Citrix NetScaler 1000V Release Notes

Citrix NetScaler 10.5-51.10
September 22, 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Contents

10.5-51.10

The Citrix NetScaler 1000V, version 10.5 release has the following release build

◆ Build 51.10 (2014-08-20) (Current build)

Review the enhancements, bugs fixed, and known issues that are provided for the latest released version. For more specific details on previously released builds, refer to the release notes copy (html) that is provided on the Citrix downloads page.

> **Note:** You can find the build in which the issue was provided by viewing the **[From Build xxxx]** label that is provided below each issue.

Points to Note

The list of points to note available in Build 51.10.

System

◆ Wireshark Version for Getting NetScaler Trace

Wireshark is required to open nstrace files (cap and pcap). For NetScaler 10.5 and later releases, Wireshark must be upgraded to version 1.11.3 or any later version. You can download the latest version from: https://www.wireshark.org/download.html.

[From Build 51.10] [#462557]

◆ FreeBSD version for Auditlog Server

For NetScaler 10.5 and later releases, the auditlog server fails to start if it is deployed on a FreeBSD 6.3 system.

Background: In this release, the NetScaler supports auditlog servers on FreeBSD 8.4. Therefore, auditlog servers that are deployed on FreeBSD 6.3 systems will not start.

Workaround: Upgrade to FreeBSD OS on which you have the auditlog server, from 6.3 to 8.4.

[From Build 51.10] [#447571]

Web Interface

◆ OpenJDK version for Web Interface on NetScaler (WIonNS)

For NetScaler 10.5 and later releases, Web Interface on NetScaler (WIonNS) must use the OpenJDK7 package since NetScaler now uses FreeBSD 8.x/amd64. You can download the package from either one of the following links:

* http://ftp.freebsd.org/pub/FreeBSD/releases/amd64/amd64/8.4-RELEASE/
packages/java/openjdk-7.17.02_2.tbz

* ftp://mirror.is.co.za/FreeBSD/ports/amd64/packages-8.4-release/devel/
openjdk-7.17.02_2.tbz

Background: When the NetScaler is upgraded to version 10.5, it still has OpenJDK1.6
instead of OpenJDK1.7 which is required for NetScaler version 10.5. Therefore,
when the configurations are saved (after upgrading), the Web Interface sites
become inaccessible.

Workaround: Before you save the configurations on the upgraded appliance, make
sure you re-install the Web Interface on NetScaler version 10.5 by using
OpenJDK1.7.

[From Build 51.10] [#464854]

What's New?

NetScaler Insight Center

◆ NetScaler Insight Center now supports monitoring of CloudBridge 2000, 3000, 4000,
and 5000 appliances. It analyzes the ICA traffic flowing through the CloudBridge
appliances and generates HDX Insight performance reports. With this feature,
datacenter administrators can gather information about traffic flowing between
XenApp/XenDesktop clients and XenApp/XenDesktop servers.

[From Build 51.10] [#430880]

Fixed Issues

The list of issues that are fixed in Build 51.10.

AAA-TM

◆ To unlock an external user account, you must first add that user to the NetScaler
ADC, and then run the "unlock aaa user <user name>" command.

[From Build 51.10] [#483526]

Application Firewall

◆ If you update default signatures on the primary NetScaler ADC in an HA pair, you
cannot sync the updated signatures to the secondary ADC.

[From Build 51.10] [#486231]

◆ On a NetScaler ADC that has the application firewall enabled and the Learning
feature enabled for one or more security checks, the Learning module might
become unresponsive. When this happens, no additional learning takes place and no
recommendations for new relaxations or rules are generated.

[From Build 51.10] [#478109, #484323]

Command Line Interface

◆ The command line interface fails when a non-nsroot user without superuser permission executes the "show techsupport" command from the command line interface.

[From Build 51.10] [#488781]

Configuration Utility

◆ The "STA Auth ID" property is not shown along with the details of the STA Server.

[From Build 51.10] [#482609, #485852]

◆ When using the XenApp/XenDesktop wizard, when you click on "Getting Started", you get an error message that says that you need a AAA license. Therefore, you cannot proceed with the wizard. In an ideal case, the AAA license is not needed when using the wizard.

[From Build 51.10] [#488199]

◆ In the configuration utility, you cannot apply an SSL profile to an SSL VPN virtual server.

[From Build 51.10] [#484583]

◆ The "XenApp and XenDesktop" wizard is not available in the configuration utility when the appliance is a part of a cluster.

[From Build 51.10] [#483517]

◆ When configuring a Web Interface on NetScaler (WIonNS) site by using the configuration utility, you cannot modify the NetScaler Gateway URL if the SSL certificate that is bound to the VPN virtual server is a wildcard (has an *).

[From Build 51.10] [#490027, #489788]

◆ The NetScaler graphical user interface (GUI) has been enhanced to provide a better user interaction experience. It now provides you with a workflow-based experience, which guides you through the entire configuration. The configuration settings have been classified as basic and advanced for some features. The NetScaler ADC configuration utility and NetScaler Gateway configuration utility has also been reimplemented in HTML. As a result of these enhancements, the GUI does not display pop-up dialog boxes for most features and you no longer need Java Runtime Environment (JRE) to access these features through the GUI.

For more information, see http://support.citrix.com/proddocs/topic/ns-rn-main-release-10-5-map/ns-rn-changes-gui-10-5-con.html

[From Build 51.10] [#251336, #251607, #251645, #251760, #251797, #257879, #257949, #261240, #261339, #285382]

◆ Java Runtime Environment (JRE) does not work on Internet Explorer version 10.

[From Build 51.10] [#482135]

DNS

◆ Statistics do not appear correctly for a DNS load balancing virtual server.

[From Build 51.10] [#462862]

GSLB

- If a GSLB domain is queried through VPN, NetScaler fails. This issue is fixed in this release.

  [From Build 51.10] [#488161]

Integrated Caching

- With integrated caching enabled, the NetScaler can crash when the evaluation of a callout 'result expression' (configured with the resultExpr parameter) results in a UNDEF condition.

  [From Build 51.10] [#488145]

Load Balancing

- If the secure option is enabled on a CITRIX-WI-EXTENDED monitor that is bound to a service, then the monitor incorrectly marks the monitor probes as failed.

  [From Build 51.10] [#488007, #487724]

- The NetScaler ADC fails if both the following conditions are met:

  - a large number of SIP messages are received.

  - the size of the SIP messages is greater than the jumbo MTU configured on the ADC.

  [From Build 51.10] [#484547]

NetScaler Insight Center

- A NetScaler ADC fails when it receives ICA traffic from metro receiver client.

  [From Build 51.10] [#482413, #492160]

- If you add more than one NetScaler or CloudBridge devices to the NetScaler Insight Center inventory, the afdecoder subsystem may stop functioning.

  [From Build 51.10] [#489534, #491193, #492523, #495674]

- If you enable AppFlow on a NetScaler ADC, the ADC might crash due an internal memory dependency.

  [From Build 51.10] [#486792]

- In the NetScaler Insight Center graphical user interface, you might not be able to configure a Terminal Access Controller Access-Control System (TACACS) server.

  [From Build 51.10] [#483118]

- The Applications report might not display any data for geo maps.

  [From Build 51.10] [#490416]

- The Applications reports (Dashboard > HDX Insight > Applications) display incorrect values for Active Apps and Active sessions.

  [From Build 51.10] [#484659, #487457]

- Even after you delete a CloudBridge device from NetScaler Insight Center, it displays the device in the inventory and continues to collect AppFlow data.

  [From Build 51.10] [#474616]

Networking

- For a link load balancing with RNAT configuration, the NetScaler ADC might use an incorrect subnet IP (SNIP) address to communicate to the external devices.

  [From Build 51.10] [#480621]

- For an IPv6 load balancing configuration in which the IPv6 virtual server and the bound services are in different traffic domains, and USIP is enabled, the NetScaler ADC might become unresponsive when the IPv6 virtual server receives traffic.

  [From Build 51.10] [#490398]

- The NetScaler ADC might become unresponsive when you run the "bind rnat global" command.

  [From Build 51.10] [#483502]

- The CPU usage might be approximately 10% higher in NetScaler 10.5 version as compared to NetScaler 9.3 version.

  [From Build 51.10] [#432192]

- The NetScaler ADC might use a large amount of CPU cycles when it receives a burst of GRE traffic, which meets the following criteria:

  - The NetScaler ADC is not the GRE end point for this traffic.

  - The NetScaler ADC creates a NAT session information for this traffic.

  [From Build 51.10] [#480573]

- For a link load balancing with RNAT configuration in which persistence is enabled for the virtual server, the NetScaler ADC might become unresponsive when the virtual server receives traffic.

  [From Build 51.10] [#471651, #479882, #485831, #493232]

Platform

- The SDX 24100/24150 and MPX 24100/24150 platforms are now supported in this release.

  [From Build 51.10] [#487831]

SSL

- In rare cases, if the random number generated for the DH key exchange has a leading zero, DH negotiation fails because of a hardware limitation.

  [From Build 51.10] [#414388, #345883, #349858, #428257, #428259]

System

- With SPDY enabled, creating an AppFlow structure results in memory initialization issues.

  [From Build 51.10] [#488487]

- With USIP mode enabled, when the client FIN comes along with the final ACK for the server response, the NetScaler TCP module does not acknowledge the FIN.

  [From Build 51.10] [#478356]

- ◆ SNMP walk shows the operational status of a LA channel as DOWN even when it is in the PARTIAL-UP state.

  [From Build 51.10] [#477709]

- ◆ When using DNS request pipelining with request switching, the audit log feature causes the NetScaler appliance to crash and reboot.

  [From Build 51.10] [#488997, #493835]

- ◆ When using Web Interfaces, after logging in to the VPN, users are not authorized to access published resources.

  [From Build 51.10] [#484960]

- ◆ The Monupload process monitors the power supply and sends a "show techsupport" bundle as soon as a power failure is observed. This behavior is now modified to upload the bundle only in case the power supply does not recover in a 1 minute.

  [From Build 51.10] [#452240]

Known Issues

The list of known issues available in Build 51.10.

AAA-TM

- ◆ In the configuration utility, when you filter out specific IPs and IP ranges specified as IP/netmask, the sessions are not filtered out. All sessions still appear on the list. When you filter out sessions by AAA user or AAA group, those sessions are filtered out and the list appears as it should.

  [From Build 50.10] [#446755, #468475]

- ◆ Occasionally a AAA-TM session on one core of an nCore or cluster ADC is not duplicated to other cores. When this condition occurs, counters do not include the session, which causes monitoring and statistics displays to show incorrect information.

  [From Build 50.10] [#480298]

AppExpert

- ◆ Creating an AppExpert application with the name 'ns' (uppercase or lowercase) results in conflicts and therefore the creation of a content switching policy fails.

  Workaround: Do not create AppExpert applications with name 'ns' (uppercase or lowercase).

  [From Build 50.10] [#483427]

AppFlow

- ◆ The following behavior is seen during a high availability failover on a NetScaler appliance that has active ICA session applications launched:

  - The applications stop functioning, but are visible on the browser.

  - The Citrix Receiver displays a dialog box, with a message stating that the connection is disconnected.

- When you click OK on the dialog box, the applications are not displayed anymore.

- If you launch any fresh applications without re-login, all the previously launched applications will resume with the previous status.

[From Build 50.10] [#388563, #438710, #488206]

Application Firewall

- A NetScaler ADC that has the application firewall feature enabled might reset the connection after a protected web server issues an HTTP 204 response.
  [From Build 51.10] [#427798]

- The application firewall PCI-DSS report does not contain information on the "SQLInjectionCheckSQLWildChars" parameter.
  [From Build 50.10] [#423150]

- When a user attempts to upload a file to a server that is protected by the application firewall, the file upload fails. The underlying cause is that the application firewall included an invalid character in the MIME boundary when encoding the file.
  [From Build 51.10] [#472476, #418036]

- The General tab on the Modify Field Format Check dialog box is not functional. To work around this issue, you can enable or disable the action items (block, learn, log, stats) in the Application Firewall Wizard, or by using the NetScaler command line.
  [From Build 50.10] [#445931]

- If the application firewall blocks a request because of a limiting policy, such as a maximum upload size limit on a web form, the blocking action is not logged. If a custom redirect page has been configured for that web page, the application firewall does not display it.
  [From Build 51.10] [#466329]

- If the application firewall receives a multipart POST request with a Content-Type header that contains a charset, it blocks that request as malformed.
  [From Build 51.10] [#464641]

- In the NetScaler configuration utility, when you approve Form Field Consistency check learned relaxations, you must close and then reopen the Modify Form Field Consistency Check dialog box before the new relaxations appear in the list.
  [From Build 50.10] [#457954]

- Signature Bindings Not Shown in PCI-DSS Report

  The Application Firewall PCI-DSS report does not display signature bindings. The Profile Settings section of the report shows bound signatures as "not set".

  [From Build 51.10] [#443673]

- If a user request triggers an application firewall policy that is bound to the APPFW_BYPASS profile, the application firewall might fail to generate an SNMP alarm.
  [From Build 51.10] [#489691]

Cache Redirection

- In the event of a cache miss, the request is sent as an SSL request instead of an HTTP request to the origin server even though the backendssl parameter is disabled on the NetScaler ADC.

  [From Build 50.10] [#442353]

CloudPlatform

- The NetScaler 10.5 release does not support Citrix CloudPlatform.

  [From Build 50.10] [#447834]

Cluster

- In a NetScaler cluster, UDP fragments from the server are not bridged to the client in case of ANY * virtual servers.

  [From Build 50.10] [#480324]

Command Line Interface

- The rbaOnResponse system parameter fails to work after you upgrade NetScaler ADC nCore or nCore VPX from version 9.3 to 10.x.

  [From Build 51.10] [#480639]

Configuration Utility

- After installing Java, if you disable Java on the Java Control Panel, the graphical user interface (GUI) applet remains blank.

  Workaround: Be sure to enable Java on the control panel.

  [From Build 50.10] [#460020]

- If you use the MAC Safari browser to upgrade a NetScaler ADC and, in the upgrade wizard, you click the browse button to choose a build file on the appliance, the dialog box does not shown any files or folders. If you navigate back to the root folder, the dialog box displays the top level folder, but you cannot browse the files in the folder.

  Workaround: Click the Settings icon and navigate to Preferences > Security > Manage Website Settings > Java, and then change the When visiting other websites setting to Run in unsafe mode.

  [From Build 50.10] [#466245, #475388]

- You cannot use the configuration utility to add signatures to an existing application firewall policy.

  Workaround: Use the command line interface .

  [From Build 51.10] [#470941]

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

[From Build 51.10] [#375277, #322602, #334465, #396405, #412455, #419503, #438382, #438534, #438796, #441853, #446387, #448361]

◆ In some cases, while binding an entity, such as a service or a certificate, if you unbind another entity from the list, the list is refreshed and the entities that you selected for binding are no longer displayed. Therefore, you must again select the entities that you want to bind.

Workaround: Bind and unbind entries in separate operations.

[From Build 50.10] [#459906, #485041]

◆ You cannot create load balancing virtual servers or NetScaler Gateway virtual servers with the name pattern that matches the virtual servers created on the XenMobile wizards.

[From Build 50.10] [#485698]

◆ The Traffic Management > Load Balancing > Set up NetScaler for XenApp/ XenDesktop wizard, displays an error if more than one service group is bound to the virtual server that is used for load balancing the XenApp/XenDesktop servers, or if more than one service is bound to the service group.

[From Build 51.10] [#414807]

◆ To display the newly added HTML imports, you have to refresh the page on the browser.

[From Build 50.10] [#441408]

◆ If you are binding classic policies, set empty values for the "Gotoexpression" and "Invoke" columns as these parameters are not applicable for classic policies.

[From Build 50.10] [#454246, #478532]

◆ For integrated caching, the details of a cache object are not available in the configuration utility. However, the list of cached objects is available.

Workaround: Use the CLI command to view the details of a cache object.

[From Build 50.10] [#457623]

◆ After the first reboot of a cluster setup that has large configurations, the NetScaler ADC takes more time to load these configurations and to allow you to logon.

[From Build 50.10] [#483442]

◆ The key filename property of Import FIPS key (Configuration > Traffic Management > SSL > FIPS > FIPS keys >Action > Import > Key Filename) fails if you provide an incomplete filepath, folder1/folder2/rsa.key, where folder1 and folder2 are the folders within the nsconfig/ssl path.

Workaround: Provide the complete file path nsconfig/ssl/folder1/folder2/rsa.key, or provide only the file name, rsa.key.

For 10.5---Complete file path must be given(Either by typed or selected by browsing)

[From Build 51.10] [#483226]

◆ You cannot install a server, client, or intermediate certificate with a FIPS key by using the configuration utility.

Workaround: Use the FIPS wizard to create and install the certificate.

[From Build 50.10] [#485942]

◆ The graphical user interface (GUI) does not display the following search fields on the Cache Objects page:

- HTTP Status Code

- Ignore Marker Objects

- Include-Not Ready Object

[From Build 50.10] [#447915]

◆ If you create a load balancing virtual server with a name matching the pattern "_XM_LB_MDM," the XenMobile dashboard might display incorrect port values.

[From Build 51.10] [#486590]

◆ If a policy is bound or unbound from system global or the priority of the policy is modified, the changes are not reflected automatically. To see the current status, you should click on the "Refresh" icon at the top right corner of the policy view. After refreshing the view, the policies display their bound status as well as the priorities.

[From Build 50.10] [#452669, #391434, #453555, #453597, #478131, #479434, #481397]

◆ The IP Bindings tab on the Create VLAN and Configure VLAN pages does not display IP addresses that are in the same subnet as the management IP (NSIP) address.

[From Build 50.10] [#456428]

◆ The new look editor for classic policies has the following limitations:

- The option to modify an expression is not intuitive.

- The options to match any expression, match all expressions, and tabular form are not provided.

- The option to remove individual expressions within a compound expression is not provided.

- Named expressions are not classified and displayed.

- Named expressions cannot be previewed.

- The add or remove bracket buttons are not provided.

[From Build 50.10] [#480536]

◆ When using the expression editor to modify an existing expression, select the expression and click Expression Editor. Alternately, you can modify the expression directly in the text field.

[From Build 50.10] [#483421]

DNS

- When NetScaler is deployed as a DNS server, with caching enabled, and "flush dns proxyRecords" is used when it is serving a large volume of traffic and large number of records are cached on NetScaler, the appliance may sometimes fail.

  [From Build 51.10] [#484069]

- While adding a DNS record (such as addrec and nsrec) from the GUI or by using the NITRO API, when you specify the TTL value as 3600, the value of the minimum TTL of the SOA record will be considered.

  Workaround: Use the corresponding CLI command to add the DNS record.

  [From Build 51.10] [#382478]

Front End Optimization

- Some websites might not be able to render the page if the AppFlow clientSideMeasurements parameter is enabled along with some front end optimization actions.

  [From Build 50.10] [#475535]

GSLB

- If you change the GSLB configuration while the GSLB feature is disabled, the NetScaler ADC might process some stale messages when you enable the feature. As a result, the ADC might dump core and restart.

  [From Build 51.10] [#485811]

High Availability

- When upgrading HA nodes that have Web Interface on NetScaler (WIonNS) to build 126.x, the updates made in the Webinterface.conf file are over-written by the previous version of the file. This is due to the rolling upgrade of HA nodes or due to the file sync operation between HA nodes.

  To avoid this issue, use the following steps when upgrading the HA nodes:

  1. Before upgrading, run the command: "set ns param -internaluserlogin DISABLED"

  2. Upgrade the secondary HA node to NetScaler 10.1 Build 126.x release.

  3. Force failover to make the upgraded node as the primary node.

  4. Upgrade the other HA node to NetScaler 10.1 Build 126.x release.

  5. Restore the previously disabled "internaluserlogin" parameter to enabled using the command: "set ns param -internaluserlogin ENABLED".

  6. Save the configurations.

  Note: Before upgrade sync files between the HA nodes by using CLI command: "sync ha files all".

  [From Build 51.10] [#471294]

Integrated Caching

- When a selector-based content group has been configured, the NetScaler ADC can fail when a policy associated with this content group is matched and the response status is "404 Not Found".

  [From Build 51.10] [#440107, #440389]

Load Balancing

- If a client connection is in the CLOSE_WAIT state, the NetScaler ADC does not send PUSH notifications to the client. However, it reports success to the PUSH server.

  [From Build 51.10] [#489197]

- In a deployment with multiple MAC-mode virtual servers, some changes in the configuration can result in a MAC-mode virtual server failing to serve traffic. Changes that can cause the problem include:

  - Disabling and enabling the interface through which the MAC of a service is learnt.

  - Removing virtual servers or clearing their configurations.

  - Changes caused by high availability failovers.

  [From Build 51.10] [#471938]

- Command line output is not displayed on the GUI while configuration is synchronized. The output is not displayed even when the "No Warning" check box is not selected.

  [From Build 50.10] [#456144]

NetScaler Insight Center

- The following error might occur if you open the dashboard on the NetScaler Insight Center graphical user interface using Internet Explorer 8:

  "Error fetching licensing information."

  Workaround: Access the NetScaler Insight Center using any other browser. For more information about browser support, see http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-access-ni-con.html.

  [From Build 51.10] [#496805]

- If you enable AppFlow for ICA on a NetScaler ADC and access Windows XP VDI through XenDesktop 5.6, the Windows XP VDI might fail to launch.

  [From Build 51.10] [#484515]

- If Appflow for ICA is enabled on a NetScaler ADC, the NetScaler Insight Center reports display should show XenDesktop details, but that is not always the case. When certain users access XenDesktop, the reports show the application details instead.

  [From Build 51.10] [#482590]

- The NetScaler ADC might fail if you enable AppFlow for ICA and access XenApp or XenDesktop through the Windows receiver client.

  [From Build 51.10] [#490680]

- If AppFlow is enabled for a virtual server on more than one NetScaler Insight Center virtual appliance, the clear AppFlow configurations (Configuration > Inventory > <ipaddress> > Application List > <ipaddress> > Action > Clear AppFlow Configuration) operation does not work on the virtual server that has the lowest priority.

  [From Build 50.10] [#405853]

- On the HDX Insight reports, a Y-axis value of 0 is sometimes shown at a location higher than the x axis.

  [From Build 51.10] [#414214]

- NetScaler Insight Center displays the following error if a NetScaler ADC maintains more than 20 active sessions.

  'Excess connection than the CFE limit for NetScaler'

  [From Build 50.10] [#484492]

- All the metrics except bandwidth and hits display the average values.

  [From Build 51.10] [#409634]

- The Web Insight reports might not display geo maps for some locations.

  Workaround: The tabular representation displays the details.

  [From Build 50.10] [#484578]

- In some instances, the bar line on a graph appears outside the time points on the x-axis.

  [From Build 51.10] [#446120]

- After the NetScaler upgrade or downgrade operation, NetScaler Insight Center does not report any data on the dashboard.

  [From Build 50.10] [#405936]

- NetScaler Insight Center displays the RTT value as NA in cases where the ICA RTT value exported from device is zero.

  [From Build 51.10] [#486191]

- A NetScaler Insight Center report that displays the launch duration value display multiple rows for the same application

  [From Build 51.10] [#473936, #473967]

- NetScaler Insight Center reports might show a different gateway and network mask for a CloudBridge device used for monitoring AppFlow traffic.

  [From Build 51.10] [#488886]

- Downgrading NetScaler Insight Center from release 10.5 to release 10.1 is not supported.

  [From Build 50.10] [#486295]

- NetScaler Insight Center might not correctly report user sessions with multi-stream ICA connections.

  [From Build 51.10] [#470481]

NetScaler insight Center

- The NetScaler Insight Center reports display an incorrect session reconnect value for CloudBridge appliances.

  [From Build 51.10] [#496899]

Networking

- In a high availability (HA) configuration, VMAC configuration might be lost when continuous HA failover happens.

  [From Build 51.10] [#477402]

- When the MTU of a VLAN is set to 500, the adjacency of Intermediate System to Intermediate System (IS-IS) protocol fails in this VLAN because the IS-IS process on the NetScaler ADC works with a minimum MTU value of 520.

  [From Build 50.10] [#485391]

- When the NetScaler appliance forwards packets that are larger than the interface's MTU value, the appliance fragments the packets into 2048-byte packets, regardless of the MTU value configured.

  For example, if the appliance forwards a 9000-byte packet on an interface that you have configured with an MTU of 4000, the appliance fragments the 9000-byte packets into 2048

  [From Build 50.10] [#429006]

- ZebOS API call to NetScaler ADC fails when the ns ipv6-routing command is part of the input routing config set.

  [From Build 50.10] [#439294]

- If a NetScaler appliance on which the cache redirection feature is enabled supports jumbo frames on the client-side connection but not supported on the server-side connection, the client-side connection behaves as a regular connection.

  [From Build 50.10] [#422858]

- The source IP persistency functionality might not work for an RNAT rule that does not have the NAT IP parameter set to an IP address.

  [From Build 50.10] [#455936]

- In an active-active high availability configuration using Virtual Router Redundancy Protocol (VRRP) protocol, PING to a virtual IP address (VIP) might fail from a node, which is a backup node for this VIP address.

  [From Build 51.10] [#485260]

- If you have enabled Source IP Persistency on multiple IPv4 RNAT rules that have the same condition but with different NAT IP addresses, the NetScaler command line and the configuration utility displays Source IP Persistency as ENABLED only for one of these rules.

  [From Build 50.10] [#459679]

- Jumbo frames are not supported on NetScaler VPX appliances.

  [From Build 50.10] [#485905]

- On a NetScaler ADC, when the MTU of a VLAN and Intermediate System to Intermediate System (IS-IS) Link Sate Packet (LSP) are set to a value lesser than

1500, the IS-IS process fails to send the IS-IS protocol data units (PDUs) of the set MTU size until the process is restarted.

[From Build 50.10] [#485374]

◆ In an HA configuration in INC mode where both the nodes run the OSPF routing protocol, the secondary node drops all the L3 traffic that has the destination that was advertised by the secondary node.

[From Build 51.10] [#318684]

◆ In a high availability (HA) configuration, VLAN Interface binding configuration might be lost when continuous HA failover happens.

[From Build 51.10] [#477415]

◆ Jumbo frames are not supported on an IPv6-IPv6 tunnel.

[From Build 50.10] [#420198]

◆ The IS-IS level 1-2 adjacency between NetScaler ADC and Cisco Nexus Router might flap.

[From Build 50.10] [#485385]

◆ For a link redundancy using LACP channels configuration with two sub channels, the maximum supported throughput for both the sub channels falls below the configured lrMinThroughput value, link failover does not occur when the maximum supported throughput of the standby sub channel becomes equal to or greater than the lrMinThroughput value.

[From Build 50.10] [#470980]

◆ High availability (HA) synchronization does not work properly after you upgrade an HA setup from beta build of 10.5 release to GA build of 10.5 release.

Workaround: Disable HA propagation and HA synchronization before upgrading the HA setup and enable them after the upgrade process is complete.

[From Build 50.10] [#486131]

Platform

◆ L2 mode is not supported on Netscaler VPX instances running on a Linux-KVM host.

[From Build 51.10] [#402113]

Policies

◆ When a responder policy is configured with a log action, an issue in evaluating the policy expression that is configured in the log action can result in the NetScaler crashing.

Workaround: There is no workaround for this issue. However, you can attempt to disable the log action if this issue is observed.

[From Build 51.10] [#446507]

SSL

◆ If you try to add a certificate bundle with the complete path to the file, an error message appears. For example,

> add ssl certkey bundle -cert /nsconfig/ssl/bundle3.pem -key /nsconfig/ssl/bundle3.pem -bundle YES

ERROR: Processing of certificate bundle file failed.

Workaround: Specify only the file name. For example,

> add ssl certkey bundle -cert bundle3.pem -key /nsconfig/ssl/bundle3.pem -bundle YES

[From Build 50.10] [#481878]

- If CRL auto refresh is enabled and the LDAP method is selected, the following, incorrect, error message appears: "Either URL or server-IP required on CRL"

  This message should indicate that a server IP address is required.

  [From Build 50.10] [#459987]

- In a cluster setup, if you include the "cipherdetails" option in the "show ssl service" or "show ssl vserver" command, an incorrect message appears. This is only a display issue.

  For example,

  > sh ssl service svc1 -cipherDetails

  ERROR: No such resource [serviceName, svc1]

  [From Build 50.10] [#402423]

- An SSL chip is disabled at the third reinitialization attempt. That is, the maximum reinitialization limit is 2. Earlier, this limit was 5.

  [From Build 50.10] [#455821]

System

- The NetScaler randomly crashes when SPDY is enabled on a NetScaler deployment which has integrated caching or front end optimization enabled. This occurs due to some interaction issues.

  Workaround: Disable SDPY when integrated caching or front end optimization is enabled.

  [From Build 51.10] [#486257]

- Changes made to the time zone are not reflected till the NetScaler appliance is warm rebooted.

  [From Build 51.10] [#471100]

- If a NetScaler interface configured for jumbo frames is subjected to persistent congestion, and the NetScaler appliance is operating under low memory conditions, the appliance might not have enough buffers to handle jumbo frames.

  [From Build 50.10] [#431913]

- If you change the IP address of a load balancing virtual server that shares the same server information (IP address, port and service) with an audit server and then clear the configurations, the NetScaler is expected to remove the virtual server, the audit

server, and other NetScaler configurations. However, when you now add the virtual server with the original server details, the NetScaler throws an error message that says "resource already exists".

Note: In a HA setup, this behavior is displayed even when you perform a force sync or a force failover operation.

[From Build 51.10] [#484527]

♦ For virtual servers and services using the default TCP profile (nstcp_default_profile) with the MSS parameter set to zero, the NetScaler appliance uses 1460 as the value for TCP MSS instead of using a value based on interface MTU and VLAN MTU.

[From Build 50.10] [#472833]

♦ When the management CPU is running at close to 100% of capacity, the aggregator might not be able to process some of the statistics requests from clients, such as requests from the configuration utility, the CLI, and SNMP. If the aggregator fails to respond within the timeout period, the client returns following error:

Invalid response from the aggregator [Device not Configured]

[From Build 51.10] [#377618, #341460, #351127, #364015]

♦ When an interface of a static channel becomes inactive because of an MTU mismatch, the peer device of the channel still sends traffic to that interface.

[From Build 50.10] [#463571]

♦ The NetScaler randomly crashes when SPDY is enabled on a NetScaler deployment which has integrated caching enabled. This occurs due to some interaction issues.

Workaround: Disable SDPY when integrated caching is enabled.

[From Build 50.10] [#487437]

♦ The NetScaler appliance may display messages that are a result of file system compatibility checks that are performed when booting up. These messages are informational only, and do not have any adverse impact on the functioning of the NetScaler.

[From Build 51.10] [#452382, #459464]

♦ When configuring Web Interface sites through the wizard, when the "Trust ssl certificate" option is checked, certificates bound to the VPN virtual server are not imported to the JVM.

Workaround: You must import the certificates manually by executing the following command from the shell prompt:

> /netscaler/wi/export_cert.sh

[From Build 50.10] [#481008]

♦ When using MPTCP, if a single SSL record is split into a large number (> 100) of small segments, an SSL buffer overrun causes the NetScaler appliance to crash.

[From Build 51.10] [#427126, #441982, #452885, #456645]

♦ The "unset authentication localPolicy" command is removed from this version onwards.

[From Build 50.10] [#483524]

◆ Downloading a file over a TCP connection in which the client side has a non-jumbo MSS (less than or equal to 1460 bytes) and the server side has a jumbo MSS (greater than or equal to 1460 bytes), causes a slight increase in latency.

[From Build 50.10] [#428209]

◆ In a high availability setup, a crash in the nsfsyncd process results in HA failover.

[From Build 51.10] [#490622]

Web Interface

◆ On a NetScaler ADC, if WIHome is configured to point to an IPv6 load balancing virtual server that points to the IPv6 StoreFront services, a user trying to log on receives a 500 Internal Server Error message.

Workaround: Remove the IPv6 load balancing virtual server configuration and configure WIHome to point directly to the StoreFront server URL.

[From Build 51.10] [#397150]

What's New in Previous 10.5 Builds

The list of enhancements that were released in builds that were released prior to Build 51.10.

AAA-TM

◆ NetScaler as SAML IDP

The NetScaler ADC can now act as a SAML identity provider (IDP). As an IDP, the ADP accepts SAML tokens from user sthat request access to a protected application, redirecting users to the SAML service provider (SP) logon page to authenticate. After the user authenticates, the ADC generates a SAML assertion that grants access to the protected resource and redirects the user to it. When the user logs out or is logged out by any SP, the ADC sends logout requests to all other SPs that the user accessed during the current session and terminates the session.

For more information, see the NetScaler documentation.

[From Build 50.10] [#406525]

◆ Unlocking Locked-Out User Accounts

You can now unlock a user account that was locked out after too many failed logon attempts or after repeated violations of logon attempt time slice limits. To unlock a locked-out user account by using the configuration utility, navigate to Security > AAA-Application Traffic > Users. In the data pane, select the user account to unlock, and then in the Actions drop-down list, choose Unlock. To unlock a locked-out user account from the command line, type the following command:

unlock aaa user <userName>

[From Build 50.10] [#437164]

- Strong Encryption Support in Kerberos KCD

  AAA-TM now supports the aes256-sha1 and aes128-sha1 strong encryption methods for Kerberos KCD. Previously, when KCD was configured to use delegated user credentials, AAA used the relatively weak RC4-HMAC encryption algorithm to encrypt the timestamp when sending a ticket-granting request to the Kerberos server. If the system administrator had restricted use of weak encryption algorithms on the Kerberos server, the Kerberos server would respond with an error instead of the requested ticket, causing KCD to fail. AAA now uses aes256-sha1 to encrypt timestamps for delegated user credentials.

  [From Build 50.10] [#427766]

- NetScaler Default Expressions support for authentication subsystem

  AAA-TM now supports NetScaler default syntax expressions in the following parts of the authentication subsystem:

  * Authentication policy rules. You can use default syntax expressions as Authentication policy rules. The default syntax expression editor now appears in the configuration utility when you create or configure an authentication policy, From the command line, you can simply use default syntax to create the rule for your policy and AAA-TM will recognize and implement it.

  * Authentication policy bindings. Authentication policies, when bound, can each be associated with the "nextFactor" policyset. The nextFactor policyset is evaluated if the policy to which it is associated succeeds. nextFactor support permits policy pairing and grouping, and allows you to create cascading chains of policies all of which can be evaluated in turn. There is no upper limit to the number of policies that can be chained in this manner.

  All policies bound to a single authentication server must be either NetScaler default syntax policies or NetScaler classic syntax policies. You cannot mix both types of policy on a single authentication server.

  [From Build 50.10] [#418615]

- Web-based Authentication

  AAA-TM is now able to authenticate a user to a web server, providing the credentials that the web server requires in an HTTP request and analyzing the web server response to determine that user authentication was successful.

  To set up web-based authentication with a specific web server, first you create a web authentication action. Since authentication to web servers does not use a rigid format, you must specify exactly which information the web server requires and in which format when creating the action. To do this, you create an expression in NetScaler default syntax. Next you create a policy associated with that action. The policy is similar to an LDAP policy, and like LDAP policies uses NetScaler classic syntax.

  [From Build 50.10] [#431391]

- With previous versions of the NetScaler ADC, OWA 2010 connections did not timeout because OWA sends repeated keepalive requests to the server to prevent timeouts,

which interfered with single sign-n and posed a security risk. AAA-tm now supports forced timeouts that ensure that OWA 2010 sessions timeout after the specified period of inactivity.

For more information and configuration instructions, see the documentation.

[From Build 50.10] [#247952, #419622, #426196]

◆ AAA-TM can now be configured to authenticate users with an external RADIUS or LDAP authentication server at a specific FQDN instead of only at a specific IP. Configuration via FQDN can simplify an otherwise much more complex AAA configuration in environments where the authentication server might appear on any of several IPs, but always uses a single FQDN.

Note: When you configure AAA to authenticate to an external server via FQDN instead of IP, you add an extra step to the authentication process because the ADC must resolve the FQDN each time that it authenticates a user. If a great many users attempt to authenticate simultaneously, the DNS lookups might slow the authentication process.

To configure authentication by using a server's FQDN instead of IP, follow the normal configuration process except when creating the authentication action, where you substitute the serverName parameter for the serverIP parameter, as shown below:

> add authentication ldapAction <name> -serverName <serverName>

> add authentication radiusAction <name> -serverName <serverName>

For <serverName>, substitute the fully-qualified domain name (FQDN) of the LDAP or RADIUS authentication server.

[From Build 50.10] [#338718, #314443]

◆ Extracting SAML Attributes from Keytab

The AAA Negotiate Action command can now extract user information from a keytab file instead of requiring you to enter that information manually. If a keytab has more than one SPN, AAA selects the correct SPN. You can configure this feature at the NetScaler command line, or by using the configuration utility.

To configure AAA to extract user information from a keytab file at the command line, type the appropriate command:

add authentication negotiateAction <name> [-keytab <string>]

set authentication negotiateAction <name> [-keytab <string>]

For <name>, substitute the name of the negotiateAction. If you are adding a new action, the name can be from one to 127 characters in length and can consist of upper- and lowercase letters, numbers, and the hyphen (-) and underscore (_) characters. For <string>, substitute the full path and filename of the keytab file that you want to use.

To configure AAA to extract user information from a keytab file by using the configuration utility, do the following steps:

1) Open Security, AAA, Policies, Authentication, Negotiate.

2) In the Data pane, click the Servers tab.

3) Do one of the following:

* If you want to create a new Negotiate action, click Add.

* If you want to modify an existing Negotiate action, in the data pane select the action, and then click Edit.

4) If you are creating a new Negotiate action, in the Name text box, type a name for your new action.

The name can be from one to 127 characters in length and can consist of upper- and lowercase letters, numbers, and the hyphen (-) and underscore (_) characters.

If you are modifying an existing Negotiate action, skip this step. The name is read-only; you cannot change it.

5) Under Negotiate, if the Use Keytab file check box is not already checked, check it.

6) In the Keytab file path text box, type the full path and filename of the keytab file that you want to use.

7) In the Default authentication group text box, type the authentication group that you want to set as default for this user.

8) Click Create or OK to save your changes.

[From Build 50.10] [#405134]

◆ Responder After AAA

On a NetScaler ADC that has AAA configured, the ADC now invokes responder policies after authenticating users. Previously, users could not bookmark the authentication sign-on page. This limitation no longer exists.

[From Build 50.10] [#258274, #258277]

◆ Authentication Server Stickiness

After a user authenticates successfully to an LDAP, RADIUS, or TACACS authentication or authorization server, the NetScaler ADC now connects to the same server for subsequent user authentications or authorizations. When a primary server is unavailable, this feature prevents delays while the ADC waits for the first server to time out before resending the request to the second server.

For example, assume that you have AAA configured on your ADC with three authentication policies--authpol1, authpol2, and authpol3--with priorities set to 10, 20, and 30 respectively. A user requests authentication, and the ADC discovers that the authentication server behind authpol1 does not respond to authentication

requests. The ADC then tries authpol2, which responds. When other users attempt to authenticate after this situation occurs, the ADC skips authpol1 and proceeds directly to authpol2.

[From Build 50.10] [#358894]

◆ KCD Performance Improvements

When creating a KCD Account with a delegated user certificate and CA certificate, AAA now searches the /nsconfig/ssl directory for the two certificate files, where those certificates are kept, instead of searching /nsconfig/krb.

[From Build 50.10] [#412687]

◆ Renegotiate Support for Certificate-based Policies

AAA-TM now prompts for the client certificate only when it requires the certificate to authenticate a user, not every time that a protected application requests authentication. It retrieves the certificate if two factor authentication is not enabled, or if it is configured to extract the user name from the certificate.

[From Build 50.10] [#425621]

AAA-TM, Responder

◆ Using a Responder HTML Response Page to provide Customized Error Responses

You can use the Citrix NetScaler Responder feature to create custom error responses when a user attempts to authenticate with AAA-TM and authentication fails. The Responder feature is flexible; you can create as many error responses as you wish, and respond to as many different error conditions. For example, if your users log on to different authentication servers in different geographic areas, you can customize responses to each region. A user in the United States can receive an error message that is appropriate to his or her authentication server, and be directed to a customer service telephone number in the United States. A user in Japan can receive the same for his or her different authentication server and customer service telephone number.

Briefly, to create a Responder configuration for this scenario, first create each error message and place that error message on a web server. The web server should not be located on the same physical server as the authentication server, and preferably not on the same subnet. If you have multiple regional data centers that host separate authentication servers, it is advisable to locate each error response in a different data center than hosts the authentication server that it is used for, so that local power outages or Internet connectivity problems do not affect the web server that hosts the error messages. Then, on the ADC, do the following steps:

1) Create one load balancing virtual server for each error message.

2) Create a policy for each error message that selects the requests that should receive this error message if authentication fails, and bind each policy to the appropriate load balancing virtual server.

3) Create a responder action for each error message that contains an HTTP 307 Redirect that points to the URL of the customized error message.

4) Create a responder policy for each error message that selects connections that should receive that error message, and bind that policy to the appropriate responder actions. You must craft a rule for the responder policy that selects connections that meet the appropriate criteria. For example, if you want connections that originate in the USA and that fail authentication to receive this error message, the rule could identify the region by source IP, and the authentication failure by error message.

5) Bind each responder policy to the correct virtual server, as shown below.

> bind lb vserver <vServerName> -policyName <policyName> -priority 1 -gotoPriorityExpression END

For detailed instructions on how to set up a responder configuration of this type by using the command line, see the following article on the Citrix Customer Support web site:

http://support.citrix.com/article/CTX129108

[From Build 50.10] [#414985]

AppFlow

- Indication for End of Transaction

  A transaction flag now indicates, to external collectors, whether the transaction was successfully completed or was aborted.

  [From Build 50.10] [#252000]

- The process of collecting the load time and render time of web pages has been simplified by including the clientSideMeasurements parameter as part of the add appflow action command.

  On the command line interface, enable this option by running the following command:

  > add appflow action <name> -clientSideMeasurements ENABLED

  For details about configuring an AppFlow action, see http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-ag-appflow-config-actn-tsk.html.

  [From Build 50.10] [#434577]

- NetScaler ADC now exports AppFlow records to a set of collectors if the transaction responses are served from the NetScaler cache.

  [From Build 50.10] [#423567]

Cisco RISE Integration

- Configuring RISE with NetScaler ADC and Cisco Nexus 7000 Switches.

  You can now use Remote Integrated Service Engine (RISE) technology to integrate a NetScaler ADC and a Cisco Nexus 7000 Series switch. This combination offers layered network services, including robust application delivery capabilities that accelerate application performance for all users.

With a RISE based implementation, the NetScaler functionality is available as a centralized resource that can be leveraged across the application infrastructure supported by the Cisco Nexus 7000 series switch. The key functionalities of the RISE architecture include:

- Plug and play auto-provisioning. RISE provides a plug and play auto-provisioning feature. When you directly connect the NetScaler ADC to the Cisco Nexus 7000 series switch, auto-discovery commences.

- Discovery and bootstrapping. The discovery and bootstrap mechanism enables the Cisco Nexus 7000 Series switch to communicate with the NetScaler ADC by exchanging information to set up a RISE channel, which transmits control and data packets.

- Health Monitoring. The NetScaler ADC uses its health monitoring feature to track and support server health by sending health probes to verify server responses.

- Automatic Policy Based Routing (APBR). Automatic Policy Based Routing (APBR) automatically routes the return traffic from the servers to the NetScaler ADC, preserving the client IP addresses. The automatic policy based routes are defined on the Cisco Nexus 7000 series switch. When the return traffic from the server reaches the Cisco Nexus 7000 series switch, the APBR policies defined on the switch route the traffic to the NetScaler ADC, which in turn routes the traffic to the client.

[From Build 50.10] [#413833]

Cluster

◆ Layer2 Mode Support in a Cluster

You can now use the Layer2 mode in a NetScaler cluster. For more information, see http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-cluster-l2-mode-con.html.

[From Build 50.10] [#441320]

◆ Traffic domains are now supported on a NetScaler cluster.
[From Build 50.10] [#415065]

◆ A NetScaler cluster can now be configured to run with less than (n/2 + 1) number of nodes online. To do this, while creating a cluster instance, you must set the "quorumType" parameter to none as shown here:

> add cluster instance <clid> -quorumType None

[From Build 50.10] [#407139]

◆ You can now add a failover interface set (FIS) on the nodes of a NetScaler cluster. On the cluster IP address, specify the ID of the cluster node on which the FIS must be added as follows:

> add fis <name> -ownerNode <nodeId>

Note:

- The FIS name for each cluster node must be unique.

- A cluster LA channel can be added to a FIS. You must make sure that the cluster LA channel has a local interface as a member interface.

[From Build 50.10] [#430035]

- MPTCP is now supported on a NetScaler cluster.

[From Build 50.10] [#423654]

- Net profiles are now supported on a NetScaler cluster. You can bind spotted IP addresses to a net profile which can then be bound to spotted load balancing virtual server or service (defined using a node group) with the following recommendations:

- If the "strict" parameter of the node group is "Yes", the net profile must contain a minimum of one IP address from each node of the node group member.

- If the "strict" parameter of the node group is "No", the net profile must include at least one IP address from each of the cluster nodes.

- If the above recommendations are not followed, the net profile configurations will not be honored and the USIP/USNIP settings will be used.

[From Build 50.10] [#416827]

- VRID/VRRP is now supported on a NetScaler cluster.

[From Build 50.10] [#407100]

- Link Redundancy Support in a Cluster

The NetScaler cluster now provides link redundancy with LACP. For more information, see http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-cluster-traf-dist-link-redundancy-con.html.

[From Build 50.10] [#415116]

Compression

- Specifying a Vary Header Value

When using HTTP compression, you can explicitly specify a "vary" header value for compressed responses. Prior to this enhancement, the vary header was implied to be "Accept-Encoding, User-Agent".

To specify the customized vary header globally:

> set cmp parameter -addVaryHeader ENABLED -varyHeaderValue <string>

To specify the customized vary header for a specific compression action:

> add cmp action <name> <cmpType> -addVaryHeader ENABLED -varyHeaderValue <string>

[From Build 50.10] [#346214]

Configuration Utility

- The NetScaler graphical user interface (GUI) has been enhanced to provide a better user interaction experience. It now provides you with a workflow-based experience, which guides you through the entire configuration. The configuration settings have been classified as basic and advanced for some features. The NetScaler ADC

configuration utility and NetScaler Gateway configuration utility has also been reimplemented in HTML. As a result of these enhancements, the GUI does not display pop-up dialog boxes for most features and you no longer need Java Runtime Environment (JRE) to access these features through the GUI.

For more information, see http://support.citrix.com/proddocs/topic/ns-rn-main-release-10-5-map/ns-rn-changes-gui-10-5-con.html

[From Build 50.10] [#251336, #251607, #251645, #251760, #251797, #257879, #257949, #261240, #261339, #285382]

◆ Distinguish between Commands Executed from Different NetScaler Interfaces

The NetScaler now keeps track of the interfaces through which operations are executed. You can view this information in syslogs (in the NetScaler GUI, navigate to Configuration > System > Auditing > Audit Messages > Syslog messages) or in the ns.log (located at the /var/log/ directory) file.

For example, operations that are performed through the API are flagged as "API CMD_EXECUTED".

[From Build 50.10] [#361917]

Content Accelerator

◆ Content accelerator is a NetScaler feature that you can use in a Citrix ByteMobile T1100 deployment, to store data on a Citrix ByteMobile T2100 appliance. This saves bandwidth and provides faster response times, because the NetScaler does not have to connect to the server for repeated requests of the same data.

For more information, see http://support.citrix.com/proddocs/topic/ns-optimization-10-5-map/ns-content-accl-con.html.

[From Build 50.10] [#427565]

Content Switching

◆ Multiple Port Content Switching Support for HTTP and SSL Virtual Servers

You can now configure the NetScaler ADC so that HTTP and SSL content switching virtual servers listen on multiple ports without having to configure separate virtual servers. This feature is especially useful if you want to base a content switching decision on a part of the URL and other L7 parameters. Instead of configuring multiple virtual servers with the same IP address and different ports, you can now configure one IP address and specify the port as *. As a result, the configuration size is also reduced.

For more information, see http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-5-map/ns-cs-customizing-multiport-http-ssl-tsk.html

[From Build 50.10] [#386601]

◆ Content Switching Support for Diameter

The NetScaler ADC now supports content switching for the Diameter protocol. A number of expressions have been added, and you can use them to examine the header and the attribute-value pairs (AVPs) in a Diameter packet. On the basis of

that information, you can forward the request to the selected load balancing virtual server.

For more information, see http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-5-map/ns-cs-customizing-diameter-for-cs-tsk.html.

[From Build 50.10] [#413072]

◆ When you create a content switching virtual server, NetScaler now supports using DNS TCP as the protocol used by the virtual server.

[From Build 50.10] [#365650]

◆ Multiple Port Content Switching Support for SSL_TCP Virtual Servers

You can now configure the NetScaler ADC so that SSL_TCP content switching virtual servers listen on multiple ports without having to configure separate virtual servers. Instead of configuring multiple virtual servers with the same IP address and different ports, you can now configure one IP address and specify the port as * . As a result, the configuration size is also reduced.

[From Build 50.10] [#450367]

DNS

◆ Enabling or Disabling the Recursion Available Flag

A new parameter -RecursionAvailabe (YES|NO) is introduced in load balancing virtual server (for DNS and DNS_TCP types). The option by default has a value of NO. When you use the load balancing virtual server to load balance recursive resolvers, you can turn this option to YES. This will cause NetScaler to respond with RA bit set on all responses.

[From Build 50.10] [#403114, #248936, #269857, #388338]

◆ NAPTR DNS Record

NetScaler ADC supports DNS NAPTR (Naming Address Pointer) record type. NAPTR records are generic DNS record type, but are commonly used in internet telephony for service discovery. They therefore enable clients to discover which server the request should go to for a particular service and which protocol to use to connect to the server.

NetScaler ADCs support NAPTR in two modes: ADNS mode and proxy mode. You can create a NAPTR record using both, command line interface and the NetScaler Configuration Utility.

For more information, see http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-5-map/ns-tmg-dns-crt-naptr-rec-tsk.html

[From Build 50.10] [#413773]

◆ CNAME Record Caching

NetScaler ADC when deployed in a proxy mode does not always send the query for an address record to the back-end server. This happens when for an answer to a

query for an address record, a partial CNAME chain is present in the cache. Under few conditions, ADC caches the partial CNAME record and serves the query from the cache.

For more information, see http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-5-map/ns-tmg-dns-caching-cname-record-con.html

[From Build 50.10] [#422509]

◆ AA bit set for response from NetScaler Cache

In the previous releases, for NODATA responses with AA bit, NetScaler would ignore AA bit (authoritative bit) while caching. For such DNS queries NetScaler would reply with NODATA response from cache without setting the AA bit. The behavior has been enhanced with current release. NetScaler will respond with the AA bit for negative cached responses just as it does for positive cache responses.

[From Build 50.10] [#285009]

DataStream

◆ Support for Fallback to NTLM Authentication

Currently AAA supports Kerberos authentication only with Datastream Windows Authentication. AAA does not support fallback to NTLM if Kerberos authentication fails.

[From Build 50.10] [#382693]

◆ Support for Database Specific Load Balancing for MySQL

Database specific load balancing is now supported for MySQL databases. If a database is available on multiple servers but is online on only some of these servers, the client request is forwarded to the server on which the database is online. Enable the DBSLB option when you create a load balancing virtual server. To store the database list on the NetScaler ADC, while creating a MYSQL-ECV monitor, enable storeDB.

[From Build 50.10] [#418490]

◆ Support for SQL Server High-Availability (HA) Group Deployment

The NetScaler ADC now supports AlwaysOn Availability group deployment in database specific load balancing for MSSQL 2012.

For more information, see http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-5-map/ns-dbproxy-db-specific-lb-for-mssql-2012-tsk.html

[From Build 50.10] [#415485]

◆ Support for Transparent Deployment Mode in MySQL

You can now configure the NetScaler ADC to operate transparently between MySQL clients and servers, and to only log or analyze details of all client-server transactions. Transparent mode is designed so that the ADC only forwards MySQL requests to the server, and then relays the server's responses to the clients. As the requests and responses pass through the ADC, the ADC logs information gathered from them, as specified by the audit logging or AppFlow configuration, or collects

statistics, as specified by the Action Analytics configuration. You do not have to add database users to the ADC.

[From Build 50.10] [#410824]

GSLB

◆ GSLB Auto Sync Enhanced to to Sync Static Proximity Database

GSLB autosync has been enhanced to synchronize global server load balancing (GSLB) static proximity databases. When autosync is triggered on the master site, first the static proximity database is synchronized followed by the synchronization of configuration.

For more information see, http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-5-map/ns-gslb-synchro-static-proximity-db.html

[From Build 50.10] [#286236]

Integrated Caching

◆ Increased Metadata Cache Capacity

The number of cached objects that the cache memory can store has now been increased.

[From Build 50.10] [#417677]

◆ Cache Object Persistence in a High Availability Setup

When integrated caching is used in a high availability setup, in addition to storing the cached objects on the primary appliance, the objects are also stored on the secondary appliance. This reduces bandwidth usage as cached objects are not lost during failover and the request can then be served directly from the cache of the secondary appliance.

To enable this functionality globally, execute the following command:

> set cache parameter -enableHaObjPersist Yes

To enable this functionality on a specific content group, execute the following command:

> set cache contentGroup <name> -persistHA Yes

[From Build 50.10] [#329012]

Load Balancing

◆ Monitors for XenMobile Device Manger (XDM) and XenMobile Device Connector (XNC)

NetScaler allows a user to create monitors to check the status of the XenMobile Device Manager (XDM) and XenMobile NetScaler Connector (XNC) servers. The citrix-xdm monitor is used to monitor the XDM server while the citrix-xnc-ecv monitor is used to monitor the XNC server. You can add these monitors by using the add lb monitor command from the command-line interface or by using the GUI.

* The XDM monitor uses the username, password, and site path strings to probe the XDM server.

* The XNC monitor uses the username, password, send, and recv strings to probe the XNC monitor.

[From Build 50.10] [#402361]

◆ Support for Jumbo Frames in RADIUS

The NetScaler ADC now supports RADIUS jumbo frames.

For more information on jumbo frames, see http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-nw-jf-overview-con.html.

[From Build 50.10] [#429415]

◆ Increased Limits on the Number of Service Groups

You can now configure up to 8K (8192) service groups on a NetScaler appliance. The earlier limit was 4K (4096) service groups.

[From Build 50.10] [#406355]

◆ Rate Limiting Support for Diameter

You can now configure rate limiting for diameter messages. In the following example, NetScaler limits the rate to 100 messages per second and sends UNABLE_TO_DELIVER if the rate exceeds that limit.

> add ns limitidentifier rslm1 -threshold 100 –timeSlice 1000 -mode REQUEST_RATE -limittype bursty

> add responder action rsact1 respondwith "DIAMETER.NEW_ERROR_ANSWER + DIAMETER.NEW_AVP(263, DIAMETER.REQ.SESSION_ID.VALUE) + DIAMETER.NEW_AVP_UNSIGNED32(268, 3002)"

> add responder policy rspol1 "SYS.CHECK_LIMIT("rslm1")" rsact1

[From Build 50.10] [#399053]

NITRO API

◆ Python SDK for NetScaler SDX and NetScaler Insight Center NITRO

NITRO now provides Python SDKs for configuring the NetScaler SDX appliance and the NetScaler Insight Center appliance. The SDKs can be downloaded from the Downloads page of the appliance's configuration utility.

[From Build 50.10] [#451606]

◆ Python SDK for NetScaler NITRO

NITRO now provides a Python SDK for configuring the NetScaler appliance. The SDK can be downloaded from the Downloads page of the NetScaler appliance's configuration utility.

[From Build 50.10] [#425725]

◆ Uploading and Retrieving Files for NetScaler Using NITRO

NetScaler operations such as configuring SSL certificates requires the input files to be available locally on the NetScaler appliance. NITRO allows you to perform file operations such as uploading file to the NetScaler, retrieving a list of files and the file content from the NetScaler, and also delete files from the NetScaler. These operations can be performed for files of type: txt, cert, req, xml, and key.

For more information, see http://support.citrix.com/proddocs/topic/netscaler-main-api-10-5-map/ns-nitro-rest-file-ops-ref.html.

[From Build 50.10] [#262824, #257935, #259969]

NetScaler Insight Center

- NetScaler Insight Center now saves the following data for a specific time period before it is purged:

  * 30 second data - Saves for 6 minutes

  * 5 minute data - Saves for 65 minutes

  * Hourly data - Saves for 25 hours

  * Daily data - Saves for 31 days

  [From Build 50.10] [#404805]

- Even if Appflow is disabled for a virtual server, you can clear the configuration in the NetScaler Insight Center by selecting Clear AppFlow Configurations from the Action list.

  [From Build 50.10] [#399329]

- HDX Insight now provides a report about active sessions, grouped by server IP and gateway IP.

  [From Build 50.10] [#398322]

- Cache Redirection Insight Support

  NetScaler Insight Center now analyzes the traffic flowing through NetScaler ADC to cache servers and origin servers, and provides useful information about the cache performance, such as:

  - Bandwidth saved while serving requests from the cache server instead of the origin server.

  - Bandwidth consumed when requests bypassed the cache server and were served from the origin server.

  - Number of times a URL was accessed from the cache server instead of the origin server.

  For details on Cache Redirection Insight, see http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-usecase-webinsight-cache.html.

  [From Build 50.10] [#409842]

- Authentication and Authorization Support.

Authentication with the NetScaler Insight Center virtual appliance can be local or external. With external authentication, NetScaler Insight Center grants user access on the basis of the response from an external server. It supports the following external authentication protocols:

-Remote Authentication Dial In User Service (RADIUS)

-Terminal Access Controller Access-Control System (TACACS)

-Lightweight Directory Access Protocol (LDAP)

Authorization through the NetScaler Insight Center virtual appliance is local. The virtual appliance supports two levels of authorization. Users with superuser privileges are allowed to perform any action. Users with readonly privileges are allowed to perform only read operations. The authorization of SSH users requires superuser privileges. Users with readonly privileges cannot log on through SSH.

For more information see, http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-configuring-authentication-authorization-settings.html

[From Build 50.10] [#412466]

◆ HDX Insight reports now include details about session reconnects, client-side retransmissions, and server-side retransmissions.

[From Build 50.10] [#392016]

◆ On the dashboard, if you move the columns in a table and refresh the page, the column ordering is sometimes reset to default.

[From Build 50.10] [#414155]

◆ In the dashboard, you can now select and rearrange the columns displayed in the tables. These changes persist across user sessions.

[From Build 50.10] [#423451]

◆ Data Record Log Settings

NetScaler Insight Center now supports data record logs, which provide detailed information about AppFlow records that NetScaler Insight Center collects from NetScaler ADCs.

For more information, see http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-change-data-record-log-settings.html

[From Build 50.10] [#421777]

◆ NetScaler Insight Center adaptive threshold functionality dynamically sets the threshold value for the maximum number of hits on each URL.

For more information, see http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-manage-threshold-tsk.html

[From Build 50.10] [#378995]

◆ EUEM Session Data on HDX Insight Reports

HDX Insight reports now displays EUEM session data, which indicates the availability of EUEM data when an EUEM channel is established between the client and the server.

[From Build 50.10] [#367114]

◆ The top-right corner of the page now displays a percentile icon, which you can click to display percentile values and the highest and lowest values for a selected metric.

[From Build 50.10] [#418196]

◆ NetScaler Insight Center can now dynamically set the threshold value for the maximum number of hits on each URL. For details, see http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-manage-threshold-tsk.html

NetScaler Insight Center now facilitates efficient querying of its database.

For details on enabling this functionality, see http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-change-db-index-settings.html

You can now enable NetScaler Insight Center to periodically remove the out-of-date content from its database. For details, see http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-change-db-cleanup-settings.html

[From Build 50.10] [#479004]

◆ The active sessions data on the dashboard now include the following metrics:

Client IP: IP address of the client

Server IP: IP address of the server

NetScaler IP: NetScaler IP address

[From Build 50.10] [#427504]

◆ You can now customize NetScaler Insight Center reports to display the metrics that you want, and you can specify bar graphs or line graphs.

To make these changes, open the drop-down list next to the percentage icon in the top-right corner of the dashboard.

[From Build 50.10] [#427187]

◆ You can now configure the ICA session timeout value for inactive sessions on the NetScaler Insight Center configuration tab.

For details, see http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-ica-session-timeout-tsk.html

[From Build 50.10] [#431957]

◆ Hop Diagram Support

The HDX Insight reports now support hop diagrams, which provide complete details about the client, NetScaler ADC, and server in an active session.

To display the hop diagram, on the dashboard tab, navigate to HDX Insight > Users >, click on a user name and, in the Current Application Sessions table, click on the session diagram icon.

[From Build 50.10] [#443824]

◆ Geo Map Support

The NetScaler Insight Center geo maps feature displays the usage of web applications across different geographical locations on a map. Administrators can use this

information to understand the trends in application usage and for capacity planning.

Geo maps provide information that answers questions such as the following:

-Which region has the highest number of clients accessing an application?

-Which region has the highest response time?

-Which region is consuming the most bandwidth?

For more information, see http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-usecase-geo-maps.html

[From Build 50.10] [#322120]

◆ The database cache functionality of NetScaler Insight Center stores database content locally in the cache and serves the content to users without accessing the database server.

For more information, see http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-change-db-cache-settings.html.

[From Build 50.10] [#456295]

◆ Managing Session Timeout Period

You can now configure the timeout period for how long a user or a group can remain in an idle state before being terminated.

Enable this option while configuring user accounts or user groups.

For more details on configuring a user account or a group account, see http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-add-user.html or http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-add-group.html.

[From Build 50.10] [#452424]

◆ If the length of URLs displayed in the Web Insight reports is very long, you can enable the trim URL functionality to remove the query string from the URL.

For details about configuring this functionality, see http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-change-url-parameter-settings.html

[From Build 50.10] [#463741]

◆ Exporting Reports

You can now save the Web Insight reports or HDX Insight reports in PDF, JPEG or PNG format on your local computer. You can also schedule the export of the reports to specified email addresses at various intervals.

For more information, see http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-export-report-con.html.

[From Build 50.10] [#320860]

- For debugging an issue, the technical support bundle that you generate to send to the technical support team now automatically includes NetScaler ADC data along with the NetScaler Insight Center data.

  You can also choose to include the debug logs and data distribution logs.

  [From Build 50.10] [#474070]

- The GUI displays a real-time graphical representation of the CPU, memory, and disk resources used by the NetScaler Insight Center virtual appliance.

  To display additional details, on the Configuration tab, navigate to NetScaler Insight Center and click Statistics.

  [From Build 50.10] [#474067]

- Data record logs provide detailed information about appflow records that NetScaler Insight Center collects from NetScaler ADCs.

  For more information, see http://support.citrix.com/proddocs/topic/ni-10-5-map/ni-change-data-record-log-settings.html.

  [From Build 50.10] [#471025]

- HDX Insight Center reports now support the following metrics:

  -Client side zero window size event: This counter indicates how many times the client advertised a zero TCP window.

  -Server side zero window size event: This counter indicates how many times the server advertised a zero TCP window.

  -Client side fast RTO: This counter indicates how many times the retransmit timeout was invoked on the client-side connection.

  -Server side fast RTO: This counter indicates how many times the retransmit timeout was invoked on the server-side connection.

  [From Build 50.10] [#424355]

Networking

- Netprofile Support for Link Load Balancing Configurations

  You can now associate a netprofile with a link load balancing configuration. The NetScaler ADC then uses one of the IP addresses in the netprofile as the source address for outbound traffic related to the link load balancing configuration.

  A netprofile can include a NetScaler owned IP address or an IP set, which is a set of NetScaler owned IP addresses. You can associate a netprofile with link load balancing virtual servers as well as with the bound services. A netprofile associated with a link load balancing virtual server always take precedence over netprofiles associated with the bound services.

For more information on netprofiles, http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-5-map/ns-lb-clienttraffic-usespecifiedsrcip-tsk.html.

[From Build 50.10] [#356081]

◆ The ZebOS dynamic routing software package has been upgraded to version 7.10.2.

[From Build 50.10] [#435000]

◆ VMAC Based Traffic Domains

You can now associate a traffic domain with a VMAC address instead of with VLANs. The NetScaler ADC then sends the traffic domain's VMAC address in all responses to ARP queries for network entities in that domain. As a result, the ADC can segregate subsequent incoming traffic for different traffic domains on the basis of the destination MAC address. The NetScaler ADC identifies traffic for a traffic domain if it is destined to the same VMAC address that is associated with the traffic domain.

For more information, see http://support.citrix.com/proddocs/topic/ns-system-10-5-map/nw-td-vmac-traffic-domain-intro-tsk.html.

[From Build 50.10] [#425108]

◆ IPv6 Forwarding Session Rules

Now, you can create forwarding session rules for IPv6 traffic. By default, the NetScaler appliance does not create session entries for traffic that it only forwards (L3 mode). For a case in which a client request that the appliance forwards to a server results in a response that has to return by the same path, you can create a forwarding-session rule. A forwarding-session rule creates forwardingsession entries for traffic that originates from or is destined for a particular network and is forwarded by the NetScaler appliance.

When configuring an IPv6 forwarding-session rule, you can specify either an IPv6 prefix or an ACL6 as the condition for identifying IPv6 traffic for which the forwarding-session entry to be created:

- Using an IPv6 prefix . When you specify an IPv6 prefix, the appliance creates forwarding sessions for those IPv6 traffic that are sourced from networks that matches the IPv6 prefix.

- Using an ACL6 rule . When you use an ACL6 rule, the appliance creates forwarding sessions for those IPv6 traffic that match the conditions specified in the ACL6 rule.

Note: When the appliance is configured as a high availability node, Connection Failover for synchronizing IPv6 forwarding session entries with the secondary node is not supported.

For more information, see http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-nw-interfaces-confrng-fwd-sessions-tsk.html.

[From Build 50.10] [#251234]

◆ Support for Inter Traffic Domain Entity Bindings

You can now bind services in one traffic domain to a virtual server in another traffic domain. All the services to be bound to a virtual server in a different traffic domain must reside in the same traffic domain.

There is no command or parameter introduced for this support. You configure this support by using the existing bind lb vserver command or the related configuration utility procedure. This capability can facilitate interaction between different traffic domains. In an enterprise, servers can be grouped in different traffic domains. Virtual servers are created in a traffic domain that faces the internet. A virtual server from this traffic domain can be configured to load balance servers in another traffic domain. This virtual server receives connection requests from the Internet to be forwarded to the bound servers.

For more information, see http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-nw-supp-traff-enty-tsk.html.

[From Build 50.10] [#405295]

 ◆ A parameter Source IP Persistency has been introduced in RNAT rules and Netprofiles:

Source IP Persistency for RNAT Sessions

The source IP persistency of a RNAT rule enables the NetScaler ADC to use the same NAT IP address for all RNAT sessions initiated from a particular server.

Source IP Persistency for NetProfiles

The source IP persistency of a netprofile associated with a virtual server or service enables the NetScaler ADC to use the same address, specified in the net profile, for all sessions initiated from a particular client.

[From Build 50.10] [#437359]

 ◆ Increased Number of Interfaces for Link Aggregation Channels

You can now bind up to 16 interfaces to a link aggregation channel. The channel can be either static or LACP.

[From Build 50.10] [#437366, #389319]

 ◆ Support for VXLANs

Now the NetScaler ADC supports Virtual eXtensiable Local Area Network (VXLANs). A VXLAN is an overlay solution that creates layer 2 overlay networks over layer 3 infrastructure by encapsulating Layer-2 frames in UDP packets. Each VXLAN is identified by a unique 24-bit identifier called the VXLAN Network Identifier (VNI). Only network devices within the same VXLAN can communicate with each other.

[From Build 50.10] [#366992]

 ◆ ZebOS API Access

With a new configuration object, router DynamicRouting, you can use NITRO APIs to configure dynamic routing protocols on a NetScaler appliance.

[From Build 50.10] [#229714, #222015, #406589]

◆ The NetScaler ADC now supports the industry standard (EEE 802.1AB) Link Layer Discovery Protocol (LLDP). LLDP is a layer 2 protocol that enables the NetScaler ADC to advertise its identity and capabilities to the directly connected devices, and also learn the identity and capabilities of these neighbour devices.

Using LLDP, the NetScaler ADC transmits and receives information in the form of LLDP messages known as LLDP packet data units (LLDPDUs). An LLDPDU is a sequence of type, length, value (TLV) information elements. Each TLV holds a specific type of information about the device that transmits the LLDPDU. The NetScaler ADC sends the following TLVs in each LLDPDU:

* Chassis ID

* Port ID

* Time-to-live value

* System name

* System description

* Port description

* System capabilities

* Management address

* Port VLAN ID

* Link aggregation

Note: You cannot specify the TLVs to be sent in LLDP messages.

For more information, see http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-nw-config-llayer-dics-protocol-tsk.html.

[From Build 50.10] [#235640]

◆ Configuring Link Redundancy by using LACP channels

Link Redundancy by using LACP channels enables the NetScaler appliance to logically create sub channels from a LACP channel where one of the sub channel is active and the remaining sub channels stay in standby mode. If the active sub channel fails or does not meet a minimum threshold throughput, one of the standby sub channel takes over and becomes active.

The NetScaler appliance forms a sub channels from links that are part of the LACP channel and are connected to a particular device. For example, for a LACP channel with four interfaces on a NetScaler appliance, where two of the interface is connected to device A, and the other two interfaces are connected to device B, then the NetScaler appliance logically creates two sub channels, one sub channel with two links to device A, and the other sub channel with the remaining two links to device B.

The lrMinThroughput parameter is introduced for configuring link redundancy for a LACP channel. This parameter specifies the minimum throughput threshold to be met by the active sub channel of a LACP channel. When the throughput of the active channel falls below the lrMinThroughput , link failover occurs and one of the standby sub channels becomes active.

For example, set channel la/1 -lrMinThroughput 2000

Link redundancy for a LACP channel is disabled, which is also the default setting, when you set the lrMinThroughput parameter of the LACP channel to zero or when you unset this parameter.

Note: In an HA configuration, if you want to configure throughput (throughput parameter) based HA failover and link redundancy (lrMinThroughput parameter) on a LACP channel, you must set a lesser or equal value to the throughput parameter as compared to the lrMinThroughput parameter.

For example, set channel la/1 throughput 2000 -lrMinThroughput 2000

HA failover does not occur if any of the sub channels meets the lrMinThroughput parameter value even when the total throughput of the LACP channel does not meet the throughput parameter value.

HA failover occurs only when the entire sub channels of the LACP channel does not meet the lrMinThroughput parameter value and the total throughput of the LACP channel does not meet the throughput parameter value.

For more information, see http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-nw-config-lr-lacp-tsk.html.

[From Build 50.10] [#346763]

Optimization

◆ Front End Optimization Support

The NetScaler ADC now supports the front end optimization feature, which reduces the load time and render time of web pages by simplifying and optimizing the content to be served to the client browser.

This feature optimizes HTML content, and the cascading style sheets (CSS), JavaScript, and images that are embedded in the HTML content.

For details, see http://support.citrix.com/proddocs/topic/ns-optimization-10-5-map/ns-feo-con.html.

[From Build 50.10] [#292039, #392818, #449669, #450295]

Policies

◆ Variable Support for Policies

Policy variables are named objects that can hold one or more values that can be set and modified at runtime. The concept of variables is essentially the same as in programming languages. Variable values can be of two types:

- ulong (a 64-bit unsigned integer, with values from 0 to 2^64-1)

- text (a sequence of bytes with a configured maximum length).

Additionally, there are two variable types:

- Singletons variables hold one ulong or text value.

- Maps hold one or more entries, each entry having a text key and a ulong or text value. The key can be used to find the value. In a map, more than one map entry may have the same value, but each map entry must have a different key.

For more information, see http://support.citrix.com/proddocs/topic/ns-main-appexpert-10-5-map/ns-pol-variable-con.html.

[From Build 50.10] [#368447]

Responder

♦ Embedded Expressions in Responder Responses

You can now add Netscaler expressions with default syntax to HTML pages that are used with responder actions of the respondWithHtmlpage type. Any expression that is supported for use in a respondWith response can be used in a respondWithHTMLPage response. To embed expressions in HTML pages simply surround the expressions with "${" and "}". This functionality enables you to include information about the request that generated the Responder action in the response.

[From Build 50.10] [#423928]

♦ The Responder feature now supports the Diameter protocol.

A number of NetScaler expressions have been added that enable the user to examine the header and the attribute-value pairs (AVPs) in a diameter packet. These expressions enable the user to look up AVPs by index, ID, or name, examine the information in the AVP, and send a response based on that information.

[From Build 50.10] [#318387]

Rewrite

♦ The Rewrite feature now supports the Diameter protocol.

A number of NetScaler expressions have been added that enable the user to examine the header and the attribute-value pairs (AVPs) in a diameter packet. These expressions enable the user to look up AVPs by index, ID, or name, examine the information in the AVP, and replace/insert/delete AVPs if necessary.

[From Build 50.10] [#318382]

SSL

♦ SSL Certificate Chain

As part of the SSL handshake, when a client requests a certificate, the NetScaler ADC presents a certificate and the chain of issuer certificates that are present on

the ADC. An administrator can view the certificate chain for the certificates present on the ADC and install any missing certificates.

For more information, see http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-5-map/ns-ssl-display-cert-chain-tsk.html

[From Build 50.10] [#437610]

◆ Creating an SSL Profile

You can use an SSL profile to specify how a NetScaler appliance processes SSL traffic. The profile is a collection of SSL parameter settings for SSL entities, such as virtual servers, services, and service groups, and offers ease of configuration and flexibility. Previously, you could specify only one set of global parameters. Now, you can create multiple sets (profiles) of global parameters and assign different sets to different SSL entities. SSL profiles are classified into two categories:

-Front end profiles, containing parameters applicable to the front-end entity. That is, they apply to the entity that receives requests from a client. For example, an SSL virtual server.

-Backend profiles, containing parameters applicable to the back-end entity. That is, they apply to the entity that sends client requests to a server. For example, an SSL service.

For more information, see http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-5-map/ns-ssl-profiles-tsk.html

[From Build 50.10] [#401011, #321967]

◆ Importing SSL Resources from Remote Hosts

The NetScaler appliance now supports importing SSL resources, such as certificates, private keys, CRLs, and DH keys, from remote hosts even if FTP access to these hosts is not available. This is especially helpful in environments where shell access to the remote host is restricted.

For more information, see http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-5-map/ns-ssl-importing-ssl-files-from-remote-hosts-tsk.html

[From Build 50.10] [#210405]

◆ Support for DTLS Protocol

The NetScaler ADC now supports DTLS protocol to secure UDP traffic. The DTLS protocol (RFC 4347), can be used to secure UDP applications such as media streaming, VOIP, and online gaming for communication.

For more information, see http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-5-map/ns-ssl-config-dtls-server-tsk.html

[From Build 50.10] [#400350]

◆ Sending an SSLv2 Compliant Client Hello Message

As part of the SSL handshake with the server, the NetScaler appliance now sends a Client Hello message based on the version (for example SSLv3 or TLS1.0) that is configured on the appliance. Earlier, it sent an SSLv2 compliant Client Hello message to the server.

[From Build 50.10] [#378806, #204465, #406907]

◆ Support for Common Name Check during Server Authentication

In end-to-end encryption with server authentication enabled, you can include a common name in the configuration of an SSL service or service group. The name that you specify is compared to the common name in the server certificate during an SSL handshake. If the two names match, the handshake is successful. This configuration is especially useful if there are, for example, two servers behind a firewall and one of the servers spoofs the identity of the other. If the common name is not checked, a certificate presented by either server is accepted if the IP address matches.

For more information, see http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-5-map/ns-ssl-config-common-name-for-cert-tsk.html

[From Build 50.10] [#381821, #332628]

◆ SSL Renegotiation

SSL renegotiation is now blocked by default. In earlier releases, the default setting was to allow SSL renegotiation.

[From Build 50.10] [#481577]

◆ Setting the Limit for Disabled SSL Chips

You can now set a limit to the number of disabled SSL chips after which the appliance restarts.

At the command prompt, type:

> set ssl parameter -cryptodevDisableLimit <positive_integer>

A chip is marked disabled after the third failed reinitialization attempt.

[From Build 50.10] [#376153]

System

◆ SNMP V3 Support for Traps

Trap class, destination along with version will now act as unique identifier for a trap destination. This will allow configuration of same destination with different versions. All commands will take version V2 as default value. Set and Unset commands can no longer change version.

[From Build 50.10] [#416930]

◆ Explicit Congestion Notification (ECN)

The NetScaler appliance now supports ECN, which sends notification of network congestion state to the sender and takes corrective measures for data congestion or data corruption. When ECN is enabled, the NetScaler automatically differentiates between corruption loss and congestion loss. The NetScaler implementation of ECN is RFC 3168 compliant.

ECN must be enabled on the TCP profile to which you want it to apply.

To enable ECN using the CLI:

> add ns tcpProfile <name> -ecn ENABLED

[From Build 50.10] [#249145]

◆ TCP Timestamp based on RFC 1323

The NetScaler now provides the TCP timestamp as detailed in RFC 1323. Using this timestamp, the NetScaler can provide the Round Trip Time Measurement (RTTM). For this option to work, at least one side of the connection (client or server) must support it.

[From Build 50.10] [#204374, #249144, #317249, #401162]

◆ SNMP Trap for Port Allocation Failures

NetScaler ADC sends SNMP trap when port allocation fails on the NetScaler. The following SNMP OID is added: dstip (1.3.6.1.4.1.5951.1.1.0.143)

[From Build 50.10] [#360334]

◆ Restrict Interface-level System Session Timeout

The system session timeout for a specific NetScaler interface (GUI, CLI, API) is now restricted to the timeout value that the administrator has configured for the user that is accessing the interface. For example, let us consider an user "publicadmin" who has a timeout value of 20 minutes. Now, when accessing an interface, the user must specify a timeout value that is within 20 minutes.

[From Build 50.10] [#405501, #439031]

◆ Application Layer Protocol Negotiation (ALPN) Extension support

The NetScaler now supports the APLN extension for negotiating the SPDY protocol over SSL/TLS. The use of ALPN provides higher rate of TPS performance on the NetScaler. APLN replaces the previous method of NPN (Next Protocol Negotiation).

[From Build 50.10] [#430862]

◆ When the configured external authentication server is not available, the NetScaler can be configured to allow local user access to perform administrative tasks. To enable this function, enable the "localAuth" parameter of the "set system parameter" command.

[From Build 50.10] [#315474]

◆ MPTCP Enhancements

The NetScaler now supports the following MPTCP enhancements:

- One RTT subflow setup

- Long-lived MPTCP sessions

- MPTCP fast open

[From Build 50.10] [#435632]

◆ SPDY v3 Support

The NetScaler appliance now supports SPDY v3 with Application Layer Protocol Negotiation (ALPN).

[From Build 50.10] [#329669]

- NetScaler support for D-SACK AND F-RTO

  The NetScaler appliance can now detect spurious re-transmissions by using TCP duplicate selective acknowledgement (D-SACK) and Forward RTO-Recovery (F-RTO). In case of spurious re-transmissions, the congestion control configurations are reverted to their original state. The NetScaler implementation of D-SACK is RFC 2883 compliant and F-RTO is RFC 5682 compliant.

  D-SACK and F-RTO must be enabled on the TCP profile to which you want it to apply.

  To enable these settings by using the CLI:

  > add ns tcpProfile <name> -dsack ENABLED -frto ENABLED

  [From Build 50.10] [#439129]

- Differentiated services code point (DSCP) Support

  The NetScaler ADC can now retain and forward received DSCP code in end-point mode. This capability supports end-to-end quality of service (QOS) checks for load balanced traffic.

  [From Build 50.10] [#436946]

- NetScaler now supports BIC and CUBIC TCP congestion control algorithms.

  [From Build 50.10] [#406270]

Traffic Domain

- Features Supported in Traffic Domains

  The following NetScaler features are now supported in all traffic domains configured on a NetScaler appliance:

  * RNAT6

  * IPv4 and IPv6 Forwarding Sessions

  * NAT64

  * NAT46

  You can use the new Traffic Domain (TD) parameter to specify or identify a traffic domain in commands and GUI elements related to these features.

  For more information, see http://support.citrix.com/proddocs/topic/ns-system-10-5-map/nw-td-supportd-unsupportd-ns-featurs-con.html.

  [From Build 50.10] [#383056]

- You can now configure rate limiting for traffic domains. The following expression has been added to the NetScaler expressions language for identifying traffic associated with traffic domains.

  client.traffic_domain.id

You can configure rate limiting for traffic associated with a particular traffic domain, a set of traffic domains, or all traffic domains.

For more information, see http://support.citrix.com/proddocs/topic/ns-main-appexpert-10-5-map/ns-nw-ratelimit-td-con.html.

[From Build 50.10] [#403748]