfragments = Enabled fwmode = EXTENDED or EXTENDEDPLUS or FULL	Dropipfragments = Disabled	Dropipfragment = Disabled The remaining functions of the mode set to the fwmode parameter will work as expected.
Dropipfragments = Enabled fwmode = EXTENDED or EXTENDEDPLUS or FULL	fwmode = None	Dropipfragment = Disabled

Set Interval for Generating ACL Log Messages

Issue ID 0301716: You can now set the interval at which a log message is to be generated by the NetScaler appliance for a particular flow that matches an extended ACL configured on the appliance.

To set the interval, set the AclLogTime (**ACL Log Time**) parameter in one of the following ways:

- On the NetScaler command line, by running the **set L3 param** command.
- In the configuration utility, by using the **Configure Layer 3 Parameters** dialog box (Network > Settings > Configure Layer 3 Parameters).

AclLogTime (**ACL Log Time**) parameter is set to 1 sec (1 second) when you set the fwmode (**Network firewall mode**) parameter to EXTENDED or EXTENDEDPLUS or FULL in one of the following ways:

- On the NetScaler command line, by running the **set ns config** command.
- In the configuration utility, by using the **Configure Network firewall mode settings** dialog box (System > Settings >Change Network firewall mode).

The following table displays the resulting setting for the AclLogTime option for various combinations of AclLogTime and fwmode settings.

Existing settings	Changes to the settings	Resulting settings
AclLogTime = A secs fwmode = None	fwmode = EXTENDED or EXTENDEDPLUS or FULL	AclLogTime = 1 sec
AclLogTime = A secs fwmode = None	AclLogTime = B secs	AclLogTime = B secs
AclLogTime = 1 secs fwmode = EXTENDED or EXTENDEDPLUS or FULL	AclLogTime = B secs	AclLogTime = B secs
AclLogTime = A secs fwmode = EXTENDED or EXTENDEDPLUS or FULL	fwmode = None	AclLogTime = 5 secs (default value)

Stateful NAT64 Translation

Issue ID 0316933: The stateful NAT64 feature enables communication between IPv4 clients and IPv6 servers through IPv6 to IPv4 packet translation, and vice versa, while maintaining session information on the NetScaler appliance.

A stateful NAT64 configuration on the NetScaler appliance has the following components:

- **NAT64 rule**: An entry consisting of an ACL6 rule and a netprofile, which consists of a pool of NetScaler owned SNIPs.
- **NAT64 IPv6 Prefix**: A global IPv6 prefix of length 96 bits (128-32=96) configured on the appliance.

When an IPv6 request packet received by the NetScaler appliance matches an ACL6 defined in a NAT64 rule and the destination IP of the packet matches the NAT64 IPv6 prefix, the NetScaler appliance considers the IPv6 packet for translation.

The appliance translates this IPv6 packet to an IPv4 packet with a source IP address matching one of the IP address in the netprofile defined in the NAT64 rule, and a destination IP address consisting of the last 32 bits of the destination IPv6 address of the IPv6 request packet. The NetScaler appliance creates a session and forwards the packet to the IPv4 server. Subsequent responses from the IPv4 server and requests from the IPv6 client are translated accordingly by the appliance for the duration of the session.

Configure Traffic Domains

Issue ID 0319241: Traffic domains are a way to segment network traffic for different applications. You can use traffic domains to create multiple isolated environments within a NetScaler appliance. An application belonging to a specific traffic domain communicates with entities and processes traffic within that domain. The traffic belonging to one traffic domain cannot cross the boundary of another traffic domain.

The main benefits of using traffic domains on the NetScaler appliance are the following:

- **Use of duplicate IP addresses in a Network**—Traffic domains allow you to assign the same IP address or network address to multiple devices on a network, or multiple entities on a NetScaler appliance, as long as each of the duplicate address belongs to a different traffic domain.
- **Use of Duplicate entities on the NetScaler appliance**—Traffic domains allow you to use duplicate NetScaler feature entities on the appliance. You can create entities with the same settings as long as each entity is assigned to a separate traffic domain.
- **Multitenency**—Using traffic domains, you can provide hosting services for multiple customers by isolating each customer's type of application traffic within a defined address space on the network.

Block Non-IP Packets

Issue ID 0329548: You can configure the NetScaler appliance to drop any non-IP related packet that it receives. For example, you can drop ARP packets. This feature can be useful in the following cases:

- To prevent security attacks based on non-IP traffic
- To prevent very heavy non-IP traffic from affecting the performance of the appliance

To block non-IP traffic, set the fwmode (**Network firewall mode**) parameter to FULL in one of the following ways:

- On the NetScaler command line, by running the **set ns config** command.
- In the configuration utility, by using the **Configure Network firewall mode settings** dialog box (System > Settings >Change Network firewall mode).

Powering off an Interface

Issue ID 0338863: Now, when you disable an interface or an LA channel, the NetScaler appliance powers off the interface or interfaces of the LA channel and sends a link-down message to the peer device to notify that the interface(s) are disabled.

Controlling the L2 Conn Behavior of Load Balancing Virtual Servers

Issue ID 0339846: 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

NITRO API

Find Virtual Servers to which a Service is bound

Issue ID 0257279: You can now get a list of all virtual servers to which a service is bound.

Log Support

Issue ID 0328051: All NITRO operations are now logged in the /var/nitro/nitro.log file on the appliance.

Unlicensed Feature Handling

Issue ID 0328055: NITRO operations are now restricted to the features that are licensed on the NetScaler appliance.

Policies

HTTP Callouts

The following enhancements have been made for HTTP callouts:

- Issue ID 0215794: HTTP callouts now support IPv6 addresses.
- Issue ID 0233253: HTTP callout responses can now be cached for a specified time duration.

  For more information, see Caching HTTP Callout Responses.
- Issue ID 0317392: HTTP callouts can now generate HTTPS requests. When configuring the HTTP callout, you must set the scheme parameter of the **set policy httpCallout** command.
- Issue ID 0340586: You can now specify an expression that produces a body of the HTTP callout. The expression must be specified in the -bodyExpr parameter of the

set httpCallout command. A “Content-Length” header is automatically added with an appropriate value indicating that the request message contains a body. You can use the **unset httpCallout** command with the -bodyExpr parameter when you do not want to use the body expression for the HTTP callout.

Support for Hashing Text Strings

Issue ID 0236496: You can now hash text strings by using the following algorithms: MD2, MD4, MD5, SHA1, SHA224, SHA256, SHA384, and SHA512. The method provided for this purpose is DIGEST(algorithm) and it can be used on text strings. For example, to hash the body of a HTTP request by using MD5 algorithm, the expression is: HTTP.REQ.BODY(1000).DIGEST(MD5)

TCP Level Expressions

Issue ID 0236816: You can now get the smoothed round trip time and the bandwidth of TCP connections for the client and server by using the following expressions:

- CLIENT.TCP.SMOOTHRTT
- CLIENT.TCP.BANDWIDTH
- SERVER.TCP. SMOOTHRTT
- SERVER.TCP.BANDWIDTH

Get Information of RPC Request

Issue ID 0320216: You can now get information about an RPC request by using the following expressions:

- MSSQL.REQ.RPC.BODY—Returns the body of the SQL request as a string in the form of parameters represented as "a=b" clauses separated by commas, where "a" is the RPC parameter name and "b" is its value.
- MSSQL.REQ.RPC.BODY(n)—Returns part of the body of the SQL request as a string in the form of parameters represented as "a=b" clauses separated by commas, where "a" is the RPC parameter name and "b" is its value. Parameters are returned from only the first “n” bytes of the request, skipping the SQL header. Only complete name-value pairs are returned.

Both expressions return text data, on which any text operation can be performed.

Statistics

Clearing Statistical Counters

Issue IDs 0228298 and 0241836: You can now clear the counters that are displayed by the configuration utility's Dashboard and by stat commands in the NetScaler command-line interface. Clearing a counter resets it to zero, from which point it is incremented as the appliance processes traffic. You can clear the counters regardless of whether the NetScaler appliance is currently processing traffic. The ability to clear counters enables you to observe them over a specific period of time and troubleshoot the configuration.

SSL

Add a Certificate Bundle

Issue ID 0236585: You can 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.

Configuring SSL Close-notify at the Entity Level

Issue ID 0257122: Although the global sendCloseNotify parameter must be set to YES if any entity is to send an SSL close-notify, an entity no longer has to inherit this setting from the global settings. You can set the sendCloseNotify 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.

Restrict the Root CA's distinguished names (DN) sent by the NetScaler Appliance

Issue ID 0262041: As a part of the SSL handshake, in the **Certificate Request** message during client authentication, the server lists the distinguished names (DNs) of all the certificate authorities (CAs) bound to the server from which it will accept a client certificate. If you do not want the DN name of a specific CA certificate to be sent to the SSL client, set the `skipCA` flag. This setting indicates that the particular CA certificate's distinguished name should not be sent to the SSL client.

Support for TLS1.1 and TLS 1.2

Issue ID 0271648: The SSL virtual server on the NetScaler appliance supports TLS1.1 and TLS1.2 protocol based clients. These protocols helps prevent Browser Exploit Against SSL/TLS (BEAST) attacks.

For more information about this protocol, see https://tools.ietf.org/html/rfc5246.

The following ciphers support the TLS1.1 and TLS1.2 protocol:

- SSL3-RC4-MD5
- SSL3-RC4-SHA
- SSL3-DES-CBC3-SHA
- TLS1-AES-256-CBC-SHA
- TLS1-AES-128-CBC-SHA
- SSL3-EDH-RSA-DES-CBC3-SHA
- TLS1-DHE-RSA-AES-256-CBC-SHA
- TLS1-DHE-RSA-AES-128-CBC-SHA

The following ciphers support the TLSv1.1 protocol:

- SSL3-DES-CBC-SHA

- SSL3-EDH-RSA-DES-CBC-SHA
- SSL3-ADH-RC4-MD5
- SSL3-ADH-DES-CBC-SHA
- SSL3-ADH-DES-CBC3-SHA
- TLS1-ADH-AES-128-CBC-SHA
- TLS1-ADH-AES-256-CBC-SHA

Support for SPDY in SSL

Issue ID 0284270: The NPN extension is now supported on the NetScaler appliance.

Certificate Expiry Monitoring

Issue ID 0351522: The certificate expiry monitoring option is now enabled by default, and the default expiry notification period is set to 30 days.

System

Public Key Authentication for Non-nsroot Users

Issue ID 0209190: All NetScaler users can now access the NetScaler appliance by using public key authentication in SSH.

Enabling CallHome Feature while Upgrading the NetScaler Appliance

Issue ID 0311617: While upgrading the NetScaler appliance from an older release to release 10.1 or later, the NetScaler appliance prompts you to enable the CallHome feature in one of the following cases:

- The CallHome feature is not supported in the older release.
- The CallHome feature is disabled in the older release.

Send Buffer Support for TCP Profiles

Issue ID 0315625: You can now set the window that is advertised to the server by using the sendBuffsize parameter of the **set ns tcpProfile**.

New Parameters for Web Interface Site

Issue ID 0317793: The following parameters are added for a web interface site:

- For the **add wi site** command:
  - welcomeMessage. Localized welcome message that appears on the welcome area of the login screen.
  - footerText. Localized text that appears in the footer area of all pages.
  - loginSysMessage. Localized text that appears at the bottom of the main content area of the login screen.

- appWelcomeMessage. Localized text that appears at the top of the main content area of the applications screen.
- preLoginButton. Localized text that appears as the name of the pre-login message confirmation button.
- preLoginMessage. Localized text that appears on the pre-login message page.
- preLoginTitle. Localized text that appears as the title of the pre-login message page.
- showSearch. Enables the Search option on XenApp websites.
- showRefresh. Provides the Refresh button on the applications screen.
- wiUserInterfaceModes. Appearance of the login screen.
  - Simple - Only the login fields for the selected authentication method are displayed.
  - Advanced - Displays the navigation bar, which provides access to the pre-login messages and preferences screens.
- userInterfaceLayouts. Specifies whether or not to use the compact user interface.
- domainSelection. Domain names listed on the login screen for explicit authentication.

- For the **bind wi site** command:
  - farmName. Name for the logical representation of a XenApp or XenDesktop farm to be bound to the Web Interface site.
  - groups. Active Directory groups that are permitted to enumerate resources from server farms. Including a setting for this parameter activates the user roaming feature. A maximum of 512 user groups can be specified for each farm defined with the Farm<n> parameter. The groups must be comma separated.
  - recoveryFarm. Binded farm is set as a recovery farm.

User Name and Password Length Extended to 127 Characters

Issue ID 0325421: User names and passwords on the NetScaler appliance can now be up to 127 characters in length. Usernames and passwords can consist of upper-case and lower-case letters, digits, and the hyphen and underscore characters.

SPDY Support

Issue ID 0329671: NetScaler appliances can now support SPDY. You have to enable SPDY in an HTTP profile and bind the profile to a virtual server. When SPDY is enabled, the virtual server functions as a SPDY gateway and converts SPDY requests from the clients into HTTP requests that it sends to the servers. It also converts the HTTP responses from the servers to SDPY responses that it sends to the clients. The servers do not have to support SPDY. You can enable SPDY in an HTTP profile by using the **set ns httpprofile - SPDY enabled** command or by using the configuration utility.

Note: SSL is required for SPDY protocol to function.

SNMP Enhancements

Issue IDs 0339095, 0356223, and 0362132: The following changes are available with respect to SNMP:

- The owner node for the SNMP engine can be set in a cluster. Use the ownerNode parameter of the **set SNMP engineID** command.
- SNMP statistics can be cleared by using the clearstats parameter of the **stat snmp** command.
- SNMP counters for IPv6 are added.

Configuration Utility Changes

In release 10.1, the NetScaler configuration utility has a new look. The navigation tree is reorganized and grouped according to the major features of the NetScaler appliance. The action buttons have been moved to the top of the screen, and additional actions are now in a drop-down list. Some of the subnodes are also moved to the right pane of the configuration utility.

Note: In edocs, only topics that have been updated or added in the current release reflect the interface changes. For other topics, see the "Node Mapping table" below to map the former top-level nodes to their new locations.

Navigation Tree Reorganization

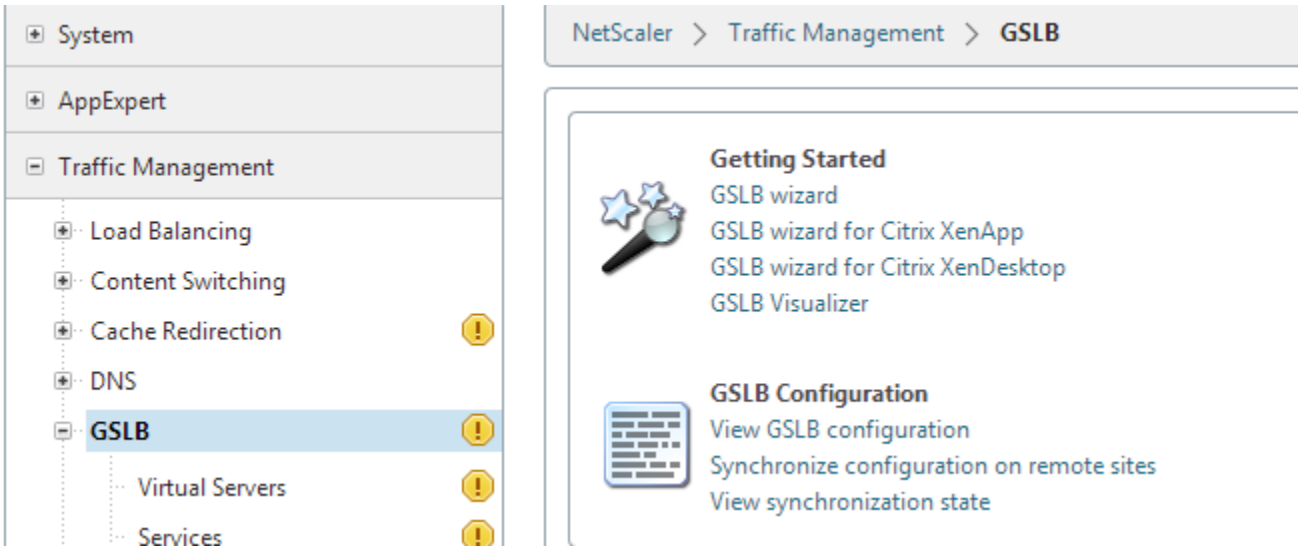
The nodes in the configuration utility are grouped by feature area, in the same way that feature documentation is organized in eDocs. The top-level nodes in the navigation tree of the configuration utility are **System**, **AppExpert**, **Traffic Management**, **Optimization** and **Security**. The following table shows the new location of nodes that were formerly at the top-level.

Table 1-1. Node mapping table

Top-level nodes in the previous version of configuration utility	Location of the nodes in current configuration utility
Network	System > Network
Group	System > User Administration
Users	System > User Administration
Database Users	System > User Administration
command policies	System > User Administration
edgesight monitoring	System > EdgeSight Monitoring

Top-level nodes in the previous version of configuration utility	Location of the nodes in current configuration utility
Network	System > Network
CloudBridge	System > Cloud bridge
Web interface	System > Web Interface
Rewrite	AppExpert > Rewrite
Responder	AppExpert > Responder
Load Balancing	Traffic Management > Load balancing
Content Switching	Traffic Management > Content Switching
Cache Redirection	Traffic Management > Cache Redirection
DNS	Traffic Management > DNS
GSLB	Traffic Management > GSLB
SSL	Traffic Management > SSL
SSL Offload	Traffic Management > SSL Offload
HTTP Compression	Optimization > HTTP Compression
Integrated Caching	Optimization > Integrated Caching
AAA-Application traffic	Security > AAA-Application traffic
Application Firewall	Security > Application Firewall
Protection features	Security > Protection features
Other changes	
GSLB > Location	AppExpert > Location

In addition to the reorganization of the nodes within the navigation tree, some of the nodes are now grouped along with the configurations options present in the right pane of the configuration utility. For example, **LDNS Entries** which was earlier present as a sub-node of GSLB, is now grouped along with the global GSLB configurations present in the details pane of the configuration utility.



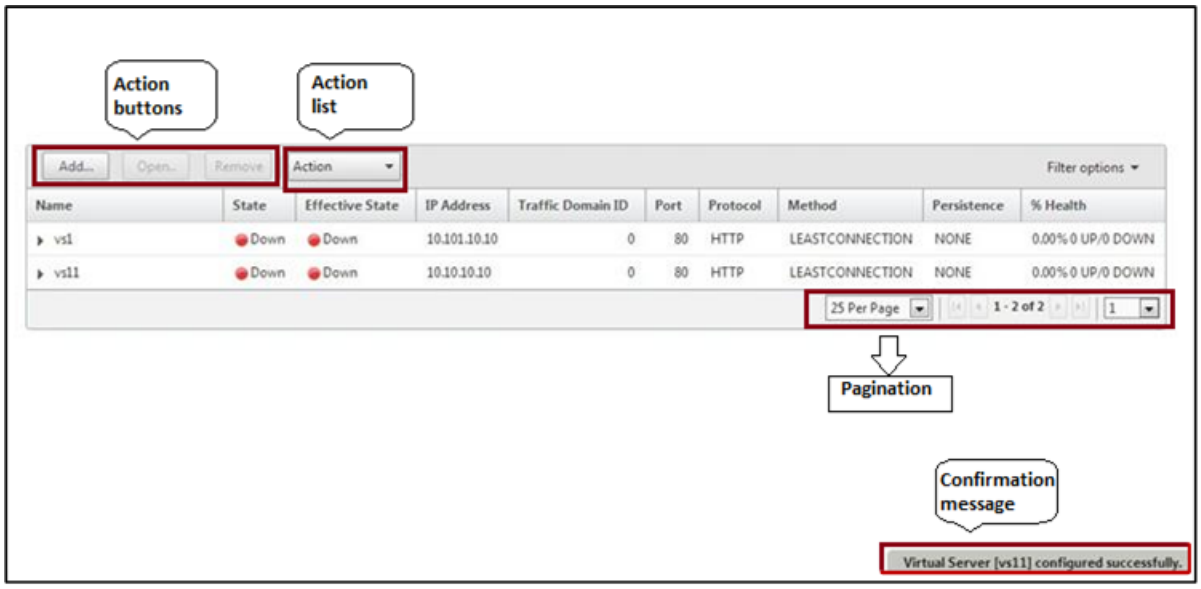
- Auto Detected Services, earlier present as a separate tab when you select **Load Balancing > Services** is now present as an option in the **Action** list when you select **Load Balancing > Services**.
- The option to view FIPS Configuration Summary is now present in the details pane, when you select **SSL**.
- The options to view the AppExpert applications, application templates, and the NetScaler Gateway Applications is present in the details pane, when you select **AppExpert**.
- The option to view cache objects is now present in the details pane, when you select **Integrated Caching**.

To locate any node in the new configuration utility, see the *Node mapping* table.

Other Changes

The following changes further enhance the usability of the configuration utility:

- The (**Add**, **Open**, and **Remove**) action buttons are now at the top of the details pane.
- The other action buttons (for example, **Rename**, **Show Bindings**, **Policy Bindings**, **Statistics**) have been replaced by Action list.
- The option for number of records to display per page has been moved to the bottom of the table that lists the entities.
- The confirmation message for any action that the user performs is displayed at the lower right corner of the configuration utility.
- A vertical scroll bar is provided in the right pane of the configuration utility for easy viewing.



Known Issues and Workarounds

The following issues have been identified in this release.

Application Firewall

- Issue ID 0372768: When you use the default browser PDF plugin to view an application fIrewall report, embedded links might be inactive.

  Workaround: Use the Adobe PDF browser plugin.

Configuration Utility

- 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 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 0361793: The count of the number of load balancing virtual servers, which is shown in the configuration summary, includes the load balancing virtual server that is created during the configuration of EdgeSight Monitoring, even though that load balancing virtual server is not displayed in the **Load Balancing** > **Virtual Servers** pane.
- Issue ID 0369900: When search results do not fit onto one page, duplicate records might appear on the second and subsequent pages.
- Issue ID 0372535: The pagination count on the page that lists SSL policies that can be bound, does not display the correct values.

- Issue ID 0374304: If you access the configuration utility through Internet Explorer 9 or 10 and rename a virtual server, a "No such resource" error message appears, even if the rename operation is successful

  Workaround: Use the mouse to click the **OK** button instead of pressing the ENTER key on the keyboard.
- Issue ID 0374437: When using the configuration utility to configure the NetScaler appliance, if you press Alt+Tab to switch between programs, the current dialog box might disappear, hidden behind the main configuration utility screen. To reach the dialog box, press Alt-Tab a second time.
- Issue ID 0387135: If you access the NetScaler configuration utility through Internet Explorer 8, an attempt to view more than 25 Load Balancing virtual servers per page results in an alert message about an unresponsive script.

  Workaround: Do not change the default pagination value (25). If you change the default pagination value and the system prompts you to stop running the script, choose to continue.
- Issue ID 0389328: When you use Google chrome browser to access the NetScaler configuration utility, and if the monitor resolution is low, you may not be able to use the mouse to scroll the screen .

  Workaround: Use the arrow keys on the keyboard to scroll the screen.

Documentation

- Issue ID 0370607: The configuration utility procedures in the NetScaler 10.1 documentation have not been updated to reflect the new top-level nodes.

  See Configuration Utility Changes, for information on the new node structure.

Domain Name System

- Issue ID 0376662: The NetScaler appliance might fail in the following scenario:
  - On the appliance, you have configured DNSSEC offload and enabled NSEC record generation for a zone.
  - The appliance receives a DNS NODATA/NXDOMAIN query for that zone, over TCP, and the DNSSEC OK bit in the query is set.

Global Server Load Balancing

- Issue ID 0385305: In a GSLB setup, if you perform auto synchronization and the configuration file in your local site contains the "add locationFile" command, the command is not synchronized to the remote location.

Monitoring

- Issue ID 0369946: If you bind an FTP user monitor to an IPv6 service, the state of the service is shown as DOWN.

- Issue ID 0383812: A monitor of type CiTRIX-wi-EXTENDED fails if the script name and site path argument are not explicitly set.

  Workaround:

  a. Create a monitor of type CiTRIX-wi-EXTENDED.
  b. Set the script name.
  c. Set the site path.

  For example,

```
add monitor wi-mon CiTRIX-wi-EXTENDED -userName
administrator -password freebsd -domain xendt -sitePath "/
Citrix/XenApp
set monitor wi-mon CiTRIX-wi-EXTENDED -scriptname "nswi.pl"
set monitor wi-mon CiTRIX-wi-EXTENDED -sitePath "/Citrix/
XenApp
```

NetScaler SDX Appliance

- Issue ID 0384909: When you disable an interface of an LA channel configured on an instance of NetScaler appliance, which is running on a NetScaler SDX appliance, the SDX appliance does not notify the peer device that the interface is disabled and this results in the peer device sending traffic to the disabled interface.

  Workaround: Disable the interface of the peer device so that the Peer device does not send traffic to the disabled interface of the SDX appliance.

Networking

- Issue ID 0371613: In a high availability configuration with the network firewall mode set to BASIC on the current secondary node, the synchronization of configuration files from the primary to secondary node fails after you run the **Sync HA file** command from the NetScaler command line or by using the **Start file synchronization** dialog box in the configuration utility.

  Workaround: Add the following extended ACL on each of the nodes of a HA configuration:

```
add acl <aclname> -srcIP <NSIP of the peer node> -protocol
TCP -destport 22
```

  For example, for an HA configuration in which the primary node's NSIP is 198.51.100.9 and the secondary node's NSIP is 198.51.100.27, you would run the following command on the primary node:

```
add acl ACL-example -srcIP 198.51.100.27 -protocol TCP -
destport 22
```

  and the following command on the secondary node:

```
add acl ACL-example -srcIP 198.51.100.9 -protocol TCP -destport
22
```

- Issue ID 0383958: "$" is an invalid value for the port parameter of any extended ACL. While configuring an extended ACL by using the configuration utility, if you set the port parameter to "$", no error message is displayed and the ACL is not configured.

Policies

- Issue ID 0390584: The configuration utility cannot be used to define classic SSL policies. They can only be defined by using the CLI. However, you can use the configuration utility to bind and unbind classic SSL policies.

SSL

- 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.

System

- Issue ID 0388481: When upgrading from 9.3 to 10.1, the SNMP alarms namely IP-CONFLICT, HA-LICENSE-MISMATCH, and HA-PROP-FAILURE throw a time argument error. This issue occurs because, from version 10 and later, the time parameter is deprecated for the specified SNMP alarms.

  Note: The same error is also displayed when trying to set the time for the same alarms.

  Workaround: Before upgrading to 10.1, update the `ns.conf` file by removing the time parameter for the three alarms from the **set snmp alarm** command.
- Issue ID 0390257: SNMP returns incorrect values for the ifOutOctets and ifInOctets counters.

XML API

- Issue ID 0363145: The following APIs are not available from version 10.1:
  - `bindservicegroup_state2`
  - `unsetnslimitidentifier_selectorname`. Instead use `unsetnslimitidentifier_selector`.

Supported Releases on NetScaler Hardware

The following table lists the earliest NetScaler builds for releases that are supported on the NetScaler MPX platforms. Unless otherwise stated, any release later than the ones listed is supported.

NetScaler Hardware	Releases and Builds
MPX 5500	Release 8.1, build 65.5 and later Release 9.1, build 95.3.cl and later Release 9.1, build 98.5.nc and later
MPX 5550/5650	Release 9.3, build 59.5.nc and later Release 10.0, build 71.6.nc and later
MPX 7500/9500	Release 8.1, build 65.5 and later Release 9.1, build 95.3.cl and later Release 9.1, build 98.5.nc and later
MPX 8200/8400/8600	Release 9.3, build 58.5.nc and later Release 10.0, build 70.7.nc and later
MPX 9700/10500/12500	Release 8.1, build 67.7 and later Release 9.1, build 98.5.cl and later Release 9.1, build 98.5.nc and later
MPX 9700/10500/12500 10G	Release 9.1, build 100.3.cl and later Release 9.1, build 100.3.nc and later
MPX 15500	Release 8.1, build 69.4 and later Release 9.1, build 102.8.cl and later Release 9.1, build 102.8.nc and later
MPX 15500 10G	Release 9.1, build 102.8.cl and later Release 9.1, build 102.8.nc and later
MPX 11500/13500/14500/16500/18500/20500	Release 9.2, build 54.3.nc and later Release 9.3, build 52.3.nc and later
MPX 15000	Release 8.0, build 55.3 and later
MPX 17000	Release 8.0, build 55.3 and later

NetScaler Hardware	Releases and Builds
MPX 17500/19500/21500	Release 9.1, build 103.9.nc and later Release 9.2, build 45.7.nc and later
MPX 17550/19550/20550/21550	Release 9.3, build 53.5.nc and later
MPX 21550T	Release 9.3, build 62.4 and later
MPX 22040/22060/22080/22100/22120	Release 9.3, build 58.14 and later

Software Requirements

Wireshark Versions for NetScaler Releases

The following table provides the Wireshark versions that you can use with different NetScaler releases and builds.

NetScaler Release	Build Number	Wireshark Version
10.1	Later than 95.2	1.9.1
10	Later than 69.3	1.8.4
9.3.e	Later than 57.5004.e	1.9.1
9.3.e	Upto 57.5004.e	1.8.4
9.3	Upto 60.3	1.8.4
9.2	Upto 57.2	1.8.4

Licensing

If you want to upgrade your software to this release, you can use your existing license. Contact your Citrix sales representative for new licenses if you are using the standard edition and want to upgrade to the enterprise or platinum edition, or if you are using the enterprise edition and want to upgrade to the platinum edition.

For more information, see NetScaler Licenses.

Upgrading the NetScaler Software to Release 10.1

To upgrade your software, download release 10.1 and use the Upgrade Wizard (MPX or VPX) or Management Service (SDX).

To download the latest build

1. In a browser, go to www.citrix.com and click the **Downloads** tab.
2. In the **Product** list, select **NetScaler ADC**.
3. In the **Download Type** list, select **Firmware**, and then select the release and build that you want to download.
4. Click **Download**.
5. Accept the **Download Agreement**.
6. Select **Save As**, and then browse to the location of the folder on your local computer where you want to save the firmware.
7. Select the documentation file and repeat steps 5 and 6 to save the file on your local computer.

To upgrade an MPX Appliance or VPX Virtual Appliance

1. Log on to the configuration utility.
2. In the details pane, click **Upgrade Wizard**.
3. In the wizard, in **File Location**, select **Local Computer**, and then navigate to the folder that contains the software and the documentation file. Click **OK**.
4. Follow the instructions in the wizard.
5. When prompted, select **Reboot**.

To upgrade an SDX Appliance

1. Log on to the configuration utility and navigate to **Management Service** > **Software Images**.
2. Upload the software image and documentation file downloaded from the Citrix website to your SDX appliance.
3. In the **System** pane, under **System Administration**, click **Upgrade Management Service**.
4. In the **Upgrade Management Service** dialog box, select the software image and documentation file.
5. Click **OK**. The Management Service restarts after the upgrade.

Note: Your configuration is saved before you restart the appliance, and is available after you upgrade the appliance.

NetScaler Documentation

A complete set of NetScaler documentation is available on Citrix eDocs at http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler-wrapper-con.html.

You are encouraged to provide feedback and suggestions so that we can enhance the documentation.

Service and Support

Citrix® offers a variety of resources for support with your Citrix environment, including the following:

- The Knowledge Center is a self-service, Web-based technical support database that contains thousands of technical solutions, including access to the latest hotfixes, service packs, and security bulletins.
- Technical Support Programs for both software support and appliance maintenance are available at a variety of support levels.
- The Subscription Advantage program is a one-year membership that gives you an easy way to stay current with the latest product version upgrades and enhancements.
- Citrix Education provides official training and certification programs on virtually all Citrix products and technologies.

For more information about Citrix services and support, see the Citrix Systems Support Web site at http://www.citrix.com/lang/English/support.asp.

You can also participate in and follow technical discussions offered by the experts on various Citrix products at the following sites:

- http://community.citrix.com
- http://twitter.com/citrixsupport